Managed Security Services

assess risks, detect vulnerabilities, thwart attacks, block intruders & ensure compliance

Managed information technology (IT) security services from US Signal help strengthen protection across your entire network without increasing your internal team's workload. These services leverage years of IT security knowledge with industry best practices to protect your unique operation against risks, threats and potential damage. Unlike off-the-shelf options with limited capabilities, our services provide a comprehensive range of solutions backed by 24/7 customer support.

Technical Overview

Examples of the types of managed security services offered:

- **Advanced Email Security:** Powered by Acronis & Perception Point, our advanced email security services use threat intelligence and multiple scanning engines to prevent threats proactively.
- **Managed Firewall:** US Signal's managed firewall solution delivers comprehensive protection throughout your network, from the hardware inside your facilities to your mobile devices or remote workforce.
- **Website and Application Security:** Strengthen your defense by protecting against various internet-based threats like content scraping, structured query language (SQL) injection attacks and distributed denial of service (DDoS) attacks.
- **Managed Detection Response:** Prevent and resolve security issues for all your endpoints, including desktops, laptops, mobile devices and servers.
- **Managed XDR:** Our managed extended detection and response (XDR) service monitors, detects and responds to security issues across your expanded operating environment, including servers, networks and cloud platforms.
- **Patch Management:** US Signal's patch management services use manual and automated installations for Windows operating systems and various third-party applications.

In addition, our professional services team offers expert consulting on various security-centric solutions, from program assessments to advanced troubleshooting to virtual chief information security officer (vCISO) services.

At-A-Glance:

- Multiple managed firewalls
- Monitored 24/7 by US Signal’s TOC
- Firewalls available with MPLS, Virtual Ethernet Services, Dedicated Internet, and US Signal’s Cloud environments
- Easily terminate site-to-site IPsec VPNs for private connectivity into your environment from branch offices or remote offices
- Industry leading availability performance metric of 99.995%

info@ussignal.com **ussignal.com** **866.2.signal**

Secure Access Service Edge (SASE)

US Signal SASE leverages cutting-edge technology, including Software-Defined WAN (SD-WAN), Firewall as a Service (FWaaS), Zero-Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), and unified management to create a unified platform. This innovative platform allows optimal WAN management, global connectivity, WAN and internet security, cloud acceleration, and remote access to provide customers with an unparalleled level of security.

US Signal SASE eliminates the need for on-premise infrastructure, improving agility by deploying new resources effortlessly. With a simpler network and security stack, businesses can reduce upfront costs, scaling only what they need without in-house management. US Signal SASE offers full visibility into WAN and internet traffic with no blind spots, using unified policies to create a simpler, more efficient, and secure network infrastructure.

Managed Email Security

Defend against advanced persistent threats (APTs), zero-day attacks, and more with US Signal's Advanced Email Security powered by Perception Point and Acronis. Combining multiple scanning engines, advanced threat intelligence, and the power of the cloud, it enables you to proactively prevent threats — including those that often evade conventional defenses — before they reach end users' mailboxes, regardless of the email service.

Its propriety software algorithms analyze code at the CPU level to intercept attacks at the earliest stage possible. Unlike legacy sandboxing solutions, all content, including files, URLs, and the email itself, is analyzed. A clear verdict is delivered in seconds. It's also able to scan 100% of email traffic no matter what the volume is.

Managed Firewall Services

A managed firewall is one of the first lines of defense in protecting your organization against internet-based threats and attacks. A solution from a dependable and experienced managed service provider (MSP) can handle the administration, operation, maintenance and monitoring of your firewall infrastructure. The most effective firewalls require careful expertise and structure based on an organization's specific network requirements and unique needs.

Managed firewall services from US Signal are industry-leading solutions utilizing advanced technology from Palo Alto's next-generation firewall platform. These services deliver a market-best availability performance metric of 99.995% with 24/7 monitoring from our technical operations center. US Signal's managed firewalls are compatible with our cloud environments and other services, including virtual ethernet, dedicated internet and multiprotocol label switching (MPLS).

Website and Application Security

US Signal's Website and Application Security (WaAS) strengthens your defenses, protecting against a wide range of internet-based threats, including volumetric, distributed and multi-vector DDoS attacks, SQL Injection attacks, and content scraping.

Scalable, cloud-based and provided as a managed service, WaAS is available for websites and applications hosted on-premise, in colocation, and on cloud-hosted servers. You get unmetered filtering of malicious or unwanted traffic backed by a 100% uptime SLA.

WaAS is offered in 2 service tiers: **Standard and Premium**.

- Standard is designed for small to mid-size organizations with websites and applications that need advanced security and performance with 24/7/365 support.
- Premium is for mid-size to enterprise organizations with critical web assets that require enterprise-grade security and performance with 24/7/365 support that includes prioritized networking and vendor support.

Both include:

- Multi-layer, unmetered DDoS mitigation (including application attacks) up to 30 Tbps
- Protection against DDoS attacks such as HTTP, SYN, UDP, ACK, and QUIC floods
- A web application firewall (WAF) for advanced website and application protection against SQLi attacks, dangerous file upload attacks, content scraping and more
- Simplified, auto-renewing SSL certificate management with TLS 1.3 for PCI DSS 3.2 compliance
- 24/7/365 technical support
- DNS with optional DNSSEC

Managed Detection and Response Services

US Signal provides managed endpoint detection and response (MDR) services to help resolve and prevent security issues in your organization's endpoint devices, including servers, desktops and laptops. These solutions protect against today's most complex cyber threats by utilizing continuous monitoring processes and cutting-edge technologies, like machine learning, artificial intelligence (AI) and other advanced detection tools.

Our MDR services leverage a third-party software platform to collect, monitor and analyze endpoint data that could represent a threat. The tools integrate data from all endpoints to bolster security and eliminate blind spots across your network. Administrators can configure rules to respond to identified threats by removing or containing them automatically.

Managed Threat Detection and Response Service Features
The security operations center (SOC) team at US Signal will work with your organization to set up and implement the MDR service. It operates on a cloud-based deployment model, meaning software agents communicate directly with the central management platform. These agents perform endpoint monitoring and collect data throughout all your activity, processes, connections and data transfers, placing it into a central database.

After monitoring and collection, the pre-configured rules in your MDR solution identify when incoming data contains a known security breach and trigger an automatic response to log the user off or alert an administrator. Forensics tools allow information technology (IT) security professionals to investigate past incidents and understand how the breach worked to penetrate security.

Primary features include:

- Real-time network monitoring and continuous endpoint data collection
- Rule creation through automated responses and analysis
- Protection for remote workers and offline applications
- Automatic firewall control, threat blocking and quarantine
- Device management for USB and Bluetooth applications
- Policy configuration and compatibility assessments
- 24/7/365 monitoring and response

Managed Extended Detection & Response (XDR)

Trust US Signal’s security experts to monitor, detect, and respond to security issues across your extended environment with Managed Extended Detection and Response (XDR). Leveraging a third-party software platform, the US Signal Security Operations Center (SOC) team monitors, collects and correlates data from servers, network devices, cloud services and more to identify security threats and their origination.

The SOC team also receives and responds to all security alerts, freeing up your internal resources and enabling you to take advantage of the team’s in-depth security expertise.

In addition to our robust Managed XDR service, US Signal provides an add-on option for Vulnerability Management. Our SOC team conducts comprehensive vulnerability scans to identify potential threats, and offers remediation guidance to keep your network secure. With this service, you can ensure constant monitoring and proactive mitigation, enabling you to focus on what’s important.

Distributed Denial of Service (DDoS)

Our proactive approach combines state-of-the-art technology and expert support to deliver a multi-layered defense strategy:

- **Detection and Analysis** - Our systems provide constant monitoring to detect threats early, analyzing traffic patterns to distinguish between legitimate traffic and potential attacks.
- **Mitigation and Response** - Once a threat is identified, our mitigation tools kick in, blocking malicious traffic while allowing legitimate traffic through. This ensures your business operations remain uninterrupted.
- **Continuous Optimization** - We don't just stop at mitigation. Our team continuously optimizes the defense mechanisms, adapting to evolving threats and ensuring your protection evolves with them.

Patch Management

Ensure timely patch management that fits your needs with US Signal's patch management service.

Both manual and automated installation are available, based on policies defined and created between you and the US Signal Professional Services team during the onboarding process.

Patch management is offered for Windows OS and a wide variety of third-party applications from companies such as Adobe, Apple, Google, Mozilla, Opera, Skype and Sun.

IT Security Consulting Services

US Signal offers various risk assessment and data security services that can help boost your cybersecurity practices while improving your IT network's general security stance. Our consultants can help you identify the areas that need improvement and take the necessary steps for implementation. We specialize in the areas below:

Ransomware Protection Solutions for Businesses

The experts at US Signal have years of combined experience helping clients protect their networks from ransomware attacks and remediating them after they occur. Besides offering individual solutions that target ransomware directly, we provide top-class consulting services that offer general insight into your overall information technology (IT) program. We work with businesses of all sizes to deliver server protection and data backup recovery solutions, from small startup operations to large-scale enterprises.

Several examples of the services we offer to address ransomware and other security issues are:

- **Managed IT Security:** We provide a comprehensive range of managed IT solutions that help mitigate threats and potential risks, from advanced email security and website application security to managed firewalls and managed detection and response.
- **Data Backup Recovery:** Our backup solutions allow you to back up your data from any virtual or physical infrastructure to the US Signal Cloud, then access or restore it when needed.
- **Disaster Recovery:** US Signal's disaster recovery solutions are service-level-agreement (SLA) -backed and offer comprehensive protection during natural disasters, human error or ransomware attacks.
- **IT Security Consulting:** We offer top-class IT security consulting services to help your organization make more informed risk management decisions and strengthen your security posture, including assessments, policy and procedure development, augmentation and virtual chief information security officer (vCISO) services.

Virtual Chief Information Security Officer Services

Virtual Chief Information Security Officer (vCISO) services enable businesses without an in-house officer to secure sensitive data and manage information technology (IT) risk cost-effectively. Virtual CISOs comprehensively assess a company's security posture to identify weaknesses and maximize security standing over the long term. They accomplish these tasks by delivering highly qualified

helping clients protect their networks from ransomware attacks and remediating them after they occur. Besides information security expertise on demand instead of the company filling a dedicated full-time position.

US Signal offers vCISO services that range from overseeing the execution of daily security tasks to executive-level planning and guidance, including customized strategies and processes based on your organization's unique requirements. Our team offers this feature for one-off projects, on-demand or continuously for however long you need.

Augmentation

Our security operations center (SOC) consultants can help you replace or supplement your existing security efforts through services like these:

- Daily log reviews
- Vulnerability management program assistance
- Incident and endpoint security platform management
- Security information and event management (SIEM)
- Firewall rule analysis
- Payment card industry (PCI) segmentation scanning
- Department procedure and playbook updates
- Security platform implementation

Policy and Procedure Development

Our security experts can help your organization develop or enhance security policies and procedures by:

- Establishing long-term goals.
- Defining your company's business and regulatory requirements
- Reviewing your current resources and examining your organization's threat landscape.
- Comparing gaps and deficiencies to best practices.
- Developing practices and procedures to meet business objectives.
- Recommending steps for implementation, training and updates.