OVERWATCH SASE SERVICE DESCRIPTION

1. OVERVIEW

Overwatch Managed SASE (Secure Access Service Edge) as a service is a holistic, multi-layered, cloud-native security platform designed to safeguard your organization's network infrastructure and data. This service is fully backed by the Overwatch 24x7 US-based Security Operations Center (SOC) ensuring continuous monitoring, incident response, and protection against emerging threats. We provide comprehensive support throughout all stages of the product deployment and ongoing service lifecycles with dedicated and layered subject matter experts and our in-house service delivery, engineering, and development teams.

The cornerstone of this service is the SASE model, which converges networking and security services into a single, unified, cloud-based solution. It enables secure and fast access to the Internet, cloud-based applications, and internal applications, regardless of the user's location. With its identity-driven, policy-based approach, it delivers adaptive, risk-based access control, improving overall security posture.

2. SERVICE DEPLOYMENT

Overwatch Managed SASE service deployment includes:

2.1 NETWORK & SECURITY INFRASTRUCTURE ANALYSIS

The deployment process begins with a thorough analysis of your existing network and 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 SASE 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 deployed to achieve the outcomes set forth in the pre-sales process.

2.3 OVERWATCH MXDR INTEGRATION

Following the analysis and deployment of SASE services, our team will integrate the service with our existing security incident and event monitoring solution, given available integrations. This will allow our security operation center to keep a “machine-learned” eye on the events and alerts generated within the SASE environment. The Overwatch MXDR solution can also be leveraged to identify anomalies and potential threats across the entire attack surface, bringing together deployed endpoint detection and response (EDR), network traffic analysis (NTA), and security information and event management (SIEM) capabilities. These additional capabilities features can be added a la carte depending on the deployed environment's requirements.

2.4 SOAR INTEGRATION FOR AUTOMATED VALIDATION OF SECURITY ALERTS

A critical element of our managed SASE service is the automated validation of security alerts via SOAR. Our system rapidly processes alerts, filtering out false positives and prioritizing genuine threats. This reduces manual workload and response time, ensuring that our security team can focus on the most significant risks in your environment.

2.4.1 AUTOMATED RESPONSE PLAYBOOKS DEVELOPED BY IN-HOUSE SECDEVOPS EXPERTS

The heart of the Overwtach SOAR solution is the automated response playbooks, meticulously developed by our in-house security experts. These playbooks codify our team's knowledge and experience, defining a series of automated actions to respond to various types of threats. Each playbook is tailored to address specific threat scenarios, ensuring a rapid, effective response that minimizes the potential impact of any security event.

By deploying our SASE w/ SOAR service, you will significantly enhance your cybersecurity capabilities. The combination of automation and expert-driven playbooks ensures a swift, efficient response to threats, minimizing potential damage, and enhancing your security posture. Stay ahead of evolving cyber threats and protect your digital assets with our advanced SOAR service.

3. SERVICE MANAGEMENT

3.1 SERVICE FEATURE SET

3.1.1 CLOUD-BASED FIREWALL

Our cloud-based firewall offers advanced threat protection by controlling network traffic based on specified security policies. It provides comprehensive visibility and control over users, applications, and data to prevent unauthorized access and data breaches. The firewall can handle all types of traffic including web, applications, and emails, ensuring your network remains secure and protected at all times.

3.1.2 ZERO-TRUST NETWORK ACCESS

This service utilizes a Zero-Trust Network Access (ZTNA) approach, ensuring that every access request to the network is authenticated and authorized, regardless of the user’s location or device. It eliminates the traditional trust-based model and provides controlled access based on user identity, device health, and contextual factors, thereby significantly reducing the risk of insider threats and data breaches.

3.1.3 SECURE WEB GATEWAY (SWG)

The Secure Web Gateway feature protects your organization from web-based threats by monitoring and controlling web traffic. It enables real-time traffic inspection, URL filtering, and malware detection to prevent harmful content from entering your network. It also provides detailed traffic reports for comprehensive visibility and better decision-making.

3.1.4 IDENTITY & ACCESSMANAGEMENT

Our Identity and Access Management (IAM) feature manages digital identities, authenticates users, and authorizes access to network resources. This system ensures that only authenticated users and devices can access your resources, thus minimizing potential security risks.

3.1.5 SAAS APP CONTROL

We offer secure and controlled access to Software-as-a-Service (SaaS) applications. It provides granular visibility and control over user activities within SaaS applications, helping to prevent data leakage and protect against advanced threats. Each ingress/egress point (POP) of the cloud-connected network is provided with up to 2 static IP address (more available with additional licensure) for use with conditional access SAAS app control and brokering said connection with all policy and IAM support.

3.1.6 ANTI-PHISHING PROTECTION

Our service includes robust anti-phishing features to protect against phishing attacks. By scanning for malicious links and content, we prevent phishing attempts that could lead to data breaches or financial loss.

3.1.7 DEDICATED TENANT IP ADDRESS

We provide a dedicated tenant IP address for your organization, ensuring that your network traffic is isolated and protected from other networks. This significantly improves the security of your data and allows for precise control and customization of your security policies.

3.1.8 THREAT INTELLIGENCE NETWORK

Our Threat Intelligence Network provides real-time updates on emerging threats and vulnerabilities. It collects, analyzes, and disseminates information about new and existing threats, helping to proactively protect your organization from cyber-attacks.

3.1.9 SSL INSPECTION

Our service includes SSL inspection to decrypt and inspect SSL/TLS encrypted traffic for potential threats. This feature ensures that encrypted traffic, which often goes uninspected and could hide malicious activities, is thoroughly scrutinized for maximum security.

3.1.10 DNS SECURITY

We provide robust DNS security, preventing DNS-based attacks by filtering DNS requests, blocking access to malicious domains, and providing secure and reliable DNS resolution.

3.1.11 INTRUSION DETECTION/PREVENTION

Our intrusion detection and prevention system monitors network traffic for malicious activities or policy violations. It not only detects potential security breaches but also takes action to prevent and report them.

3.1.12 ANTIVIRUS / ANTIMALWARE

Our service includes robust antivirus and antimalware protection, scanning files and systems for any malicious software. It helps detect, block, and remove malware before it can cause any harm to your network or data.

3.1.13 DLP/CASB

Our Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) capabilities help prevent unauthorized data exposure or leakage, whether in use, in motion, or at rest. We provide thorough visibility and control over data across all cloud services and applications.

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

Overwatch SASE 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 SASE service, backed up by our MXDR security stack, 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. We guarantee a less than 15-minute notification Service Level Objective (SLO) for critical incidents.

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 THREAT HUNTING & INCIDENT RESPONSE

Our cybersecurity professionals actively hunt for signs of potential threats to your network and swiftly respond to any alerts. By integrating multiple industry-leading threat intelligence feeds, the MXDR platform allows our experts to investigate incidents, respond to threats, and minimize the impact on your organization.

3.5 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 SASE service evolves with your organization and continues to provide the most effective protection.

3.6 CONTINUOUS UPDATES & MAINTENANCE

Overwatch Managed SASE service and integrations are continuously updated to respond to the latest threat trends and vulnerabilities. New detection rules and SOAR response pathways are 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 SASE service is functioning optimally. Our support team 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 SASE Service helps businesses establish a more robust, secure, and flexible network infrastructure that supports their digital transformation efforts providing secure and optimized access to applications and data for users, regardless of their location or the devices they use.

- Simplified Network and Security Management: By converging networking and security into a single service, it reduces complexity and improves efficiency.

- Enhanced Security: It provides end-to-end encryption and threat protection, improving your overall security posture.

- Improved Performance: SASE improves the user experience by enabling direct, secure access to the internet and cloud services, minimizing latency.

- Cost Savings: By eliminating the need for separate security and networking hardware and software, it reduces total cost of ownership.

ADDITIONAL SERVICES (A LA CARTE)

5.1 REMOTE BROWSER ISOLATION (ADD-ON)

Our service includes Remote Browser Isolation (RBI), a feature that separates browsing activities from the network and endpoint, rendering non-executable, harmless versions of web content, thus protecting your systems from web-borne threats and attacks.

5.2 SD-WAN (ADD-ON)

Our Secure SD-WAN replaces traditional WAN routing with a cloud-native architecture, ensuring optimal network performance. This feature improves application performance, reduces network complexity, and lowers costs, all while enhancing security.

SECURE ACCESS ON-SITE (ADD-ON)

We can provide on-premises Cato Socket appliances that serve as the PoP (Point of Presence) for Cato's global, private, and SLA-backed network, but from within your environment. This device intelligently directs traffic (Full layer 7 visibility and interaction) based on policies and real-time network and threat conditions, ensuring optimized and secure access to all your enterprise resources.