Client Service Manual

WOM Technology Management Group

Contents

Purpose of this Guide 7

Solutions Agnosticism 7

Cyber Security Risk Assessment 8

- Phase I: Kick-Off 8
- Discovery Consultation ("Kick-Off Call") 8
- Remote Access Tool Deployment: 8
  1. End User Deployment 8
  2. Full-Service Deployment 8
  3. Internal IT Deployment 8
- Phase II: Assessment 8
- Scan for Personally Identifiable Information (PII) 9
- Scan for Exposure to Known Vulnerabilities 9
- Scan Equipment and Compare with CIS Standards for Security 9
- Simulated Phishing Test 9
- Dark Web Scan 9
- Run Software as a Service (SaaS) Scan 9
- Evaluate Equipment and Infrastructure 9
- Financial Exposure Analysis 9
- Cyber Liability Readiness Assessment 10
- Compliance Baseline Assessment 10
- Phase III: Review & Roadmap 11
- Present Results and Recommendations 11
- Roadmap 11
- Offering for Ongoing Services 11

Ongoing Risk Management: **Confidence as a Service® CyberWatch** 12

- Implementation Process 12
- The Critical Importance of Proactive Cybersecurity Evaluations 13
  - Anticipating Threats Before They Strike 13
  - Adapting to the Evolving Threat Landscape 13
  - Compliance and Regulatory Requirements 13
  - Strategic Decision-Making and Resource Allocation 13
  - Building a Culture of Cyber Resilience 13
- Objectives and Benefits of Simulating Real-World Attack Scenarios 14
  - Objective: Realistic Assessment of Security Posture 14
  - Benefit: Enhanced Detection and Response Capabilities 14
  - Objective: Testing of Incident Response Plans 14

Benefit: Compliance and Assurance 14
Objective: Employee Awareness and Training 14
Benefit: Strategic Cybersecurity Investments 14
Service Components 15
Penetration Testing 15
Vulnerability Analysis 16
Ongoing Vulnerability Management 18
Consulting and Executive Decision Support 19
Benefits of CyberWatch 20
Enhanced Cyber Defense Capabilities 20
Proactive Identification and Remediation of Vulnerabilities 20
Executive Decision Support 20
Scalability and Flexibility 20
Building a Culture of Cyber Resilience 20
Client Responsibilities 21
Providing Necessary Access and Information 21
Active Participation in Quarterly Reviews and Mitigation Planning 21
Incident Response Preparedness 21
Implementing Recommended Mitigation Strategies 21
Fostering a Culture of Security Awareness 21
Feedback and Continuous Improvement 22
Client Feedback 22
Continuous Improvement Practices 22
Collaboration with the Client Experience Team 22
Outcome of Continuous Improvement 22
FAQs and Common Concerns 23
Supercharged Service with Remote Monitoring and Management (RMM) 24
Here are some of the key benefits of having RMM tools at your fingertips: 24
System Monitoring 24
Real-Time Monitoring 24
Regular Health Checks 24
Minimal User Interaction 24
Help Desk Services 25
Ticketing System for Issue Tracking and Resolution 25
Remote Support Tools for Quick Issue Resolution 25
Training for End Users 25
Ticket Prioritization 25

Protecting Your Hard-Earned Digital Assets with Cloud Backup and Restoration 26
Why Microsoft 365? 26
Microsoft 365 Setup and Configuration 27
Not Using Microsoft 365 Already? No Problem, We'll Fix this Together! 27
Protecting Your Microsoft 365 Data with our Cloud-to-Cloud Backup Solutions 27
Implementing Best Practices for Microsoft 365 Management 28
Cybersecurity Implementation 28
Microsoft 365 Hardening 29
Configure Secure Score and Compliance Score 29
Set up Data Loss Prevention (DLP) Policies 29
Enable Mobile Device Management (MDM) 29
Configure Office 365 Advanced Threat Protection (ATP) 29
Zero Trust Architecture 29
Network-Based Zero Trust 30
Application-Based Zero Trust 30
Identity and Access Management 30
Password Management System 31
Multifactor Authentication 31
The Importance of MFA 32
MFA Enrollment Process 32
Endpoint Security Deployment 33
Antivirus 33
Endpoint Detection and Response (EDR) 33
Network Security 33
Firewall Protection 33
Intrusion Detection and Prevention 33
Web Filtering and Content Filtering 33
Email Security and SPAM Filtering 34
Email Encryption 34
Current Solution for Email Security and Encryption: Proofpoint (Proofpoint.com) 34
Vulnerability Management 35
Vulnerability Scanning and Patch Management 35
Patch Management Software 35
Automated Patching and Alerting 35
Ongoing Support 36
C-Level Collaboration and Consulting 36
Reporting 36

Client Policy Management 37
Existing Policy and Procedure Review 37
New Policy and Procedure Review Creation 37
Policy and Procedure Implementation 37
Policy Management 37
Policy Enforcement 37
SaaS Management 37
Review Existing SaaS Applications 38
Analyze New SaaS Applications 38
Monitor and Secure SaaS Applications 38
Security Awareness Training for End Users 38
End User Evaluations and Customized Training Plans 38
Simulated Phishing Attacks and Real-Time Feedback 38
Promoting a Culture of Security Awareness 38
Measuring Training Effectiveness 38
Complaint Policy and Procedure 39
How to Make a Complaint 39
Complaint has been Filed 39
Complaint has been Received 39
Incident Review Conducted 39

Welcome Aboard!

Welcome to WOM Technology Management Group, a leading provider of cutting-edge IT services and cybersecurity solutions for small and medium-sized businesses. We provide our clients with the best possible experience, especially during major implementations such as our cybersecurity management program.

We understand that adapting to new procedures can be a challenge, but we want to reassure you that our team is here to guide you through the process. This document is designed to provide you with a clear understanding of why these implementations are so important and how they can benefit your organization and end users.

At WOM Technology Management Group, we believe in putting people first. Our focus is on ensuring that our clients have everything they need to be productive, satisfied, and safe while using technology. We are committed to providing the highest level of service and support to our clients.

We understand that this process is challenging on many fronts, and we are here to help you every step of the way. Our team will work closely with you to minimize any downtime or issues that may arise. We encourage you to play an active role in the process by communicating openly with us, providing access to necessary systems and data, and adhering to our security policies and procedures.

Cybersecurity and risk management are crucial for the success of your business in today's environment. While the onboarding process will seem daunting at times, we believe that the benefits of implementing these programs far outweigh the costs. By doing so, you can protect your organization from the potentially devastating consequences of a data breach.

Our aim is to help your organization succeed with our advanced cybersecurity and risk management programs. We are committed to providing the highest level of service and support to our clients, and we look forward to working with you to overcome any challenges and achieve your business goals.

Derreck Ogden, CEO

Purpose of this Guide

The purpose of this guide is to provide our clients at WOM Technology Management Group with a comprehensive reference document for the most popular solutions that we implement and manage. As a living, breathing document, this guide will continue to evolve and change over time as the technology landscape shifts and we adapt to provide the best quality services and solutions to our clients.

This guide is not a contract or a commitment to continue providing any of these tools or services to our clients. The processes, services, and products described in this guide will vary greatly from client to client, and our team works closely with each client to tailor our solutions to their specific needs and circumstances.

We believe in providing our clients with exclusive offerings like Confidence as a Service™ (CaaS). CaaS is a unique approach to cybersecurity that prioritizes proactive measures and risk assessments to prevent cyber threats before they can occur. Our commitment to this approach is reflected in the solutions we implement and manage, which are designed to provide our clients with the highest levels of security and performance possible.

This guide is intended to be used as a reference for our clients to better understand the solutions we provide, and it is referenced in other documents we provide to our clients, including sales proposals, presentations, service agreements, and invoices. By providing a comprehensive reference guide, we are demonstrating our commitment to transparency and communication, which are essential to building strong, long-lasting relationships with our clients.

This guide reflects our commitment to providing our clients with the best possible service and solutions. We will continue to adapt and evolve as the technology landscape shifts, and we remain dedicated to tailoring our solutions to meet the unique needs and circumstances of each of our clients.

Solutions Agnosticism

At WOM Technology Management Group, we understand that there's no one-size-fits-all solution when it comes to providing our clients with the support and security they need. That's why we are agnostic when it comes to the tools we use to achieve our clients' goals. We don't believe in promoting specific products or vendors, but rather in selecting the best tools for the job, based on our clients' unique needs and circumstances.

Our team frequently changes tools and completes behind-the-scenes migrations to improve performance for our clients. As new threats arise that need to be defended against, or when new opportunities arise to make our clients' networks and systems more secure or more effective, we add new tools to our arsenal. Our aim is always to provide our clients with the best possible service, and that means staying on top of the latest developments and advancements in the industry.

In this guide, we mention several tools for the sake of explanation, but as new tools are selected, we do our best to update this guide with the new tools as quickly as we are able. Our commitment to being tool-agnostic means that we can provide our clients with the most effective solutions for their unique situations, regardless of the vendor or product.

Our team is always evaluating new tools and technologies to ensure that we are providing our clients with the best possible service. We understand that the technology landscape is constantly changing, and we are committed to staying ahead of the curve to provide our clients with the most secure and effective solutions. By remaining tool-agnostic, we can adapt to changes in the industry and provide our clients with the best possible service.

Cyber Security Risk Assessment

Cybersecurity is a critical component of any organization's infrastructure, and it is essential to ensure that your network is secure against the ever-evolving threat landscape. A Cybersecurity Risk Assessment (CSRA) is an essential tool that organizations can use to identify potential security risks and vulnerabilities within their IT network. At WOM Technology Management Group, we work with our clients' leadership teams and end-users to deploy lightweight tools on endpoints, networks, and provide scanning for websites and domains, as well as research the dark web to identify potential threats.

Our team of cybersecurity experts uses a comprehensive and proven approach to the Cybersecurity Risk Assessment Process to help identify and mitigate potential risks to your IT infrastructure. We understand that each organization's needs are unique, and our process is tailored to your specific requirements.

Phase I: Kick-Off

The Kick-Off Phase is the beginning of the Cybersecurity Risk Assessment Process. During this phase, WOM and your organization will meet to discuss and gain a comprehensive understanding of your IT Network. WOM will ask a series of discovery questions to familiarize ourselves with your system's hardware, software, equipment, network, IT system, configuration, infrastructure, products, and processes. The consultation helps to ensure that WOM can tailor our assessment to your specific needs and ensure we do not miss any crucial details. Following the consultation, WOM will install remote access software that allows us to access and scan your network for malware and vulnerabilities.

Discovery Consultation ("Kick-Off Call")

An in-person or Zoom consultation attended by You and one of Our representatives in which we ask a series of discovery questions to familiarize ourselves with Your hardware, software, equipment, network, IT system, configuration, infrastructure, products, and processes constituting Your IT environment (Your “IT Network”). Discovery consults are typically 60-90 minutes in length.

Remote Access Tool Deployment:

Following the Discovery Consultation, we will install our lightweight remote access and scanning agents which allow our team to access and scan your network for malware and vulnerabilities. Our deployment process is designed to be quick and easy, providing minimal disruption to end-users. End-users will receive instructions on how to download and install the agent, which typically takes only 1-2 minutes to complete. In the unlikely event of any issues, our support team is always available to assist. These tools may be deployed in several ways depending on the client’s agreement:

End User Deployment – Our deployment process is designed to be quick and easy, providing minimal disruption to end-users. End-users will receive instructions on how to download and install the agent, which typically takes only 1-2 minutes to complete. In the unlikely event of any issues, our support team is always available to assist.

Full-Service Deployment – For clients who opt for full-service deployment, our team will go onsite to each client location to complete the software deployment. Our technicians will spend a few minutes at each workstation deploying the tools for the end-users, ensuring a seamless and efficient installation.

Internal IT Deployment – For clients who have internal IT personnel, we can provide our software for them to deploy using their own management software, network deployments, or in-person installations. Our team will work closely with internal resources to design the most efficient deployment for the specific environment.

Phase II: Assessment

The Assessment Phase is the core of the Cybersecurity Risk Assessment Process, where WOM Technology Management Group uses a comprehensive and proven approach to identify potential security risks and vulnerabilities within your IT infrastructure. During this phase, we use trusted scanning engines to perform a vulnerability scan of your servers, cloud systems, websites, and endpoint devices to identify cybersecurity weaknesses in your digital infrastructure. We also perform a dark web scan to identify any stolen data, usernames and passwords, Social Security numbers, and credit card numbers associated with your organization that are sold on the dark web. In addition, we run a phishing test to identify potential security weaknesses and evaluate your hardware and infrastructure to identify vulnerabilities and bottlenecks.

Our team of cybersecurity experts will analyze the results of the assessments and provide you with detailed reports outlining our findings and recommendations for improving your organization's cybersecurity posture. We understand that each organization's needs are unique, and our process is tailored to your specific requirements.

In this section, we will provide a detailed description of each step in the Assessment Phase of the Cybersecurity Risk Assessment Process, including the tools and techniques that we use, as well as the benefits of each step. We will also provide insights into how these assessments can help you to identify potential security risks and vulnerabilities, and how the recommendations provided by our team can help you to improve your organization's cybersecurity posture. By the end of this section, you will have a thorough understanding of the Assessment Phase and the importance of this phase in the Cybersecurity Risk Assessment Process.

Scan for Personally Identifiable Information (PII)

PII refers to any data that can be used to identify an individual. Examples include your addresses, email, phone numbers, IP addresses, banking credentials, login IDs, account details, and more. Our scans determine where personal and sensitive data is located and what it contains so that we can make recommendations as to how you can ensure compliance and avoid breaches or loss.

Scan for Exposure to Known Vulnerabilities

We use trusted scanning engines to perform a vulnerability scan of your servers, cloud systems, websites, and endpoint devices to identify cybersecurity weaknesses in your digital infrastructure and make recommendations as to what steps You may take to avoid costly data breaches.

Scan Equipment and Compare with CIS Standards for Security

CIS benchmarks are a set of best-practice cybersecurity standards for a range of IT systems and products developed by cybersecurity experts and industry research institutes. Our review analyzes whether Your IT Network is in line with the recommended baseline configurations to ensure compliance with industry-agreed cybersecurity standards.

Simulated Phishing Test

In this test, we create simulated phishing emails and/or webpages to be sent to You without advance notice, to determine Your security weaknesses. These simulated attacks are designed to help You understand the different forms a phishing attack can take and its identifying features, and to help You avoid clicking malicious links or leaking sensitive data in malicious forms. An overview of the test results with suggestions for improvement will be provided in the Risk Assessment Report.

Dark Web Scan

Our dark web scan checks the dark web for your information among lists of stolen data, such as usernames and passwords, Social Security numbers, and credit card numbers. This data is usually stolen during data breaches and is bought and sold on the dark web. If we discover your data on one of these sites, our report will advise you of the necessary next steps to protect your organization and data in the future.

Run Software as a Service (SaaS) Scan

This scan allows us to scan Your network perimeter, identify potential threats relating to SaaS solutions currently in use, and provides a report of possible security risks.

Evaluate Equipment and Infrastructure

We take a detailed look at your hardware and infrastructure to identify vulnerabilities and bottlenecks such as outdated hardware and equipment, connectivity and integration problems, and other issues that prevent Your IT Network from running at its highest uptime potential. We will make recommendations for troubleshooting network elements that cause inefficiency or may recommend a complete network overhaul if necessary.

Financial Exposure Analysis

We analyze various cyber-attack and data breach scenarios to assess their potential financial impacts. This involves evaluating direct costs like recovery expenses, and indirect costs such as reputational damage. By estimating the financial toll of these scenarios, we provide executives with data-driven insights to support decisions on Cyber Liability

Insurance coverage limits and financial planning. Our analysis helps in understanding the extent of coverage needed to mitigate financial risks associated with cyber threats, ensuring the organization's resilience and financial stability.

Cyber Liability Readiness Assessment

We review the organization's current security measures, assets, and configurations to gauge its cyber risk profile. This, coupled with our Financial Exposure Analysis—which quantifies potential losses from cyber incidents—helps in determining the business's eligibility for Cyber Liability Insurance (CLI). By identifying the types of cyber attacks posing the greatest threat, we pinpoint specific coverage needs. This comprehensive assessment aids decision-makers in understanding the coverage essential for mitigating identified risks. Armed with this information, executives can collaborate effectively with licensed professional insurance advisors to select and procure a CLI policy that best suits the organization's needs, ensuring a robust defense against cyber threats.

Compliance Baseline Assessment

We conduct a basic/baseline compliance assessment to ascertain if a client meets the necessary compliance standards, as identified by their licensed legal advisor. This process involves a straightforward "yes or no" evaluation of each technical control mandated by the regulatory requirements. Our team meticulously reviews the client's existing security controls against the specified standards, documenting compliance or highlighting areas of deficiency for each criterion. This clear, binary assessment approach provides clients with an immediate understanding of their compliance status, identifying where they align with required regulations and where improvements are necessary to meet legal and regulatory obligations.

Phase III: Review & Roadmap

The Review Phase is the final phase of the Cybersecurity Risk Assessment Process. During this phase, WOM will present the results of the assessment to your organization. The Risk Assessment Report will include an executive summary and detailed reports of the scans performed, outlining the findings of the assessment. The report will provide you with recommendations on how to manage identified risks moving forward. The review phase will help you to make informed strategic decisions based on the results of the assessment.

Present Results and Recommendations

We will provide You with a Risk Assessment Report outlining the findings of the risk assessment, including an executive summary and detailed reports of the scans performed. You can use this Risk Assessment Report to make strategic decisions on managing the identified risk moving forward. Our recommendations will include tasks and items which in Our opinion are required to bring the Environment up to the standards recommended by Us. We will also make a recommendation as to the monthly reoccurring services to maintain the environment's security and provide for quick and safe recovery in the event of a breach or issue.

Roadmap

One key item included in our Risk Assessment Report is a Roadmap for mitigating vulnerabilities and improving your organization's cybersecurity posture. Our team of cybersecurity experts will work with your organization to design a detailed plan that outlines the necessary steps to address identified vulnerabilities and improve your overall cybersecurity posture. This Roadmap is presented in a format that can be used to create an RFQ (Request for Quote) for the client to send out for bid.

We understand that each organization's needs are unique, and our team will work closely with you to design a Roadmap that is tailored to your specific requirements. The Roadmap will include a detailed breakdown of each recommendation, including the associated costs and timelines for implementation. By providing a clear and concise plan for mitigating vulnerabilities and improving your cybersecurity posture, our team can help you to make informed strategic decisions based on the results of the assessment.

Offering for Ongoing Services

In addition to providing a Roadmap, WOM Technology Management Group can also provide a bid to act on the recommended mitigations and roadmap for the client. Our team of cybersecurity experts can work with you to implement the necessary changes and ensure that your organization's cybersecurity posture is enhanced and better protected against potential security risks. With our comprehensive approach, you can be confident that your organization's cybersecurity posture will be improved, and your IT infrastructure will be better protected against potential security threats.

Ongoing Risk Management: Confidence as a Service® CyberWatch

In today's rapidly evolving digital landscape, safeguarding your organization's cyber infrastructure is not just a necessity—it's imperative for maintaining trust, ensuring operational continuity, and protecting the invaluable data that serves as the backbone of your business. Recognizing this essential need, we introduce Confidence as a Service® CyberWatch, a pioneering cybersecurity service designed to empower your organization with unparalleled security insights and proactive defense mechanisms.

CyberWatch stands at the forefront of cybersecurity innovation, offering a robust solution that transcends traditional security measures. By adeptly simulating the tactics and strategies employed by real-world attackers, CyberWatch provides your organization with a critical advantage: the ability to anticipate, identify, and mitigate potential cyber threats before they can manifest into breaches. This proactive approach is grounded in the principle that the best defense is a good offense. By understanding the methodologies of potential attackers, your organization can fortify its defenses more effectively and resiliently.

Our service is characterized by its comprehensive and recurring cybersecurity evaluations, which are essential for navigating the complexities of the digital age. These evaluations are not one-time assessments but a continuous cycle of testing, analysis, and improvement that ensures your cyber defense capabilities remain robust and adaptive to new threats. Quarterly penetration testing forms the cornerstone of CyberWatch, covering multiple attack vectors to provide a holistic view of your organization's cybersecurity posture. These tests are meticulously designed to uncover vulnerabilities in both external and internal defenses, including the potential for supply chain compromises and insider threats.

Beyond mere detection, CyberWatch is dedicated to building a culture of cyber resilience within your organization. Each evaluation is accompanied by in-depth analysis, quarterly reviews, and bespoke mitigation planning tailored to your unique business context. This not only addresses existing vulnerabilities but also empowers your leadership with the Executive Decision Support necessary to make informed, strategic decisions regarding cybersecurity investments and policies.

In essence, Confidence as a Service® CyberWatch is more than just a service—it's a commitment to your organization's future security and success. By choosing CyberWatch, you are not just implementing a cybersecurity solution; you are investing in the confidence to navigate the digital future securely and assertively. Our team of experts is dedicated to ensuring that your organization can thrive in an increasingly interconnected world, free from the constraints of cyber threats and vulnerabilities.

Implementation Process

The Confidence as a Service® CyberWatch implementation process can be conducted in two ways. The first is full-service managed implementation in which our team will deploy all agents and software. The second is the client can opt to install agents themselves through manual installation or through their IT team’s RMM solutions. For either deployment type chosen, our team will collaborate with client to make the process as smooth and swift as possible avoiding unnecessary downtime or complications for the client.

The Critical Importance of Proactive Cybersecurity Evaluations

In an era where cyber threats evolve with alarming speed and complexity, the significance of proactive cybersecurity evaluations cannot be overstated. Traditional reactive security measures—where actions are taken only after a breach occurs—are no longer sufficient to protect organizations against the sophisticated and ever-changing landscape of cyber threats. Proactive cybersecurity evaluations, such as those offered by Confidence as a Service® CyberWatch, are essential for several compelling reasons.

Anticipating Threats Before They Strike

The primary advantage of proactive evaluations is the ability to anticipate and neutralize threats before they can exploit vulnerabilities. By identifying potential security gaps and weaknesses through regular, comprehensive testing, organizations can implement corrective measures in advance, significantly reducing the risk of a successful attack. This foresight is invaluable, as it not only protects against data breaches but also safeguards an organization's reputation, customer trust, and financial stability.

Adapting to the Evolving Threat Landscape

Cyber threats are not static; they evolve constantly, leveraging new technologies and methodologies to bypass security defenses. Proactive cybersecurity evaluations keep pace with these changes, employing the latest tactics and strategies used by real-world attackers. This continuous adaptation ensures that an organization's defenses are always tested against the most current and relevant threats, providing a dynamic shield against cybercriminals.

Compliance and Regulatory Requirements

Many industries are subject to strict regulatory requirements that mandate regular cybersecurity assessments. Proactive evaluations not only ensure compliance with these regulations but also demonstrate a commitment to maintaining the highest standards of data protection and security. By exceeding the minimum compliance requirements, organizations can avoid costly penalties and reinforce their commitment to cybersecurity excellence.

Strategic Decision-Making and Resource Allocation

Proactive cybersecurity evaluations provide critical insights that inform strategic decision-making. By understanding the specific vulnerabilities and threats facing their organization, leaders can make informed decisions about where to allocate resources for maximum impact. This strategic approach to cybersecurity investment not only enhances an organization's defensive posture but also optimizes spending, ensuring that every dollar contributes to strengthening security measures.

Building a Culture of Cyber Resilience

Finally, proactive evaluations contribute to building a culture of cyber resilience within an organization. By regularly assessing and improving cybersecurity practices, organizations can instill a mindset of continuous vigilance and improvement among their employees. This cultural shift not only improves security but also empowers employees to take an active role in safeguarding their organization's digital assets.

The critical importance of proactive cybersecurity evaluations lies in their ability to anticipate threats, adapt to the evolving threat landscape, ensure compliance, inform strategic decision-making, and cultivate a culture of cyber resilience. Confidence as a Service® CyberWatch embodies these principles, offering organizations a comprehensive solution to navigate the complexities of cybersecurity with confidence and strategic foresight.

Objectives and Benefits of Simulating Real-World Attack Scenarios

Simulating real-world attack scenarios is a cornerstone of proactive cybersecurity strategies, providing an invaluable layer of defense against potential cyber threats. This approach, central to Confidence as a Service® CyberWatch, is designed with specific objectives in mind, each contributing to a comprehensive and resilient cybersecurity posture. The benefits of this simulation-based approach are profound, impacting every aspect of an organization's cyber defense capabilities.

Objective: Realistic Assessment of Security Posture

The primary objective of simulating real-world attack scenarios is to provide organizations with a realistic assessment of their security posture. By employing tactics, techniques, and procedures (TTPs) used by actual attackers, businesses can gain insight into how a cybercriminal might penetrate their defenses. This realistic assessment helps identify both strengths and vulnerabilities within an organization's cybersecurity framework, allowing for targeted improvements.

Benefit: Enhanced Detection and Response Capabilities

One of the key benefits of simulating real-world attacks is the enhancement of an organization’s detection and response capabilities. Through regular simulations, security teams become adept at recognizing the signs of a breach and responding swiftly and effectively. This training in a controlled environment ensures that when a real threat presents itself, the team is prepared to act with confidence, minimizing potential damage.

Objective: Testing of Incident Response Plans

A critical objective of attack simulations is to test and refine an organization's incident response plan. These simulations provide a practical, high-pressure environment to evaluate the effectiveness of response protocols, communication channels, and decision-making processes. The insights gained from these exercises are invaluable for strengthening an organization’s response to actual incidents.

Benefit: Compliance and Assurance

Simulating attacks also serves to ensure compliance with industry regulations and standards, many of which require evidence of proactive cybersecurity measures. Beyond compliance, these simulations offer assurance to stakeholders, including customers, investors, and partners, demonstrating a commitment to maintaining a secure and trustworthy digital environment.

Objective: Employee Awareness and Training

An often-overlooked objective of simulating real-world attack scenarios is the role it plays in employee training and awareness. By exposing staff to simulated phishing attacks, social engineering tactics, and other strategies used by attackers, organizations can significantly reduce the risk posed by human error. This form of practical training is crucial for building a culture of security awareness throughout the organization.

Benefit: Strategic Cybersecurity Investments

Finally, the insights gained from simulating real-world attacks enable organizations to make strategic cybersecurity investments. By identifying the most pressing vulnerabilities and threats, decision-makers can allocate resources more effectively, ensuring that investments directly contribute to enhancing security measures and protecting critical assets.

Simulating real-world attack scenarios is an essential strategy for assessing and improving an organization’s cybersecurity posture. Through realistic assessments, enhanced detection and response capabilities, rigorous testing of incident response plans, compliance assurance, employee training, and strategic investment, Confidence as a Service® CyberWatch provides organizations with the tools and insights needed to navigate the complex landscape of cyber threats with confidence and efficacy.

Service Components

Penetration Testing

Penetration testing, a pivotal component of Confidence as a Service® CyberWatch, embodies our commitment to safeguarding organizations through rigorous and comprehensive security evaluations. This section details the methodology, frequency, and strategic importance of penetration tests within the broader cybersecurity strategy.

Methodology

Penetration testing under CyberWatch employs a sophisticated approach designed to mimic the actions of an actual attacker as closely as possible. Utilizing a blend of automated tools and manual techniques, our team conducts extensive assessments across various attack vectors. The process typically begins with a seemingly benign activity—an email sent to all users within an organization, instructing them to click on a link. This simulates the common tactic employed by cybercriminals, using malicious links to infiltrate systems.

Once initiated, our proprietary penetration testing software meticulously scans the organization's systems, searching for sensitive data, uncovering network vulnerabilities, and identifying exploitable credentials in a manner akin to a hacker's approach following a successful phishing attempt. The goal is to uncover what a hacker would access or compromise, offering a window into the potential damage and identifying weak spots in the security posture.

Frequency and Customization

Recognizing that the threat landscape and organizational needs vary, CyberWatch offers flexibility in the frequency of penetration testing. While quarterly tests are standard, providing a balance between thoroughness and manageability, we accommodate preferences for more frequent assessments or one-time deep dives. The frequency can be adjusted based on regulatory requirements, insurance policy stipulations, and the client's specific risk profile, ensuring a tailored approach to cybersecurity.

This flexibility extends to the customization of penetration tests to address unique industry challenges and compliance standards. Whether adhering to GDPR, HIPAA, or other regulatory frameworks, our testing is designed to meet and exceed the specific security benchmarks required by various industries.

Attack Vectors

CyberWatch penetration testing focuses on two primary attack vectors to provide a comprehensive evaluation of an organization's defenses:

Supply Chain Attacks

This vector examines vulnerabilities that might arise from compromised software within the organization's environment, allowing attackers to gain access to computer systems. By simulating attacks that exploit third-party software weaknesses, we can assess the resilience of an organization’s supply chain security.

Insider Threats

Recognizing that threats can originate from within, this vector simulates scenarios where an employee might intentionally or unintentionally provide attackers access to the organization's systems. This aspect of testing is crucial for understanding how well an organization's internal controls and monitoring systems can detect and mitigate actions by malicious insiders.

Data Security and Analysis

A paramount concern during penetration testing is the security of the data involved. Our specialized team, dedicated solely to penetration testing and analysis, employs proprietary software to securely gather, transmit, and analyze client data. Sensitive information, such as passwords uncovered during testing, is obscured in reports to prevent leakage, ensuring that the integrity and confidentiality of client data are maintained at all times.

Outcome and Reporting

The outcome of penetration testing is a detailed report that provides in-depth analysis of detected vulnerabilities, the potential impact of these weaknesses, and prioritized recommendations for remediation. This report serves as a critical tool for executive decision-making, offering actionable insights that guide the strengthening of the organization's cybersecurity posture.

The Penetration Testing component of CyberWatch is essential for identifying vulnerabilities that could be exploited by attackers, providing organizations with the knowledge and insights needed to fortify their defenses against the evolving landscape of cyber threats.

Vulnerability Analysis

A cornerstone of Confidence as a Service® CyberWatch, Vulnerability Analysis, extends beyond the surface-level assessment of penetration testing to delve into the intricate details of an organization’s cybersecurity defenses. This rigorous examination is designed to uncover, prioritize, and recommend remediation strategies for vulnerabilities across the organization's digital landscape. Here, we outline the comprehensive approach taken in vulnerability analysis, including its key components and methodologies.

Comprehensive Testing Areas

Vulnerability Analysis under CyberWatch encompasses a wide array of critical testing areas to ensure a thorough evaluation of an organization's cyber defense capabilities:

Firewall Testing

This involves a detailed assessment of Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), and the firewall’s antivirus capabilities. The goal is to verify that these critical defensive mechanisms are configured optimally to detect and thwart potential attacks.

Active Directory Evaluation

Given its central role in managing policies and access within networked environments, Active Directory is scrutinized for user, administrator, and service account configurations, as well as for policy and setting effectiveness. This helps identify potential avenues of exploitation that could be leveraged by attackers.

M365 Security Evaluation

Microsoft 365 environments are examined for security settings, with a focus on identifying misconfigurations and non-adherence to best practices that could compromise security.

External Network Analysis

This aspect involves assessing the security of the network's external perimeter by methods such as brute-forcing DNS, examining the external addresses of devices, and analyzing open ports for vulnerabilities. This helps in understanding how accessible an organization's network is from the outside.

Endpoint and Server Security

Given that endpoints and servers are often targets for initial access or lateral movement by attackers, this analysis focuses on identifying misconfigurations that could ease such activities.

Local and Active Directory Account Configuration

The configuration of local and Active Directory accounts and policies is evaluated for weaknesses in ticket rotation, password policy enforcement, and account deactivation practices, which, if exploited, could provide attackers with extensive access to an organization's data by compromising a single account.

Methodology and Tools

The Vulnerability Analysis employs proprietary software alongside industry-standard tools, ensuring a blend of depth and breadth in the evaluation. This dual approach allows for the detection of known vulnerabilities while also uncovering new or unique weaknesses specific to the organization's infrastructure.

Data Security and Analysis

Data security remains paramount throughout the vulnerability analysis process. All collected data is handled with the highest standards of confidentiality and integrity, employing encryption and secure protocols to protect information during transmission and analysis. The findings are presented in a manner that prioritizes actionability, with sensitive details obscured to prevent unauthorized access.

Outcome and Reporting

The culmination of the Vulnerability Analysis is a comprehensive report that not only lists found vulnerabilities but also provides a prioritized roadmap for remediation. This includes linking vulnerabilities to potential business impacts, offering a clear perspective on risk prioritization. Recommendations are tailored to the organization's specific context, ensuring that remediation efforts are both effective and efficient.

Additionally, the report integrates insights into best practices and security enhancements, equipping organizations with the knowledge to not just address current vulnerabilities but to also strengthen their overall cybersecurity posture against future threats.

Vulnerability Analysis as part of CyberWatch offers an indispensable deep dive into an organization's cyber defenses, providing a critical layer of insight and foresight in the cybersecurity strategy. Through meticulous assessment and tailored recommendations, it empowers organizations to proactively address vulnerabilities, significantly enhancing their resilience against cyber threats.

Ongoing Vulnerability Management

Ongoing Vulnerability Management is a critical aspect of Confidence as a Service® CyberWatch, designed to ensure that cybersecurity defenses evolve in lockstep with the ever-changing threat landscape. This continuous process involves the identification, assessment, remediation, and monitoring of vulnerabilities to protect against potential threats. Here, we detail the proactive approach and methodologies employed in ongoing vulnerability management, highlighting its pivotal role in maintaining an organization's cyber resilience.

Automated Continuous Scanning and Remediation

At the core of Ongoing Vulnerability Management is the automated continuous scanning capability. This system tirelessly scans all operating systems—Windows, Linux, Darwin, and ARM—across the client's digital estate for vulnerabilities. The automation aspect ensures that the scanning process is both comprehensive and unobtrusive, minimizing disruption to daily operations while maximizing coverage.

The remediation process is equally sophisticated, with identified vulnerabilities being addressed promptly. Automated remediation workflows are configured for common vulnerabilities, enabling quick fixes that reduce the window of exposure. For more complex issues, detailed remediation guidance is provided, ensuring that the client's IT team can address them effectively.

Missing Patches and Updates Identification

A significant portion of cyber vulnerabilities arises from missing patches and updates. The Ongoing Vulnerability Management system is adept at identifying these gaps in both Microsoft Windows environments and third-party applications. With support for over 600 applications, this service ensures that no stone is left unturned in securing the software landscape against known vulnerabilities.

Third-Party Applications Support

Recognizing the diverse software ecosystem within modern organizations, CyberWatch extends its vulnerability management to encompass third-party applications. This broad support ensures that vulnerabilities in less common or niche applications don't become overlooked backdoors for attackers.

Automated Scheduling for Continuous Scanning

The scheduling of continuous scanning is fully automated, removing the need for manual intervention and ensuring that scans are conducted at optimal intervals. This automation supports a proactive security posture, allowing for the early detection of new vulnerabilities as they emerge.

CVE Links and EPSS Scoring

To provide context and prioritize vulnerabilities, each identified issue is linked to its corresponding Common Vulnerabilities and Exposures (CVE) entry. This link offers detailed information about the vulnerability, including its potential impact and known exploits. Additionally, vulnerabilities are scored using the Exploit Prediction Scoring System (EPSS), which assesses the likelihood of a vulnerability being exploited. This scoring aids in prioritizing remediation efforts based on the actual risk posed by each vulnerability.

Outcome and Reporting

The outcome of the Ongoing Vulnerability Management process is a dynamic, actionable report that provides a real-time view of the organization's security posture. This report includes details of identified vulnerabilities, their severity, remediation status, and recommendations for improvement. It serves as a crucial tool for both technical teams and executive decision-makers, offering insights that guide strategic cybersecurity investments and policy decisions.

Ongoing Vulnerability Management as part of CyberWatch represents a commitment to continuous improvement and adaptation in the face of evolving cyber threats. By automating the detection and remediation of vulnerabilities, providing comprehensive coverage across all systems and applications, and prioritizing vulnerabilities based on detailed risk assessments, CyberWatch ensures that organizations can maintain a strong, proactive cybersecurity posture. This process not only protects against immediate threats but also builds a foundation for long-term cyber resilience.

Consulting and Executive Decision Support

The Consulting and Executive Decision Support component of Confidence as a Service® CyberWatch transcends traditional cybersecurity services by offering strategic insights and guidance tailored to each organization's unique context. This facet of CyberWatch is designed to empower business leaders and IT teams with the knowledge and tools needed to make informed decisions about their cybersecurity posture and strategic direction. Here, we explore the comprehensive consulting services provided and the invaluable support it offers to executive decision-making processes.

Quarterly Business Review (QBR)

A cornerstone of our consulting service is the Quarterly Business Review (QBR). These sessions provide a platform for a round-table discussion between our consulting team and the client's stakeholders, including IT leaders, compliance officers, and other key decision-makers. The QBR focuses on reviewing the outcomes of the past quarter's cybersecurity efforts, analyzing the effectiveness of implemented strategies, and planning for the upcoming period.

During these reviews, we present detailed reports on the findings from penetration testing, vulnerability analysis, and ongoing vulnerability management activities. This includes a review of any incidents, the response to these incidents, and lessons learned. The aim is to ensure that stakeholders have a clear understanding of their current cybersecurity posture and are equipped with the insights needed to guide future security initiatives.

Quarterly Mitigation Planning

Integral to the consulting service is the development of a Quarterly Mitigation Plan. This plan is a comprehensive document that outlines the prioritized recommendations for addressing identified vulnerabilities and enhancing the organization's cybersecurity defenses. It is crafted in collaboration with the client's IT team, ensuring that the proposed strategies are not only effective but also feasible within the organization's operational and budgetary constraints.

The Mitigation Plan covers a range of recommendations, from immediate fixes to long-term strategic changes, all aimed at bolstering the client's cyber resilience. It also includes timelines, responsibilities, and expected outcomes, providing a clear roadmap for implementation.

Customized Consulting Services

Understanding that each organization faces unique challenges and opportunities, CyberWatch offers customized consulting services tailored to the specific needs of each client. This can range from advising on cybersecurity best practices and compliance requirements to assisting in the development of a comprehensive cybersecurity strategy that aligns with the organization’s overall business objectives.

Executive Decision Support

Beyond technical advice, CyberWatch provides Executive Decision Support, offering insights into how cybersecurity initiatives impact the broader business landscape. This includes evaluating the return on investment (ROI) of cybersecurity measures, assessing the potential business impact of cyber threats, and advising on cybersecurity governance and policy development.

Our team acts as a bridge between the technical and business aspects of cybersecurity, ensuring that executives are equipped with the knowledge to make decisions that not only protect the organization from cyber threats but also support its strategic business goals.

The Consulting and Executive Decision Support offered by Confidence as a Service® CyberWatch is essential for organizations looking to navigate the complexities of the cybersecurity landscape effectively. By combining in-depth technical analysis with strategic business insights, CyberWatch enables organizations to not just respond to cybersecurity challenges but to anticipate and strategically plan for them, ensuring long-term resilience and success in an increasingly digital world.

Benefits of CyberWatch

Confidence as a Service® CyberWatch offers a suite of comprehensive cybersecurity services designed to empower organizations with advanced protection, strategic insights, and proactive defense mechanisms. The benefits of CyberWatch extend beyond traditional security measures, providing a multi-dimensional approach to cybersecurity that addresses both immediate threats and long-term strategic goals. Here, we highlight the key advantages of integrating CyberWatch into your cybersecurity strategy.

Enhanced Cyber Defense Capabilities

CyberWatch elevates an organization's cyber defense mechanisms through continuous and comprehensive evaluations. By simulating real-world attack scenarios, conducting thorough vulnerability analyses, and managing vulnerabilities on an ongoing basis, CyberWatch ensures that defenses are always aligned with the latest threat intelligence. This proactive approach significantly reduces the risk of successful cyber attacks, ensuring that your organization remains resilient against both known and emerging threats.

Proactive Identification and Remediation of Vulnerabilities

One of the core strengths of CyberWatch is its ability to identify vulnerabilities before they can be exploited by attackers. Through automated scanning, in-depth analysis, and regular penetration testing, CyberWatch uncovers security weaknesses across the network, endpoints, and applications. The service not only detects these vulnerabilities but also prioritizes them based on their potential impact, providing clear guidance for remediation. This proactive stance on vulnerability management is crucial for maintaining a secure and robust digital environment.

Executive Decision Support

CyberWatch transcends the technical realm of cybersecurity, offering bespoke solutions and strategic insights that support executive decision-making. Through Quarterly Business Reviews and customized consulting, CyberWatch provides a clear understanding of the organization's cybersecurity posture, the effectiveness of current strategies, and recommendations for future initiatives. This executive decision support ensures that cybersecurity investments are aligned with business objectives, optimizing resource allocation and enhancing overall business resilience.

Scalability and Flexibility

Recognizing that organizations grow and evolve, CyberWatch is designed to be scalable and flexible, accommodating businesses of all sizes and industries. Whether you're a small startup or a large multinational corporation, CyberWatch can be tailored to meet your specific needs. This scalability ensures that as your organization expands, your cybersecurity measures can adapt accordingly, providing continuous protection without compromising on efficiency or effectiveness.

Building a Culture of Cyber Resilience

Beyond the immediate benefits of enhanced security and strategic insights, CyberWatch plays a pivotal role in fostering a culture of cyber resilience within organizations. By involving leadership in cybersecurity discussions, training employees on security best practices, and promoting a proactive approach to cyber defense, CyberWatch helps embed cybersecurity awareness at every level of the organization. This cultural shift is essential for creating a holistic defense strategy where every member of the organization plays a part in safeguarding against cyber threats.

The benefits of Confidence as a Service® CyberWatch are manifold, offering enhanced cyber defense capabilities, proactive vulnerability management, executive decision support, scalability, and the foundation for a resilient cybersecurity culture. By integrating CyberWatch into your cybersecurity strategy, your organization gains a powerful ally in the fight against cyber threats, ensuring not only the security of your digital assets but also the continued success and growth of your business in the digital age.

Client Responsibilities

Adopting Confidence as a Service® CyberWatch is a collaborative process that requires active participation from the client to maximize the effectiveness of the cybersecurity measures implemented. While CyberWatch provides comprehensive cybersecurity evaluations, ongoing management, and strategic consulting, the success of these initiatives also depends on the client fulfilling certain responsibilities. This ensures that the service is seamlessly integrated into the organization's existing operations and that cybersecurity efforts are aligned with the organization's strategic objectives. Below are key responsibilities clients must undertake as part of the CyberWatch service.

Providing Necessary Access and Information

For CyberWatch to conduct thorough penetration testing, vulnerability analysis, and ongoing vulnerability management effectively, clients must provide timely and secure access to their systems, networks, and relevant information. This includes granting permissions for CyberWatch tools to scan the infrastructure and access necessary data for analysis. Ensuring that CyberWatch teams have the access they need is crucial for identifying vulnerabilities accurately and developing effective mitigation strategies.

Active Participation in Quarterly Reviews and Mitigation Planning

The Quarterly Business Review (QBR) is an essential component of the CyberWatch service, offering a platform for discussing cybersecurity performance, reviewing findings, and planning future actions. Clients are expected to actively participate in these reviews, with representation from IT leadership, compliance officers, and other key stakeholders. Engaging in the QBR process ensures that the client's executive team is fully informed about their cybersecurity posture and involved in decision-making processes related to cybersecurity strategy and investments.

Incident Response Preparedness

Clients are responsible for maintaining an up-to-date incident response plan that can be swiftly enacted in the event of a detected breach or vulnerability. While CyberWatch will assist in identifying threats and providing recommendations for mitigation, the client must have the internal capabilities or partnerships in place to respond effectively to incidents. This includes having a designated team or individual responsible for managing incident response and ensuring that all employees are aware of their roles in such scenarios.

Implementing Recommended Mitigation Strategies

Upon receiving recommendations for remediation from the CyberWatch team, clients are responsible for implementing these strategies in a timely manner. While CyberWatch can provide guidance on prioritization and execution, the actual implementation of mitigation measures falls under the client's purview. This may involve updating software, revising policies, enhancing security protocols, or undertaking other corrective actions as advised.

Fostering a Culture of Security Awareness

Lastly, clients are encouraged to foster a culture of security awareness within their organization. This involves educating employees about cybersecurity best practices, promoting vigilance against phishing and other social engineering attacks, and encouraging the reporting of suspicious activities. By building a culture of security awareness, clients can significantly enhance the effectiveness of the CyberWatch service and their overall cybersecurity posture.

The partnership between clients and Confidence as a Service® CyberWatch is pivotal for achieving a robust cybersecurity defense. By fulfilling these responsibilities, clients not only enhance their protection against cyber threats but also ensure that cybersecurity efforts are strategically aligned with their organizational goals. This collaborative approach is key to building a resilient, secure digital environment capable of supporting the organization's success in an increasingly complex cyber landscape.

Feedback and Continuous Improvement

Feedback and Continuous Improvement form the bedrock of the Confidence as a Service® CyberWatch approach, ensuring that cybersecurity services not only meet the current needs of clients but also evolve in anticipation of future challenges. This dynamic process leverages client feedback, industry trends, and the latest cybersecurity research to refine and enhance the service offering continuously. Below, we delve into how CyberWatch integrates feedback mechanisms and continuous improvement practices into its cybersecurity framework.

Client Feedback

At the heart of CyberWatch's feedback process is the Quarterly Business Review (QBR), a structured forum where clients and the CyberWatch team come together to discuss service performance, achievements, and areas for improvement. These sessions are invaluable for gathering insights through direct feedback from clients on their experience with the service, including what works well and what could be enhanced, provides critical insights that shape service improvements. Discussions during QBRs ensure that CyberWatch's services remain aligned with the client's evolving business objectives and cybersecurity needs.

Continuous Improvement Practices

Leveraging the feedback collected, the CyberWatch team engages in a systematic process of continuous improvement, which encompasses:

- **Service Enhancements:** Based on client feedback and the results of service performance evaluations, CyberWatch iteratively refines its methodologies, tools, and processes to enhance service delivery. This includes adopting new technologies, adjusting testing methodologies, and tailoring consulting services to better meet client needs.
- **Training and Development:** The CyberWatch team undergoes regular training and professional development to stay at the forefront of cybersecurity advancements. This ensures that the service benefits from the latest knowledge, skills, and technologies in the field.
- **Innovation:** CyberWatch invests in research and development to innovate new solutions that address emerging cybersecurity challenges. By anticipating future trends and threats, CyberWatch ensures its clients are always one step ahead.

Collaboration with the Client Experience Team

The Client Experience Team plays a pivotal role in the continuous improvement process, acting as a bridge between clients and the CyberWatch service delivery team. They are responsible for:

- **Analyzing Feedback:** Systematically analyzing client feedback to identify trends, opportunities for improvement, and areas of excellence.
- **Action Planning:** Working with service delivery teams to develop action plans that address client feedback and enhance the overall client experience.

Outcome of Continuous Improvement

The outcome of this relentless focus on feedback and continuous improvement is a service that not only adapts to the changing cybersecurity landscape but also evolves in alignment with clients' strategic goals. Clients benefit from a service that is:

- **Responsive:** Quickly adapts to feedback and changes in the cybersecurity environment.
- **Proactive:** Anticipates and addresses future cybersecurity challenges.
- **Aligned:** Remains in sync with clients' business objectives and security needs.

Feedback and Continuous Improvement are integral to the Confidence as a Service® CyberWatch ethos, ensuring that the service remains effective, relevant, and aligned with client needs over time. Through open dialogue, a commitment to excellence, and a culture of innovation, CyberWatch continually enhances its ability to protect clients against the evolving threats of the digital age.

FAQs and Common Concerns

The integration of Confidence as a Service® CyberWatch into an organization's cybersecurity strategy often comes with questions and concerns from potential and existing clients. Addressing these queries upfront is crucial for establishing trust and ensuring a smooth partnership. Below, we tackle some of the most frequently asked questions and common concerns related to the CyberWatch service.

How does CyberWatch ensure the confidentiality and integrity of our data during penetration testing and vulnerability assessments?

CyberWatch prioritizes the security of your data above all else. Our penetration testing and vulnerability assessments are conducted using proprietary software designed with built-in safeguards to protect your information. All data collected during testing is encrypted and securely transmitted to our analysis centers. Moreover, sensitive information, such as passwords uncovered during testing, is always obscured in our reports to ensure it cannot be misused.

Can the frequency of penetration testing and vulnerability assessments be customized to fit our specific needs?

Absolutely. While we recommend quarterly penetration tests to balance thoroughness with operational feasibility, we understand that every organization has unique needs and risk profiles. CyberWatch offers the flexibility to adjust the frequency of tests based on your specific requirements, including compliance mandates, insurance policies, and your internal risk management strategy.

What differentiates CyberWatch's approach from other cybersecurity services in the market?

CyberWatch sets itself apart through its comprehensive, proactive approach to cybersecurity, combining cutting-edge technology with human expertise. Our service not only identifies and mitigates vulnerabilities but also provides strategic insights and executive decision support, ensuring cybersecurity efforts align with your business objectives. Furthermore, our use of proprietary software and third-party independent teams for penetration testing fulfills many compliance requirements for external cybersecurity evaluations.

How are vulnerabilities prioritized for remediation?

Vulnerabilities are prioritized based on a combination of factors, including their severity, the potential impact on your business, and the likelihood of exploitation. We use the Exploit Prediction Scoring System (EPSS) and link vulnerabilities to Common Vulnerabilities and Exposures (CVE) entries to provide context and prioritize remediation efforts effectively. This ensures that the most critical vulnerabilities are addressed promptly to minimize risk.

In the event of a cybersecurity incident, how does CyberWatch support our organization?

CyberWatch is not a cybersecurity measure or an incident response service. These types of events and projects are handled by a separate team under our Centurion SecOps teams. In the event of a cyber-attack or discovery of an active security event, our team will immediately respond with the cessation of any ongoing testing and promptly notify the client of the breach. The client will then engage their incident response plan as appropriate.

How does CyberWatch stay current with the latest cybersecurity threats and technologies?

Our team is committed to continuous learning and development, staying abreast of the latest cybersecurity research, threat intelligence, and technological advancements. We regularly update our methodologies, tools, and training to ensure our services reflect the current threat landscape and best practices in the industry.

Preparing You and Your Company for a Safe and Prosperous Future

Supercharged Service with Remote Monitoring and Management (RMM)

As your trusted IT service provider, WOM Technology Management Group will deploy Remote Monitoring and Management (RMM) tools to all devices in your network during the implementation phase. Our team will install and configure the RMM agent, allowing for remote monitoring and management of devices to ensure that they are running at peak performance. The process is quick and easy, and typically does not require any input or involvement from end users.

With RMM tools in place, we can set up automated monitoring and alerting to proactively identify and resolve any potential issues before they become major problems. Our team will work diligently to keep your systems running smoothly, minimizing downtime, and ensuring that your network is always up and running.

Here are some of the key benefits of having RMM tools at your fingertips:

- Early warning for performance issues
- Easy ticket creation for fast resolution from our help desk team
- Maintaining peak performance for your business systems
- Automated early warning systems for our tech team to address issues before they become problems.

Our RMM Agent is a lightweight application that does not negatively impact system performance. The installation and implementation of the RMM sometimes requires end users or internal team members to install from either a download from a website link we will provide complete with instructions or portable media such as a USB drive. The installation process is simple, straightforward, and fully supported by our help desk team and we will make sure that your team is ready prior to rollout.

System Monitoring

System monitoring is a critical component of a comprehensive cybersecurity strategy. Our team at WOM Technology Management Group will implement the following system monitoring measures to ensure the ongoing security and health of your IT environment:

Real-Time Monitoring

We will install and configure system monitoring software to enable real-time monitoring of your systems and applications. Our team will set up automated alerts and notifications to ensure that any issues are identified and addressed in a timely manner. We will also monitor system logs and metrics to detect any suspicious activity.

Regular Health Checks

We will schedule regular system health checks to ensure that your IT environment is operating at peak performance. During these health checks, our team will review system performance and identify potential issues. We will recommend and implement solutions to improve system performance and prevent downtime.

Minimal User Interaction

End user interaction is not required during the implementation of system monitoring measures. Our team will work in the background to ensure that your IT environment is running smoothly and securely.

By implementing system monitoring measures, we can help ensure that your IT environment is running smoothly and that any potential issues are identified and addressed before they can impact your business operations. Our team at

WOM Technology Management Group is committed to making this process as easy as possible for everyone involved and will work closely with you to ensure that your system monitoring measures are set up and configured to meet your specific needs.

Help Desk Services

To ensure that your business operations are running smoothly, our team will deploy help desk services to provide support for your end users. Our help desk services include the following:

Ticketing System for Issue Tracking and Resolution

We will set up a ticketing system for issue tracking and resolution, providing a centralized location for your end users to report and track issues. The fastest way to get help is to create a ticket through the help desk application found in the notifications bar of all onboarded workstations and servers. End users can also send an email to the help desk, and if these two options are unavailable, they can call the help desk hotline. Specific phone numbers and email addresses will be provided during training, along with a demonstration of how the end user can get fast support through the help desk application. With all of these methods, it is important that the end user identifies the issue they're having with as much detail as possible. The more the help desk knows about the problem, the faster it will be resolved.

Remote Support Tools for Quick Issue Resolution

We will provide remote support tools for quick issue resolution, enabling our team to quickly and efficiently resolve any issues that arise. This will help minimize downtime and ensure that your business operations can continue running smoothly.

Training for End Users

To ensure that your end users can effectively use the new systems and applications, our team will provide training sessions for your end users. We will schedule training sessions at a time that is convenient for your end users and provide training on how to use the new systems and applications. Additionally, we will provide training on cybersecurity best practices, ensuring that your end users are aware of potential security threats and know how to protect your business from cyber-attacks. End user interaction will be necessary during the training sessions to ensure that end users are engaged and fully understand how to use the new systems and applications. Our team is committed to making this process as easy as possible for your end users and will provide guidance and support throughout the training sessions.

Ticket Prioritization

Help desk tickets are prioritized based on impact and severity of the issues. Impact refers to the scope of the problem and how many people are affected by it, while severity refers to the degree of impact on the affected users or the business. Our team will use these factors to prioritize help desk tickets, ensuring that the most critical issues are addressed first. This will help ensure that your business operations are running smoothly and that any issues are resolved in a timely manner.

By deploying help desk services and providing training for your end users, we can help ensure that your business operations are running smoothly and efficiently. Our team is committed to providing top-notch support and training to ensure that your end users can effectively use the new systems and applications and are aware of cybersecurity best practices.

Protecting Your Hard-Earned Digital Assets with Cloud Backup and Restoration

At WOM Technology Management, we understand the importance of protecting your data. That's why we use the latest software to take a full disk image and store backups in the cloud. This ensures that your data is always safe, even in the event of a system failure or other disaster. Here are some of the benefits of our cloud backup solution:

- Easy restoration of entire operating systems or individual files.
- Protection against incorrectly updated, accidentally deleted or lost data.
- Reduces the risk of data loss and downtime.

During the implementation phase, our team will work to set up and secure backups to protect your data. We will configure backup schedules and retention policies to ensure that your data is always backed up and easily retrievable in case of an emergency. Our team will also test backups and restore procedures to make sure that your data can be recovered quickly and effectively in case of a disaster.

We understand that there may be some downtime during the setup and testing of backups. However, this is a necessary step to protect your business from data loss or other catastrophic events. End users and business managers play an important role in this process, and we appreciate their responsiveness and participation. Our team is committed to making this process as easy as possible for everyone involved, and we will work closely with you to ensure that your backups are set up and secure.

Rest assured that with our cloud backup solution, your data is in safe hands. If you have any questions or concerns about the backup process, please do not hesitate to reach out to our team.

Why Microsoft 365?

At WOM Technology Management, we pride ourselves on being agnostic in our approach to selecting the best tools and technologies for our clients. We believe in analyzing each client's unique needs, and then selecting the tools that will best serve those needs. With that said, we have found that Microsoft 365 is currently the leading provider in its field, and we often recommend this platform to our clients.

Microsoft 365 is more than just email and productivity tools. It includes a suite of applications and services, such as Azure, SharePoint, and Teams, which can be used to improve collaboration and productivity across an organization. By moving to Microsoft 365, organizations can take advantage of cloud-based tools that offer enhanced security, cross-platform compatibility, and productivity features.

One of the major advantages of Microsoft 365 is its security features. Microsoft 365 includes advanced security capabilities, such as identity and access management, threat protection, and information protection. The platform also provides ongoing updates and patches to protect against the latest threats and vulnerabilities and is compliant with various security standards and regulations.

Microsoft 365 is also cross-platform compatible, meaning that it can be used on a wide range of devices and operating systems. This makes it an ideal choice for organizations that have employees working from different locations and using a variety of devices. With Microsoft 365, users can access their emails, files, and applications from anywhere, on any device.

Finally, Microsoft 365 offers a range of productivity features that can help employees work more efficiently and collaboratively. Features such as co-authoring, real-time chat, and video conferencing can improve communication and collaboration between employees, regardless of their physical location. Microsoft 365 also provides tools for task management, project management, and workflow automation, which can help streamline business processes and increase productivity.

When compared to locally hosted Microsoft Exchange, Google Workspace, or other IMAP or POP email solutions, Microsoft 365 is the clear winner in terms of security, cross-platform compatibility, and user productivity. At WOM

Technology Management, we believe in recommending the best tools and technologies to our clients, and we believe that Microsoft 365 is currently the leading provider in its field.

Microsoft 365 Setup and Configuration

During the implementation phase, our team will perform the setup and configuration of Microsoft 365 services for your organization. The setup process will involve the following steps:

Not Using Microsoft 365 Already? No Problem, We'll Fix this Together!

At WOM Technology Management, we understand that the migration process can be challenging and stressful, but we have extensive experience and knowledge to make the transition as smooth as possible. There is a significant amount of preparation involved in migrating to Microsoft 365, and our team will work closely with your management teams and end-users to prepare for the migration.

It is essential that your management team and end-users are involved in the process from the start. Our team will provide clear communication and set expectations for what is required from the company during the migration process. We will work with your management teams to ensure that all necessary steps are taken to prepare for the migration, including verifying your domain and DNS settings, configuring user accounts in Microsoft 365, and migrating email data from the existing email system to Microsoft 365.

End-users will play an important role during the migration process. We will provide clear communication and instructions on what they need to do to prepare for the migration, including backing up any critical data, updating their email signature, and notifying others of the impending migration.

It is important to note that the migration process cannot be rushed. Our team works closely with engineers from Microsoft and third-party support teams to ensure that the migration process is executed correctly. This is not a process that is well-supported by an out-of-the-box process, and special circumstances and challenges arise, which manifest differently in almost every migration.

Our team will ensure that the migration process is executed with minimal impact on your business operations. Our goal is to ensure that the migration is a seamless process and that your end-users can navigate the new system with ease. We will also provide training and support to end-users, ensuring that they understand how to use the new system effectively.

We are committed to making the migration process as smooth and stress-free as possible for your business. Our team will work closely with your management teams and end-users throughout the entire onboarding process and migration to ensure that your business is up and running with minimal disruption.

Protecting Your Microsoft 365 Data with our Cloud-to-Cloud Backup Solutions

As part of our comprehensive cybersecurity plan, our team takes proactive steps to protect your data hosted in the cloud, including setting up cloud-to-cloud backups. This is a best practice recommended by Microsoft, and we make sure to cover all our clients in this area as well. This process involves configuring backup schedules and retention policies to ensure that your data is backed up frequently and kept for as long as needed.

Our team will work closely with your business managers and end users to determine the best backup schedule and retention policy that works for your business. We understand that there may be some downtime during the process, but this is necessary to allow for the proper configuration of the backup schedules and retention policies.

Once the backup solution is configured, we will test backups and restore procedures to ensure that your data can be recovered quickly and effectively in case of a disaster. This step is critical to ensure that your business can continue to operate even in the event of a data loss or other catastrophic event.

Our team will work closely with your business managers and end users to ensure that they are aware of any potential downtime during the testing of backups and restore procedures. Our goal is to minimize the impact on your business and ensure that your data is always secure and recoverable. Rest assured that our team is well-equipped with the latest tools and technology, and we work with engineers from Microsoft and third-party support teams to ensure a seamless and successful backup solution.

Implementing Best Practices for Microsoft 365 Management

After successfully migrating to Microsoft 365, it's time for us to start optimizing your experience with the platform. At WOM Technology Management, we want to ensure that your organization is getting the most out of your investment in Microsoft 365. That's why our team of experts will work behind the scenes to configure and manage your tenant, setting up the platform to meet your specific needs.

During this process, we will implement best practices for tenant management, including configuring user and group permissions, setting up role-based access control (RBAC), configuring Azure AD Connect for on-premises identity synchronization, and configuring Azure AD Identity Protection. These steps require careful planning and execution to ensure that your organization is secure and that end users have the right access to the tools they need.

We understand that end user involvement is necessary during the setup of Microsoft 365 to ensure that their accounts are properly configured and that they understand the new permissions and access controls. Our team will work closely with your business managers and end users to ensure that they are aware of any changes to their permissions and understand how to access their accounts. We will also provide training sessions to ensure that end users are familiar with the new platform and can use it effectively.

Unlike during the previous setup phases, no downtime will be necessary during the optimization phase. However, we will keep you informed of any potential changes or disruptions that may arise during the configuration process.

Cybersecurity Implementation

Now that we've prepared your company for streamlined implementations, support, and data retention, it's time to focus on the threat of bad actors in the realm of cybercrime. Cybercrime poses a significant risk to businesses and can result in costly expenses, destruction of valuable data, and harm to both businesses and individuals. Cyber threats such as identity theft can destroy people's lives, and laws and regulations hold businesses responsible for protecting the Personally Identifiable Information (PII) they collect and store.

By proactively implementing cybersecurity measures, your company has made a smart move in protecting its digital assets and the individuals whose information it is responsible for. However, it's important to understand that cybersecurity is the best effort to keep your company's digital assets safe, and no solution is 100% foolproof. That's why we work closely with your management team to ensure that proper insurance and response plans are in place in case our best efforts are overwhelmed by a targeted attack.

The statistics on the harm caused by cybercrime to businesses and individuals are alarming, with many businesses being forced to close their doors following a cyber-attack. We want to ensure that your company is not one of them. That's why we work with your company from top to bottom, from the Owner/CEO to front-line employees, to incorporate cybersecurity into your company culture and ensure that everyone is aware of the importance of maintaining a secure digital environment.

We understand the seriousness of the threat that cybercrime poses to your business, and we are here to help you protect yourself from these risks. While we strive to make your digital assets as secure as possible, we also work with you to ensure that you have proper insurance and response plans in place. With our help, your company can focus on its core business, knowing that its digital assets are protected from cyber threats.

Microsoft 365 Hardening

Our team will perform Microsoft 365 hardening to ensure that your Microsoft 365 environment is secure and protected. The hardening process involves the following steps:

Configure Secure Score and Compliance Score

We will configure Secure Score and Compliance Score in Microsoft 365. Secure Score is a tool that helps you understand your security posture and provides recommendations for improving your security. Compliance Score is a tool that helps you assess your compliance with industry standards and regulations.

End user interaction may be necessary during the configuration of Secure Score and Compliance Score. Our team will work closely with your business managers and end users to ensure that they are aware of any potential downtime and are able to plan accordingly.

Set up Data Loss Prevention (DLP) Policies

We will set up Data Loss Prevention (DLP) policies to prevent sensitive data from being leaked or shared outside your organization. Our team will work with your business managers to identify sensitive data and determine the best DLP policies to put in place.

End user interaction may be necessary during the setup of DLP policies. Our team will work closely with your business managers and end users to ensure that they are aware of any potential downtime and are able to plan accordingly.

Enable Mobile Device Management (MDM)

We will enable Mobile Device Management (MDM) to secure mobile devices that access your Microsoft 365 environment. Our team will work with your business managers to determine the best MDM policies to put in place.

End user interaction may be necessary during the setup of MDM policies. Our team will work closely with your business managers and end users to ensure that they are aware of any potential downtime and are able to plan accordingly.

Configure Office 365 Advanced Threat Protection (ATP)

We will configure Office 365 Advanced Threat Protection (ATP) to protect your Microsoft 365 environment from advanced cyber threats. ATP provides advanced protection against phishing attacks, malware, and other advanced threats.

End user interaction may be necessary during the configuration of ATP. Our team will work closely with your business managers and end users to ensure that they are aware of any potential downtime and are able to plan accordingly.

By performing Microsoft 365 hardening, we can ensure that your Microsoft 365 environment is secure and protected against advanced cyber threats. Our team is committed to making this process as easy as possible for everyone involved and will work closely with you to ensure that your Microsoft 365 environment is set up and configured to meet your specific needs.

Zero Trust Architecture

Zero Trust is a cybersecurity approach that helps protect your business from cyber-attacks by assuming that no one should be trusted until they are verified. This means that every time someone tries to access your company's network or resources, they must be verified and authorized before being granted access.

In traditional network security, once someone gains access, they are generally trusted and allowed to move freely within the network. However, Zero Trust takes a different approach by constantly verifying and monitoring users, devices, and traffic, even if they are already inside the network.

By implementing Zero Trust, your business is better protected against cyber-attacks, including insider threats and attacks that originate from outside the company's network. It also helps to ensure that only authorized users have access to sensitive information, and that all access is closely monitored and controlled.

Our team will implement a zero-trust architecture to provide the highest level of security for your network and applications. The zero-trust architecture involves the following steps:

Network-Based Zero Trust

As part of our comprehensive cybersecurity plan, our team will set up a network-based zero trust model to protect your network resources and assets. This involves the following steps: identifying network resources and assets, segmenting the network using firewalls and VLANs, and implementing access control policies. This will prevent unauthorized access to network resources and reduce the risk of cyber-attacks.

While end user interaction during the setup of network-based zero trust is unlikely, users may notice warnings when browsing the internet during their workday. If a website needs to be added to a whitelist for access, or if it is not a properly secured website, our team may need to provide workarounds or alternatives. Our team will work closely with your business managers and end users to ensure that they are aware of any potential website access issues and are able to request necessary access or workarounds.

It is important to note that while network-based zero trust is a strong security measure, no solution is 100% foolproof. That's why our team works with your management team to ensure that proper insurance and response plans are in place in case our best efforts are overwhelmed by a targeted attack.

Application-Based Zero Trust

As part of our comprehensive cybersecurity plan, our team will implement application-based zero trust to ensure the security of your applications and data stores. This involves identifying and controlling access to your applications and data stores, using multi-factor authentication to protect access to sensitive applications, and implementing access control policies based on application roles and responsibilities.

During the implementation of application-based zero trust, end user interaction may be required in certain situations. For example, if an end user needs to install or run software that is not yet added to the whitelist, they may need to request permission from our technical team. Additionally, if a software application is not properly secured, our team may need to provide workarounds or alternatives to ensure the security of your data while maintaining your business workflows.

Our team is committed to working closely with your business managers and end users to ensure that they are aware of any potential downtime and can plan accordingly. Our goal is to minimize the impact on your business while ensuring the security of your applications and data stores.

Identity and Access Management

Identity and access management (IAM) is a critical component of any solid cybersecurity plan for any business. In simple terms, IAM is the process of identifying, authenticating, and authorizing individuals or devices to access specific resources on a network.

IAM is important because it ensures that each user on the network is identified and authenticated correctly. Without proper IAM, a network is vulnerable to impersonation and other types of cyberattacks. By properly identifying and authenticating users, a business can ensure that the right people have access to the right resources and data, while also protecting against unauthorized access.

One of the key components of IAM is ensuring that user credentials are secure. This involves using strong passwords or passphrases, implementing multi-factor authentication, and ensuring that passwords are changed on a regular basis. Additionally, it is important to ensure that users only have access to the resources required to do their jobs, and nothing more.

Proper IAM also helps protect against internal threats, such as when a disgruntled employee tries to access sensitive data after they have been terminated or when a user accidentally clicks on a malicious link. By properly identifying and authorizing users, a business can minimize the risk of these types of incidents.

In short, IAM is crucial for any business that wants to protect their digital assets and data. It ensures that each user on the network is properly identified and authenticated, and that they only have access to the resources they need. By implementing proper IAM, a business can minimize the risk of cyberattacks and data breaches.

WOM Technology Management will set up a password management system, implement multifactor authentication (MFA) for all applications possible and other tools to ensure proper access is available to the proper members of your team. This will ensure that only authorized users can access your applications and data stores.

Password Management System

At WOM Technology Management, we take password security seriously. As part of our comprehensive cybersecurity plan, we use a cloud-based password vault to securely store and manage passwords. This helps prevent data breaches and unauthorized access to sensitive information.

The implementation process of the password vault involves our team configuring the vault for each user and training end users on how to use the software. Our team will also work with end users to help move saved passwords from unsecured locations such as spreadsheets, sticky notes, and browser password managers to the new password vault. Additionally, we will work with end users to ensure that their passwords are strong, unique, and not easily guessed.

Once end users are trained on how to use the password vault, they will be able to access their passwords faster and more securely. This will help them be more productive and focus on their work without the worry of remembering multiple complex passwords.

The task of directly managing credentials unavoidably falls on the end user. For security reasons, our technical team will not be able to directly assist with password management with individual credentials, but we’re happy to assist on training with end users so they are able to successfully utilize this tool to increase both security posture and efficiency. If an end user needs help using the password management system, they are encouraged to reach out to the onboarding team for further training.

This system includes features that allow us to monitor for compromised passwords, alert end users if their passwords are found on the dark web, and automatically change compromised passwords. This helps ensure that your business and your end users are protected from potential security threats.

Our use of a password vault is just one way that we work to keep our clients' digital assets secure. We take pride in our commitment to cybersecurity and will continue to work with our clients to ensure that their business and data are protected.

Multifactor Authentication

At WOM Technology Management Group, security is our top priority. That's why we require multi-factor authentication (MFA) for all MFA-enabled applications. MFA provides an additional layer of protection by requiring you to verify your identity using a second factor, usually your registered phone, when accessing sensitive applications and systems. In this section, we'll guide you through the MFA enrollment process, explain the importance of MFA, and provide information on what to expect during and after enrollment.

The Importance of MFA

MFA is essential for protecting your online accounts from unauthorized access. Passwords alone are no longer enough to prevent cyberattacks, which is why adding an extra layer of security with MFA is crucial. By requiring a second factor, such as a registered phone, to access your accounts, you significantly reduce the risk of unauthorized access, even if someone has obtained your password.

MFA Enrollment Process

1. *Introduction to MFA (Typically 30 days before enrollment)*

We'll introduce you to the concept of MFA and the benefits it provides. You'll learn how MFA works and why it's important for protecting your online accounts.

2. *First Notice (Typically 15 days before enrollment)*

We'll remind you that MFA enrollment is coming soon and provide an overview of the enrollment process and timeline. You'll receive an email with instructions on how to enroll in MFA.

3. *Second Notice (Typically 3 days before enrollment)*

We'll remind you of the upcoming enrollment and emphasize the importance of MFA for enhanced security. Our helpdesk will be available for guidance and support during the enrollment process.

4. *Enrollment Day*

We'll provide you with instructions on how to enroll in MFA. The self-enrollment process should only take approximately 2 minutes to complete. During this process, you will need to register your phone and set up MFA for each MFA-enabled application.

5. *Application MFA Setup and Support*

We'll guide you through setting up MFA for each MFA-enabled application individually. Our team will provide general guidance on setting up MFA for the most popular applications, and our helpdesk will be available to assist you with any questions or issues that may arise during the process.

6. *User Involvement and Disturbances*

Throughout the enrollment process, you'll receive email notifications to remind you of the upcoming enrollment, but no action is required during the early stages. On the day of enrollment, you'll need to spend approximately 2 minutes to complete the self-enrollment process, register your phone, and set up MFA for each MFA-enabled application. Once enrolled, you'll need to use MFA to access MFA-enabled applications.

7. *Initial Complications*

Adopting an MFA app can initially complicate processes, but this is a temporary inconvenience that will smooth out as users adapt and adopt. Our team will provide training and support to help your team navigate the new mechanism and routines. Ultimately, the added security benefits of MFA far outweigh any temporary inconvenience.

MFA is an essential component of protecting your online accounts from cyberattacks. Enrolling in MFA is an involved process that requires involvement from all levels of your team, but our team is here to provide guidance and support. Adopting an MFA app may complicate processes initially, but this is a temporary inconvenience that will smooth out as users adapt and adopt. Our team will provide training and support to help your team navigate the new mechanism and routines. The added security benefits of MFA far outweigh any temporary inconvenience, and we're committed to ensuring that you have a secure experience with our MFA solution.

Endpoint Security Deployment

Endpoint security is a crucial aspect of any comprehensive cybersecurity strategy. Our team will work to implement the following endpoint security measures to protect your endpoints:

Antivirus

We will install and configure antivirus software on all endpoints, set up automated scanning and alerting, and implement endpoint security policies. This will safeguard your endpoints from known malware and thwart cyber-attacks from compromising your endpoints.

While there will be little to no end user interaction during the implementation of antivirus software, users may see notifications or warnings from the software as it operates in the background of their workstation or server.

Endpoint Detection and Response (EDR)

We will install and configure EDR software on all endpoints, set up automated scanning and alerting, and implement endpoint security policies. This will detect and respond to advanced threats that may bypass traditional antivirus software and prevent cyber-attacks from compromising your endpoints.

As with the implementation of antivirus software, there will be little to no end user interaction during the implementation of EDR software, but end users may see warnings or alerts from the software as it operates in the background.

By implementing endpoint security measures, we can ensure that your endpoints are protected against cyber threats and provide you with a secure and reliable environment for your business operations. Our team is committed to making this process as easy as possible for everyone involved, and we will work closely with you to ensure that your endpoint security measures are set up and configured to meet your specific needs.

Network Security

Network security is a critical component of a comprehensive cybersecurity strategy. Our team will implement the following network security measures to protect your network:

Firewall Protection

We will install and configure firewalls to protect the network perimeter and implement firewall policies to control traffic in and out of the network. This will prevent unauthorized access and protect your network from cyber-attacks.

While end user interaction is not usually necessary during the implementation of firewalls, users may see new warnings or notifications from the protective application. Our team will provide clear guidance on what these warnings mean and how to respond to them.

Intrusion Detection and Prevention

We will install and configure intrusion detection and prevention systems (IDPS) and set up automated monitoring and alerting. This will detect and prevent cyber-attacks and protect your network from advanced threats.

While end user interaction is not usually necessary during the implementation of IDPS, users may see new warnings or notifications from the protective application. Our team will provide clear guidance on what these warnings mean and how to respond to them.

Web Filtering and Content Filtering

We will install and configure web filtering and content filtering software and implement policies to control access to websites and online content. This will protect your network from malware and prevent your employees from accessing malicious or inappropriate content.

While end user interaction is not usually necessary during the implementation of web filtering and content filtering software, users may see new warnings or notifications from the protective application. Our team will provide clear guidance on what these warnings mean and how to respond to them.

By implementing network security measures, we can ensure that your network is protected against cyber threats and provide you with a secure and reliable environment for your business operations. Our team is committed to making this process as easy as possible for everyone involved and will work closely with you to ensure that your network security measures are set up and configured to meet your specific needs.

Email Security and SPAM Filtering

Business Email Compromise (BEC) is one of the most significant cybersecurity threats to any organization. According to the FBI, BEC resulted in over $1.7 billion in losses to businesses in 2019. Cybercriminals use social engineering tactics to target end-users and trick them into providing access to sensitive company information or allowing them to impersonate company executives.

At WOM Technology Management Group, we understand the importance of email security in protecting your business against BEC and other email-borne threats. We will implement email security and spam filtering software, set up automated monitoring and alerting, and implement email security policies to safeguard your email from spam, phishing, and other email-based attacks.

During the implementation of email security and spam filtering software, end-user interaction may be necessary. Our team will work closely with your business managers and end-users to ensure they understand the importance of email security and how they can contribute to protecting your company's sensitive information.

By implementing email security measures, we can ensure that your email is protected against cyber threats and provide you with a secure and reliable environment for your business operations. Our team at WOM Technology Management Group is committed to making this process as easy as possible for everyone involved and will work closely with you to ensure that your email security measures are set up and configured to meet your specific needs.

Email Encryption

Email encryption is an important security measure that can protect sensitive information sent via email. Our team at WOM Technology Management Group will evaluate the need for email encryption based on your business requirements and compliance obligations. This will help us determine which email communication channels require encryption.

We will then choose an email encryption solution that meets your specific needs and budget. This solution may be cloud-based or on-premises, depending on your requirements. Our team will also implement email encryption policies that specify which types of email communications require encryption and how encryption will be enforced.

End user interaction will be necessary during the implementation of email encryption. Our team at WOM Technology Management Group will work closely with your business managers and end users to ensure that they understand the importance of email encryption and are able to use the email encryption solution effectively. We will also train your employees on email encryption best practices and how to use the email encryption solution effectively.

By implementing email encryption measures, we can ensure that your sensitive information is protected against cyber threats and that your business is following relevant regulations. Our team at WOM Technology Management Group is committed to making this process as easy as possible for everyone involved and will work closely with you to ensure that your email encryption measures are set up and configured to meet your specific needs.

Current Solution for Email Security and Encryption: Proofpoint (Proofpoint.com)

At WOM Technology Management Group, we understand the importance of email security and encryption in today's world. That's why we have chosen to use Proofpoint for our email security needs. Proofpoint is a top-rated email security provider that analyzes over 5 billion emails daily, making it one of the most experienced solutions on the

market. By deploying Proofpoint email security to our Microsoft 365 tenant, we're ensuring that our clients' emails remain safe and secure.

One of the main benefits of Proofpoint is that it significantly reduces the amount of spam that our clients receive in their inboxes. Additionally, the system quarantines any suspicious emails that could be harmful, providing our clients with a quarantine digest to review. Clients are given full control over what to do with quarantined emails, including previewing them, releasing them to their inbox, releasing and approving the sender, or blocking the sender altogether.

Proofpoint also provides end-user training, including videos tailored to our Microsoft 365 environment, to help clients understand and utilize its features effectively. The training includes an introduction to Proofpoint, a guide on how to use Proofpoint Digest, and how to send sensitive information via encrypted email using Proofpoint. By educating clients on how to use these features, we're ensuring that they're able to protect their sensitive data effectively.

In addition to providing email security, Proofpoint also offers email encryption capabilities. Email encryption ensures that only intended recipients of emails containing sensitive information can view them. This feature should be used whenever any sensitive or financial information is being emailed to a third-party recipient. Our cybersecurity team has created a video for our clients on how to open encrypted emails sent via Proofpoint, which they can share with any third-party recipients to ensure a smooth and secure experience.

Finally, if clients experience any issues opening an encrypted email from us, our cybersecurity team is readily available to provide troubleshooting support via email. They can reach out to us at Cybersecurity@wompcav.com, including "<WOM CLIENT NAME> Encrypted Email Recipient Issue" in the subject line. By doing so, we can quickly confirm their identity with your team and provide the necessary support.

Prior to rolling out your Proofpoint solution, your organization’s Primary IT Contact with WOM will receive an email informing them of the project timeline, expected operational effects and more. Our team will use a standardized format similar to the following:

Vulnerability Management

Vulnerability management is an essential aspect of a comprehensive cybersecurity strategy, and at WOM Technology Management Group, we take it seriously. Our team will work diligently in the background to ensure that your IT environment is secure and protected against cyber threats. We will implement the following vulnerability management measures:

Vulnerability Scanning and Patch Management

Regular vulnerability scans will be conducted on all endpoints and servers to identify any vulnerabilities or security weaknesses in your IT environment. We will prioritize and remediate any vulnerabilities found to keep your systems safe and secure.

Patch Management Software

We will install and configure patch management software to automate the patching process, ensuring that your systems and applications are up to date with the latest security patches. This will provide an extra layer of protection against any known vulnerabilities.

Automated Patching and Alerting

Our team will set up automated patching and alerting to ensure that any critical security patches are applied promptly, and any vulnerabilities are addressed in a timely manner. This will prevent cyber threats from exploiting any known vulnerabilities and compromising your systems.

End user interaction will not be necessary during the implementation of vulnerability management measures. Our team will work diligently in the background to ensure that your IT environment is protected against cyber threats.

By implementing vulnerability management measures, we can help ensure that your IT environment is secure and protected against cyber threats. Our team is committed to making this process as easy as possible for everyone involved and will work closely with you to ensure that your vulnerability management measures are set up and configured to meet your specific needs.

Ongoing Support

Now that the initial onboarding process is complete, we will continue to provide ongoing support for you to ensure that all systems and applications are maintained, updated, and optimized for the best performance possible.

To achieve this, we will set up regular maintenance and update schedules for all systems and applications. We will monitor system logs and metrics to identify any potential issues before they become major problems. Additionally, we will provide troubleshooting and issue resolution services to address any problems that arise, and respond to support requests in a timely manner.

We believe that communication is key to maintaining a successful long-term relationship with you. Therefore, we will schedule regular meetings with management to review system performance and discuss potential improvements. During these meetings, we will provide recommendations for improving system performance and security. Our goal is to work closely with you to ensure that your systems and applications are always operating at peak performance and to make any necessary adjustments to keep them that way.

C-Level Collaboration and Consulting

At WOM Technology Management Group, we work with our clients on the same level as a CTO, CIO, or CISSO. We bring a wealth of knowledge and experience to the table, and we're committed to providing the highest level of expertise and availability to our clients.

Our team of experts includes a range of IT professionals with deep expertise in cybersecurity, compliance, policy development, and other key areas. In addition to our in-house team, we have access to a range of third-party resources, which allows us to draw on additional expertise as needed to meet the specific needs of our clients.

Working with WOM Technology Management Group means that you have access to a dedicated team of professionals who are committed to your success. We take the time to understand your business and your specific needs, and we work closely with you to develop customized solutions that are tailored to your unique requirements.

Our approach is collaborative, and we view our clients as partners in the effort to achieve their goals. We provide regular updates and reporting, and we're always available to answer questions or provide guidance. Our goal is to ensure that our clients have the information and support they need to make informed decisions about their IT infrastructure and cybersecurity.

We work with our clients on the same level as a CTO, CIO, or CISSO, providing a high level of expertise and availability. Our team of experts, along with access to third-party resources, allows us to provide customized solutions that are tailored to the unique needs of our clients. We are committed to working collaboratively with our clients to ensure their success and provide ongoing support and guidance as needed.

Reporting

As part of our ongoing support, we want to ensure that our clients are always informed about the performance and security of their systems and applications. That's why we provide regular reporting to keep them up to date on the status of their technology infrastructure.

We will work closely with the client to establish a reporting schedule and format that meets their specific needs. These reports will provide valuable insights into system performance, security threats, and other relevant metrics. We will review these reports with management on a regular basis and take the time to discuss any potential improvements that can be made to enhance the client's technology infrastructure.

Our reporting process is designed to give our clients the information they need to make informed decisions about their technology infrastructure. By providing regular reports and working with the client to review and analyze the data, we can identify potential issues before they become major problems and make the necessary adjustments to keep their systems and applications operating at peak performance.

Client Policy Management

At WOM Technology Management Group, we understand that policies and procedures play a critical role in keeping your company safe from cyber threats. Our policy review and creation process is designed to help identify gaps and areas for improvement, develop new policies and procedures, and implement them in a way that is accessible and easy to understand.

Existing Policy and Procedure Review

To begin, we will conduct a thorough review of your current cybersecurity policies and procedures to identify any gaps or areas for improvement. We will assess their effectiveness in protecting your company from cyber threats and determine if they are following any applicable regulations.

New Policy and Procedure Review Creation

Based on the review, we will work with you to identify areas where new policies and procedures are needed. We will develop new policies and procedures to fill those gaps and ensure that they are tailored to meet your specific business needs.

Policy and Procedure Implementation

Once the new policies and procedures are developed, we will communicate them to all employees and provide training to ensure everyone understands the new policies. We will also monitor compliance with policies and procedures and update them as needed based on changing threats and risks. In addition, we will work with your team to ensure that policies and procedures are followed consistently across your organization.

Policy Management

Our policy management services include ongoing policy monitoring, updating, and enforcement. We will regularly review policies and procedures to ensure that they remain relevant and effective in protecting your business. This includes conducting periodic risk assessments to identify new threats and risks to your business and updating policies accordingly.

Policy Enforcement

Enforcement of policies is critical in maintaining a strong cybersecurity posture. We will work with you to establish a clear policy enforcement process and ensure that policies are enforced consistently across your organization. Our team will regularly monitor compliance with policies and procedures and provide guidance and training to ensure that policies are understood and followed by all employees.

By working together, we can create a culture of cybersecurity that is a part of your company's DNA. Our goal is to create a set of policies and procedures that not only protect your company from cyber threats but are also easy to understand and follow. With our policy review and creation process, ongoing policy management, and policy enforcement services, we can help ensure that your business is protected from cyber threats and follows any applicable regulations.

SaaS Management

Software as a Service (SaaS) has become increasingly popular as companies move their applications and data to the cloud. SaaS applications can provide many benefits, including cost savings, scalability, and flexibility. However, they can also introduce security risks that need to be carefully managed. Our team at WOM Technology Management Group provides comprehensive SaaS analysis and security services to help our clients manage their SaaS applications securely.

Review Existing SaaS Applications

To effectively manage SaaS security risks, it's important to understand what SaaS applications are being used by the client. We will begin by reviewing existing SaaS applications and services used by the client. This will include evaluating the security and privacy controls of each SaaS application and providing recommendations for risk mitigation or SaaS application alternatives.

Analyze New SaaS Applications

As new SaaS applications are identified or proposed, we will conduct a thorough security analysis to evaluate the security and privacy controls of each new application prior to implementation. This will include conducting a vendor risk assessment to ensure that the new application meets the client's security requirements. Based on our analysis, we will provide recommendations for risk mitigation or SaaS application alternatives.

Monitor and Secure SaaS Applications

Once SaaS applications have been identified and analyzed, our team will implement access control policies for each SaaS application, configure Single Sign-On (SSO), implement Data Loss Prevention (DLP) policies, and set up automated monitoring and alerting for each SaaS application. We will also regularly review the security and privacy controls of each SaaS application to ensure that they continue to meet the client's requirements.

Managing SaaS security risks is essential for any organization that uses SaaS applications. Our team at WOM Technology Management Group provides comprehensive SaaS analysis and security services to help our clients manage their SaaS applications securely. By reviewing existing SaaS applications, analyzing new SaaS applications, and monitoring and securing SaaS applications, we can help ensure that our clients' SaaS applications are used securely and that their data remains protected.

Security Awareness Training for End Users

At WOM Technology Management Group, we believe that ongoing security awareness training is a critical component of any effective cybersecurity program. In this section, we will discuss the importance of training for both management and end users.

End User Evaluations and Customized Training Plans

To ensure that training is effective and engaging, we begin with end user evaluations. This helps us assess the current level of security awareness among employees, identify knowledge gaps or weaknesses, and develop a customized training plan to address these issues. We use a variety of instructional materials, including emails and videos, to provide interactive and engaging training on topics such as identifying and responding to phishing attacks, creating and managing strong passwords, and using IT systems securely.

Simulated Phishing Attacks and Real-Time Feedback

We also use simulated phishing attacks to test employees' response to potential threats and provide real-time feedback on their performance. This approach helps employees understand the risks and consequences of failing for a phishing attack and reinforces the importance of staying vigilant.

Promoting a Culture of Security Awareness

In addition to the training itself, we work with our clients to promote a culture of security awareness within their organization. This involves regular communication and reminders about security best practices, as well as incentives or recognition for employees who demonstrate a strong commitment to security. This approach helps ensure that security awareness becomes a part of the organization's DNA.

Measuring Training Effectiveness

Finally, we regularly measure the effectiveness of our training program through assessments and surveys to ensure that it is having the desired impact. Based on the results of these assessments, we refine and improve the training program as needed.

WOM Technology Management's comprehensive approach to security awareness training is designed to equip employees with the knowledge and skills they need to help protect the organization from cyber threats. To ensure maximum effectiveness, it is important for both management and end users to place strong emphasis on participation in all training sessions and to prioritize a culture of security awareness.

Complaint Policy and Procedure

Our commitment to you is to always treat you with courtesy, respect, and fairness. As we strive to provide you with the best service possible, we kindly ask that you extend the same courtesy, respect, and fairness to our staff who are handling your complaint.

How to Make a Complaint

By Email: CustomerExperience@wompcav.com

Complaint has been Filed

When customers file a complaint with WOM Technology Management Group, it is essential to provide as much detail as possible, including the date of occurrence and the employees involved on both sides of the issue. This information is crucial for the company to investigate and resolve the complaint effectively.

Complaint has been Received

Once the complaint has been received, management will review it and conduct an incident review. This review process involves gathering all the necessary information and facts related to the complaint, including any relevant documentation or evidence. We will then assess the situation and determine the appropriate resolution.

Incident Review Conducted

After the incident review, the customer will be contacted by management to discuss the resolution. The resolution could range depending on the severity of the issue. Our priority is to find a satisfactory resolution that meets the customer's needs and expectations while also adhering to WOM's policies and procedures.

We also ensure that all complaints and their resolutions are filed in the customer's account records. This serves as a reference point for future interactions with us and helps to avoid any misunderstandings or confusion in the future. It also helps to track any recurring issues or trends that the company needs to address to improve their services continually.

Our process for handling complaints involves a thorough incident review, communication with the customer, and satisfactory resolution. By keeping track of all complaints and resolutions, we can identify areas for improvement and ensure that we provide the best possible service to our customers.

WOM Technology Management Group strives to ensure that our service complaints policy is user-friendly and accessible to all. If you require any reasonable adjustments to access this policy, we will take the necessary steps to accommodate your needs. If you prefer to receive our responses in alternative formats, we will be happy to accommodate you.

We want to ensure a safe and comfortable environment for our staff and customers; therefore, we have a zero-tolerance policy for any threatening, abusive, or unreasonable behavior by a complainant or staff member.