Solution brief

Monitor threats and know your risk.

Reduce risk and maintain the integrity of your data and applications with Managed Security Services—Premises.

verizon

As your business grows, so do the threats to your systems and data. According to the Verizon Data Breach Investigations Report (DBIR), methods of attack are becoming increasingly sophisticated. You're continually confronted by attacks that make avoiding damage difficult. But with comprehensive security monitoring and management services, you can protect what's most important.

To focus on your business goals, you need to manage risk across your infrastructure. That means anticipating problems, taking corrective action, and showing practical results – while controlling costs by freeing up internal IT resources. With Verizon Managed Security Services (MSS), you can proactively identify vulnerabilities and prioritize threats – helping you improve visibility and reduce risk.

Around-the-clock security expertise.

Managed Security Services – Premises provides monitoring and management for a wide array of security devices at your various locations. Your devices are connected via a Connection Kit to a hosted Local Event Collector in one of our Security Management Centers. This vendor-neutral service allows you to select world-class products, help protect past investments in technology, and avoid vendor lock-in.

Your security devices generate threat data in the form of logs or events. We collect this threat data in near-real time and send it to our Security Analytics Platform, with its proprietary correlation and classification technology. The platform filters out benign security events and escalates those incidents most likely to pose a threat. We then assign each incident a risk rating and reference the specific threat-detection use case triggered. You can view security incident information through the web-based Unified Security Portal.

We're positioned as a leader in the 2018 Gartner Magic Quadrant for Managed Security Services, Worldwide.[1]

Quickly review incident information.

The Unified Security Portal provides an up-to-date view of the security posture of serviced devices. You can view incidents by country or see the number of incidents that are escalated, open, and closed. Status bars illustrate the risk levels – critical, high, medium, and low. Risks are also presented based on an impact and likelihood scale.

The dashboard provides granular search and query capabilities, and comprehensive reporting on incidents and logs. You can review security intelligence in risk briefings, reports, and updates.

By monitoring threats, assessing risks, and maintaining security policies, we help safeguard your assets – so you can focus on your business goals.

Easily analyze data with log management.

Within the Unified Security Portal you can also collect, store, and search raw logs for all security devices we monitor. We store raw logs for one year and indexed logs for up to 90 days. The log management capability includes field-based filtering, along with raw log searches and downloads.

In-depth examination of incident trends.

Dive deeper into incident trends with the Log and Incident Analytics features. With Log Analytics, you can drill down on results and filter for a subset of logs. Incident Analytics lets you search incidents with queries on key properties. Both provide a graphical view of results. The Trends and Reporting feature allows you to display trends on your security incidents, compare your results to aggregated trends affecting other Verizon customers, and to have access to monthly executive reporting via the Unified Security Portal.

Intelligence-driven security monitoring and analysis.

Our threat-detection policies are based on a holistic and near-real-time, behavior-based, multifactor correlation capability. Security Analytics Platform evaluates and correlates reputational and behavioral patterns and characteristics, as well as signature-based detection methods. Our framework is the result of research and threat analyses conducted by our intelligence team, and is composed of use cases, correlation reasons, watch lists, DBIR findings, and "indicators of compromise" threat-based intelligence.

Security incidents are generated based on detection policies with flexible rule setting to help control incident volumes. All security incidents generated have a clear description as to why the incident was triggered. We categorize all use cases and proprietary signatures to help increase visibility into security incidents and to help reduce the number of harmless incidents you see.

The incident descriptions provide recommendations on possible actions to take, and the Security Operations Center (SOC) analysts can enrich this content.

This analysis greatly simplifies incident escalation and makes it easier for you to understand the security posture of your serviced devices.

Devices supported by Managed Security Services.

- Application-Level Firewall
- Content Screening
- E-Mail Security Gateway
- Endpoint Security
- Firewall
- Host Intrusion Detection System (HIDS)/Host Intrusion Prevention System (HIPS)
- Load Balancers
- Log Monitoring and Management
- Network Intrusion Detection System (NIDS)/Network Intrusion Prevention System (NIPS)
- Proxy Server
- Unified Threat Management (UTM) or Security Appliance
- VPN
- Operating System/Active Directory monitoring

Tailored to your needs.

We offer monitoring only or monitoring with management. You can complement your choice with the following options:

- Remote Office
- Executive Reporting
- Security Policy Program
- Security Policy Program Reporting and Review
- Security Device Service Availability SLA

Protect what's most important.

Our global infrastructure, world-class services, and security professionals are ready to help you meet a wide range of security challenges. Actionable intelligence and risk ratings help you allocate the right resources against the most dangerous threats. Consistent policy management and incident handling provide a unified view of your security posture across your serviced devices. Our experienced security consultants have the knowledge and management capabilities to help you design and roll out your security strategy on a global scale. Managed Security Services – Premises can help you mitigate vulnerabilities and better protect your infrastructure, so you can stay focused on managing your business.

Learn more:

To find out how Managed Security Services can help you better protect your organization, contact your account manager.

verizon

verizonenterprise.com

1. Gartner, Magic Quadrant for Managed Security Services, Worldwide, Toby Bussa et al, February 2018
Gartner does not endorse any vendor, product or service depicted in our research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.