Cybersecurity Services

MANAGED FIREWALL

Our certified Security Engineers and Analysts ensure that your firewalls are actively managed to provide maximum protection against the evolving threat landscape, enhancing your business continuity.

24x7 Monitoring: Round-the-clock prevention and detection of threats.

Threat Response: Resolution or mitigation of risk in the event a vulnerability is discovered or a security event occurs.

Custom Runbook: Customer-tailored rules and actions for any security events that are triggered in the firewall.

Reporting: Quarterly reporting of security threats found and remediation steps performed.

Device Management: Customer-requested and/or Edge-recommended configuration changes including remote VPN configuration, firewall rules, NAT rules, web DNS filtering whitelisting, policy audits, patch management, control rules customization, device backups.

Firewall Audit: A bi-annual audit of all firewall rules and policies, providing recommendations based on industry best practices.

This best-in-class threat prevention service can be delivered in conjunction with an Edge-provided firewall or with customer-owned hardware.

SECURITY AWARENESS TRAINING

A **managed service** that educates your employees on various social engineering attack vectors, reducing cyber risk through the protection of the integrity and confidentiality of company information.

Rules of engagement are established and customized phishing and social engineering campaigns are created. These campaigns are randomly sent to employees to assess their current awareness of common tactics used by malicious users. Based on those interactions, employees will then be enrolled in specific training which will review security best practices.

A second level of training includes a detailed and customized training for your industry. Employee interactions with these email campaigns are tracked and provided to an administration group for review. Remediation and training recommendations are provided by the Edge Security team to ensure understanding of the results and for preparation of ongoing campaigns.

MANAGED DETECTION & RESPONSE (MDR)

A combination of **security expertise** and **leading technology solutions** to detect dynamic threats quickly across your entire ecosystem to provide the hands-on, 24/7 monitoring, proactive threat hunting, effective response support, tailored security guidance, and team of experts to stop malicious activity and help you accelerate your security maturity.

Edge monitors and analyzes activity data from all deployed Rapid7 InsightIDR endpoints and collection points in your environment 24/7. This traffic from Email, endpoint, server, cloud workload, and network sources are correlated for stronger detection and greater insight into events occurring in the environment. This allows our team the capability to identify the source and spread of complex targeted attacks by utilizing User Behavior Analytics in conjunction with our Threat Based Detections.

Key Features include: Mitre Attack Framework Alignment, Threat Hunting and Deception Technologies

MANAGED VULNERABILITY MANAGEMENT

Edge leverages best-in-class tools through the Rapid7 Insight VM platform to deliver a highly effective risk-based vulnerability management program. Our experts work with your team to design a process to deliver effective risk reduction.

- Identification and communication of the vulnerabilities in your environment.
- Prioritization of risk based on our Real Risk score and knowledge of current attacker methods.
- Working with all relevant technical teams responsible for remediation.
- Tracking remediation progress and driving towards resolution.
- Showing measurable progress aligned to your program goals.

Weekly or monthly scans are performed, with Edge Security Analysts reviewing the results, documenting the findings, and providing remediation recommendations. Vulnerability remediation is prioritized and performed based upon attacker analytics.

ONE-TIME VULNERABILITY SCANNING

This service detects network vulnerabilities via the scanning of selected devices in your IT environment and reports potential exposures.

Our **External Scanning** simulates attackers from the outside world attempting to penetrate your network while **Internal Scanning** identifies inside-the-network weaknesses.

Internal scans are performed via a VPN tunnel or onsite appliance. Scans are configured based on your timing preferences. Reports are generated and reviewed by Security Engineers after each scan. An evaluation is performed to ensure the network is secure and a mitigation plan developed in the event of a discovered anomaly.

END POINT PROTECTION WITH ADVANCED MALWARE PROTECTION

Edge Managed End Point protection is powered by SentinelOne to provide a next-generation endpoint platform to tackle new and evolving threats. SentinelOne's Singularity platform unites **Detection, Response, & Remediation** to better protect your organization.

This service delivers next-generation endpoint protection backed by Edge's security team and SentinelOne machine learning to:

Detect and **mitigate** threats faster, isolating infected endpoints rapidly thus reducing remediation costs.

Block a threat everywhere after it is seen in the environment, eliminating the risk of an infection spreading across the network.

Investigate and **respond** to threats across the network, web, and endpoints.

MANAGED EMAIL SECURITY

Edge is partnered with Mimecast to provide a **complete Email Security Platform**. Mimecast's Advanced Email Security with Targeted Threat Protection uses multiple sophisticated detection engines and a diverse set of threat intelligence sources to protect email from spam, malware, phishing, and targeted attacks.

The Mimecast services defend against email-borne impersonation attempts, malicious URLs and attachments, threats that are internal to the organization, and attacks from the inside that are destined for external recipients.

VIRTUAL CHIEF INFORMATION SECURITY OFFICER (VCISO)

Edge's **vCISO program** offers a **remote security board-level leader and a team of cybersecurity specialists** to continually evaluate your cyber landscape and business security posture.

Maximize Protection and Reduce Risk: Edge will manage your technology, reduce your organizational risk, and minimize the threats that can have detrimental consequences.

You'll have a technology and security specialist that thoroughly understands your business's architecture, integrates your technology, and manages your organizational security. We'll also act as a dedicated point of contact and your continued access to expert security skills and expertise for a managed security service that helps you achieve your goals.

Response: Should an incident occur, Edge can support an investigation into the breach.

Cost-Effective Security: Our vCISO program is a cost-effective solution to bridging the gap between your technology goals and the security and protection that enables you to utilize digital tools.

It eliminates the need for a full-time or in-house Chief Information Security Officer who would only be utilized sporadically. Our service gives you access to an expert who can manage your security and protection, implement adaptations that allow you to scale to new growth and answer any queries you have along the way, without the full ongoing cost.

INCIDENT RESPONSE & FORENSIC SERVICES

Early detection and response is the key to protecting critical assets. When an attack happens, your response must be swift. In the unfortunate event of an incident, we provide on-demand incident response teams to quickly help you manage and contain damage.

Edge can assist organizations to be prepared before an attack, to develop early detection capabilities and respond effectively should an attack happen:

Readiness: Assisting organizations in developing logging and alerting capabilities as well as procedures for first response incident handling.

Response: Should an incident occur, Edge can support an investigation into the breach.

Edge proposition overview:

Incident Response & Computer Forensics: Proactive crisis management and tracing the root of a breach through computer forensics (including malware analysis).

Managed Security Services & Managed Detection Response Solutions: A complete set of services starting with log management assessment, risk assessment and strategy development, selection of Security Information and Event Management (SIEM) tool and /or Managed Security Services (MSS) solution.

MULTI-FACTOR AUTHENTICATION

Edge has partnered with Cisco DUO for multi-factor authentication. DUO requires users to authenticate in multiple ways prior to accessing authorized systems. **Edge Security Engineers will configure and manage a multi-factor solution** which meets the requirements for PCI DSS Standards.

SECURITY RISK ASSESSMENT

Edge performs **security assessments** across several industry standards including **NIST, PCI DSS, ISO 27k and general assessments**.

A security risk assessment identifies key security control conditions in applications. It also focuses on preventing application security defects and vulnerabilities. Carrying out a **risk assessment allows an organization to view the application portfolio holistically** - from an attacker's perspective. It supports managers in making informed resource allocation, tooling, and security control implementation decisions.

A comprehensive security assessment allows an organization to:

- Identify assets (e.g., network, servers, applications, data centers, tools, etc.) within the organization.
- Create risk profiles for each asset.
- Understand what data is stored, transmitted, and generated by these assets.
- Assess asset criticality regarding business operations. This includes the overall impact to revenue, reputation, and the likelihood of a firm's exploitation.
- Measure the risk ranking for assets and prioritize them for assessment.
- Apply mitigating controls for each asset based on assessment results.

RAPID7 DUO SentinelOne mimecast