OVERWATCH E-MAIL SECURITY SERVICE DESCRIPTION

1. OVERVIEW

Overwatch Managed Email and Collaboration Suite Security is an end-to-end cloud-based security solution designed to not only protect your email communication but also your collaboration tools from various cyber threats. With our tool's advanced security features, this service goes beyond traditional email security, extending protection to all collaboration platforms including Microsoft Teams, Slack, and more from data leak and malware, all monitored and managed by a 100% US-Based 24x7 Security Operations Center.

2. SERVICE DEPLOYMENT

Overwatch Managed E-mail Security Service deployment includes:

2.1 E-MAIL SUITE & COLLABORATION SUITE DEPLOYMENT ANALYSIS

The deployment process begins with a thorough analysis of your existing email service and email security infrastructure. Our team of cybersecurity experts assesses your current systems, the type of data you handle, and the threats you face. This step is crucial in understanding the specific security needs of your organization and creating a tailored Email security strategy.

2.2 SERVICE DELIVERY

A dedicated project manager with a team of layered service delivery engineers and subject matter experts will be assigned to your account to ensure the proper deployment of services into the end environment. This team will assess how the solution is to be deployed to achieve the outcomes set forth in the pre-sales process.

3. SERVICE MANAGEMENT

3.1 SERVICE FEATURE SET

3.1.1 COMPREHENSIVE THREAT DETECTION

The service harnesses AI-driven technology to detect a wide array of threats, including malware, phishing, data leakage, account takeovers, and advanced persistent threats across email and collaboration platforms. This service protects email in all directions (internal, external, outgoing), offering complete protection against all threats, including insider ones, constantly auto-correcting to eliminate false positives. We utilize a trusted reputation network to protect against Business Email Compromise (BEC) without increasing false positives; the service automatically learns and discovers your organization's supply chain to prevent malicious files and messages from compromised vendors from appearing in the inbox.

3.1.2 EXTENDED COLLABORATION SUITE PROTECTION

In addition to email, the service protects other communication and collaboration platforms like Microsoft Teams, Slack, Google Workspace, and more, providing robust, uniform security across your communication ecosystem.

3.1.3 API-BASED INTEGRATION

Our tool integrates within your E-mail and Collaboration suite (Microsoft 365, Google Workspace, Teams, SharePoint, OneDrive, Box, and Citrix FileShare) via API to sit at the back of the existing security stack and provide advanced in- line protection, along with the ability to claw-back email that has been delivered, but upon further inspection, or changes to threat-intel, have netted a positive detection. API-based integrations with cloud email platforms enable real-time scanning and analysis of email traffic. This approach minimizes latency and ensures efficient email processing without impacting performance.

3.1.4 DATA LEAK PREVENTION

We employ advanced data leak prevention capabilities to reduce the risk of sensitive or protected data from leaving the organization through email and unsanctioned file shares in collaboration suites. DLP helps prevent sensitive information from being accidentally or maliciously leaked through emails or collaboration suites, enhancing compliance with data protection regulations, and safeguarding intellectual property.

3.1.4 USER BEHAVIOR ANALYSIS

We leverage user behavior analysis to identify anomalous activities and phishing, which includes protection for account takeovers, and identifies unusual email behavior, which could indicate a potential breach. The service analyzes all historical emails to determine prior trust relations between sender and receiver, thereby increasing the likelihood of identifying user impersonation or fraudulent messages.

3.1.5 SOAR INTEGRATION

Customized Security Orchestration Automation and Response (SOAR) runbooks allow for dynamic automation to be implemented that exists outside the toolset presented solely by the main technology vendor. We leverage the orchestration and automation of our dedicated SOAR platform to decrease response times of common events, such as a user requesting restitution of a pulled or blocked e-mail, or to augment capabilities that the platform does not natively support, such as automatically pulling already delivered e-mails that now conform to new threat intel.

In the case of the latter, we poll the back-end every 60 seconds for new changes to existing detections. In this, you can be confident that the ever-changing landscape of e-mail and phishing security is constantly being monitored and reacted to, both with the human eyes of our SOC analysts and with the machine eyes of the SOAR platform, guided by our expertly crafted automation runbooks.

3.2 24/7/365 US-BASED MONITORING AND RESPONSE

Overwatch Managed Email Security service offers round-the-clock monitoring by our 100% US-Based SOC Analysts to ensure consistent protection of your integrated security solutions. We identify and neutralize threats before they can cause significant damage, mitigating the risk of downtime and data loss.

3.3 REAL-TIME ALERTS

With Overwatch Managed Email Security service, backed up by our 24x7 SOC and SOAR security platform, you will receive real-time alerts of varying levels for any unusual activity or threats. Real-time alerts enable immediate identification and response to potential threats, minimizing the potential damage and disruption.

This classification system allows us to prioritize threats and respond appropriately, ensuring the most critical issues are addressed immediately. It also enables you to understand the severity of each alert and take appropriate action. It enhances the visibility and control you have over your security point-solution applications, thereby reinforcing the overall security posture.

3.4 REGULAR REPORTING & REVIEW

We provide regular reports on the security status of your organization, including detailed analyses of detected threats, responses, and recommended improvements. Our service includes predefined compliance reports, baselining for statistical anomaly detection, and basic security reporting. Regular reviews are conducted to ensure the email security service evolves with your organization and continues to provide the most effective protection.

3.6 CONTINUOUS UPDATES & MAINTENANCE

Our managed Email and Collaboration Suite Security service and SOAR runbooks are continuously updated to respond to the latest threat trends and vulnerabilities, with new detection rules and SOAR response pathways added in as emerging threats become known. Regular maintenance ensures the efficiency and effectiveness of the service, minimizing your cybersecurity risks.

3.7 POST-DEPLOYMENT SUPPORT

Post-deployment, we provide ongoing support to ensure the Email and Collaboration Suite service is functioning optimally. Overwatch is available 24/7 to answer any queries or concerns you may have. We operate as your Tier 1 and 2 Tech support for all deployed services with dedicated SMEs on staff.

4. BENEFITS

The Overwatch Email Security service offers:

- **Risk Reduction:** Reduction in the likelihood of a business email compromise (BEC), propagation of malware, ransomware and data leak through email and collaboration suites.
- **Improved Compliance:** Help meet regulatory requirements with data protection of personal and protected information and compliance reporting.
- **Reduced Complexity:** Offload the complexities of managing multiple security solutions. Our managed service harmonizes all elements into a single robust protective shield.
- **Peace of mind:** With 24/7 100% US-Based monitoring, real-time alerts, and automated response, you can focus on your business knowing that your digital ecosystem is protected.