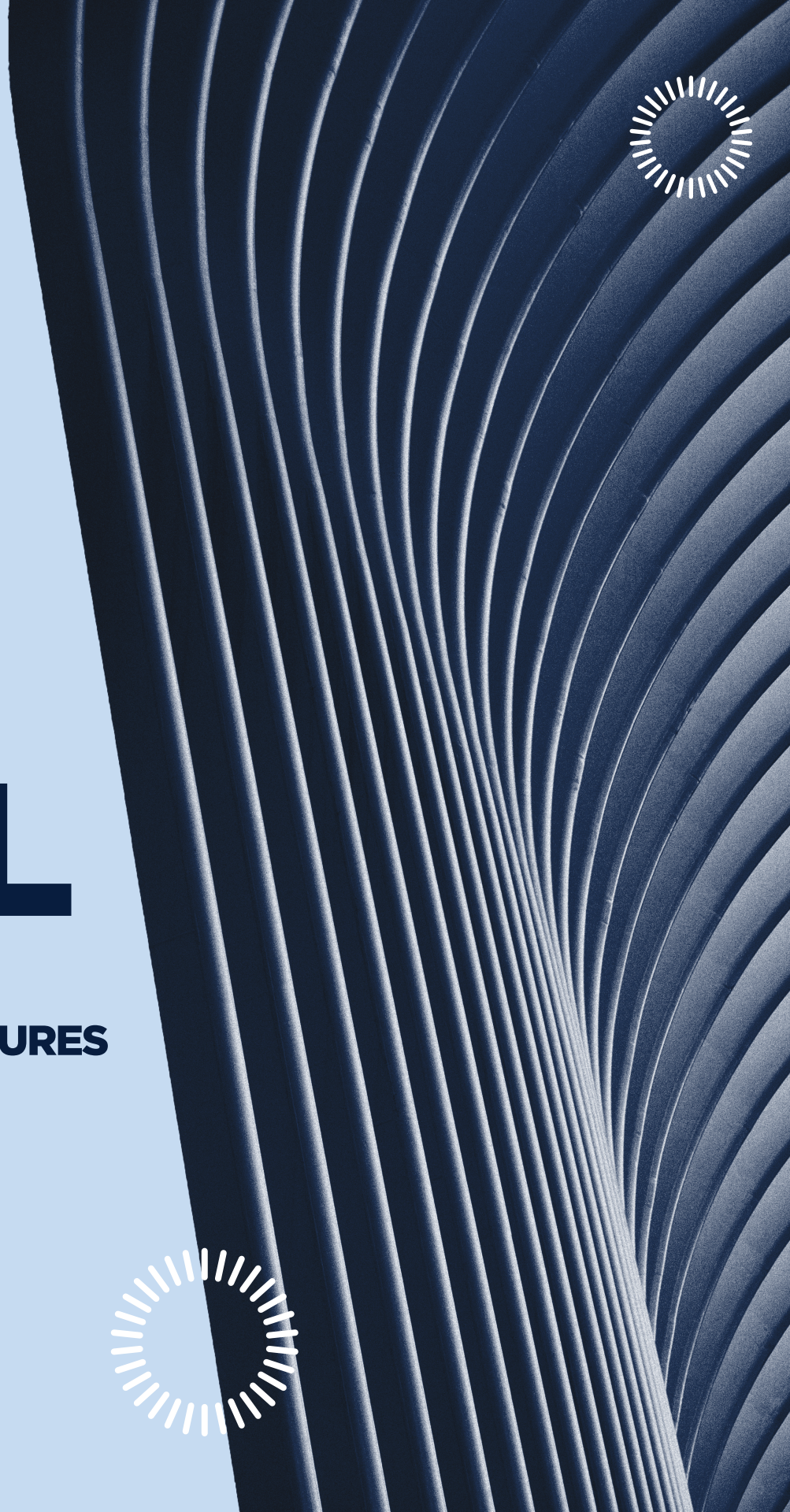
SAFE WITH US SIGNAL

AN OVERVIEW OF US SIGNAL'S SECURITY SERVICES AND FEATURES



US SIGNAL®

TABLE OF CONTENTS

Data isn't the only thing growing at an exponential rate. So are the threats to it — and to IT systems that store and process data. Mobile devices and the Internet of Things (IoT) continue to expand the threat landscape. Ransomware, zero-day vulnerabilities, and other types of cyber-attacks are becoming more sophisticated. Insider threats are increasing in frequency.

Staying on top of potential threats is hard enough for IT departments, let alone keeping pace with the technologies to combat them and the penalties for failed prevention. That doesn't have to be the case when you partner with US Signal.

US Signal offers an ever-expanding services to build a comprehensive, proactive security strategy that meets your budget parameters and compliance needs.

This eBook provides a brief overview of some of the services, as well as US Signal's own security features. They're among the many reasons your company can stay safe with US Signal.

INTRODUCTION

MANAGED DETECTION + RESPONSE (MDR)

MDR provides round-the-clock monitoring to detect, investigate, notify and respond to incidents and potential threats, as well as limit the impact of security threats. With 24/7 threat monitoring, MDR supports incident response using playbooks driven by advanced orchestration and automation systems. This process rapidly contextualizes incidents with enriched data, orchestrates response workflows, and automates threat containment.

KEY BENEFITS:

- **24/7/365 monitoring and response**
- **Remote worker protection and offline protection**
- **AI and behavioral-based detection**
- **Incident forensics reporting**
- **Automated threat blocking**
- **Firewall control**
- **Device control for USB and Bluetooth**
- **Complete endpoint visibility**
- **Custom detection rules**
- **Automated quarantine**
- **Policy configuration and compatibility assessment**

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 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.

KEY BENEFITS:

- **Extends monitoring beyond endpoints to include network and cloud sources**
- **Unifies data into a single security view**
- **Real-time continuous monitoring and collection of data**
- **AI behavioral-based detection**
- **Correlation of data across resources**
- **Contextualizes suspicious behavior by searching logs, browsing through firewall activity, or combining through IP addresses**
- **Provides fast threat detection and response**
- **Remediation guidance provided by US Signal SOC**
- **Cloud-based deployment model**
- **Agents and log collection**
- **Predictable monthly fee based on number of endpoints**

US SIGNAL®

As a first line of defense against malicious and anomalous activity, Managed Firewall offers consistent protection for your entire network — from your main facilities to your mobile and remote workforce.

This managed security solution is built on a cloud-based firewall platform developed by one of the industry's leading cybersecurity companies. It delivers all the protections afforded by the latest security technologies. Because it's fully managed, you benefit from the expertise and support of US Signal's security experts and 24/7/365 Technical Operations Center.

KEY BENEFITS:

- **Monitors inbound Internet traffic; blocks inappropriate material from view by the browser**
- **Leverages detection and prevention mechanisms**
- **Scans traffic against rules from open community definitions**
- **Integrates into your hosted email environment as an email gateway to provide anti-spam services**
- **Offers granular, role-based control over privileges and responsibilities of administrative users**
- **Enables you to create granular policies based on users and groups**
- **Allows for easily terminating site-to-site IPsec and client VPNs for private connectivity into your environment from branch offices or remote offices**
- **Identifies applications in use, including shadow applications**
- **Offers high-performance proxy caching server for web clients, saving bandwidth while increasing performance**
- **Provides comprehensive information via logging on security activity**

MANAGED FIREWALL

ADVANCED EMAIL SECURITY

Defend against advanced persistent threats (APTs), zero-day attacks, and more with 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, Advanced Email Security analyzes all content. A clear verdict is delivered in seconds. It's also able to scan 100% of email traffic no matter what the volume is.

KEY BENEFITS:

- **Blocks malicious communications with anti-spam and reputation-based filters**
- **Stops advanced attacks such as APTs and zero-days with CPU-level analysis at the exploit stage**
- **Recursively unpacks content into smaller units, which are dynamically checked by multiple engines in under 30 seconds**
- **Identifies threats with best-of-breed signature-based antivirus engines enhanced with a unique tool to identify highly complex signatures**
- **Uses URL reputation engines and advanced image recognition technology to validate URLs**
- **Prevents payload-less attacks through the use of machine-learning algorithms with IP reputation, SPF, DKIM, and DMARC record checks**
- **Monitors all traffic and analyzes malicious intent with ongoing reporting and support**
- **Flags emails with customizable banners based on policies and rules to increase security awareness**

US SIGNAL®

WEBSITE + APPLICATION SECURITY

Website and Application Security (WaAS) protects 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, WAS works 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.

The standard service tier is for small to mid-size organizations; premium is for mid-size and enterprise organizations.

KEY BENEFITS:

- **Multi-layer, unmetered DDoS mitigation up to 30 Tbps**
- **Advanced 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**
- **DNS with optional DNSSEC**
- **Blocks and filters threats and unwanted traffic before they reach origin servers and internal networks**
- **Customers who host websites and applications in the US Signal Cloud get the benefit of multiple direct peering locations between our fiber network and the Cloudflare® network**
- **Global Anycast CDN with the fastest, highest ranked DNS available**
- **Extra tools for optimizing website performance**
- **Proactive monitoring and management by US Signal Engineers**
- **PCI DSS 3.2/HIPAA compliant and GDPR friendly**
- **Supports multiple custom SSL certificate uploads**

US SIGNAL®

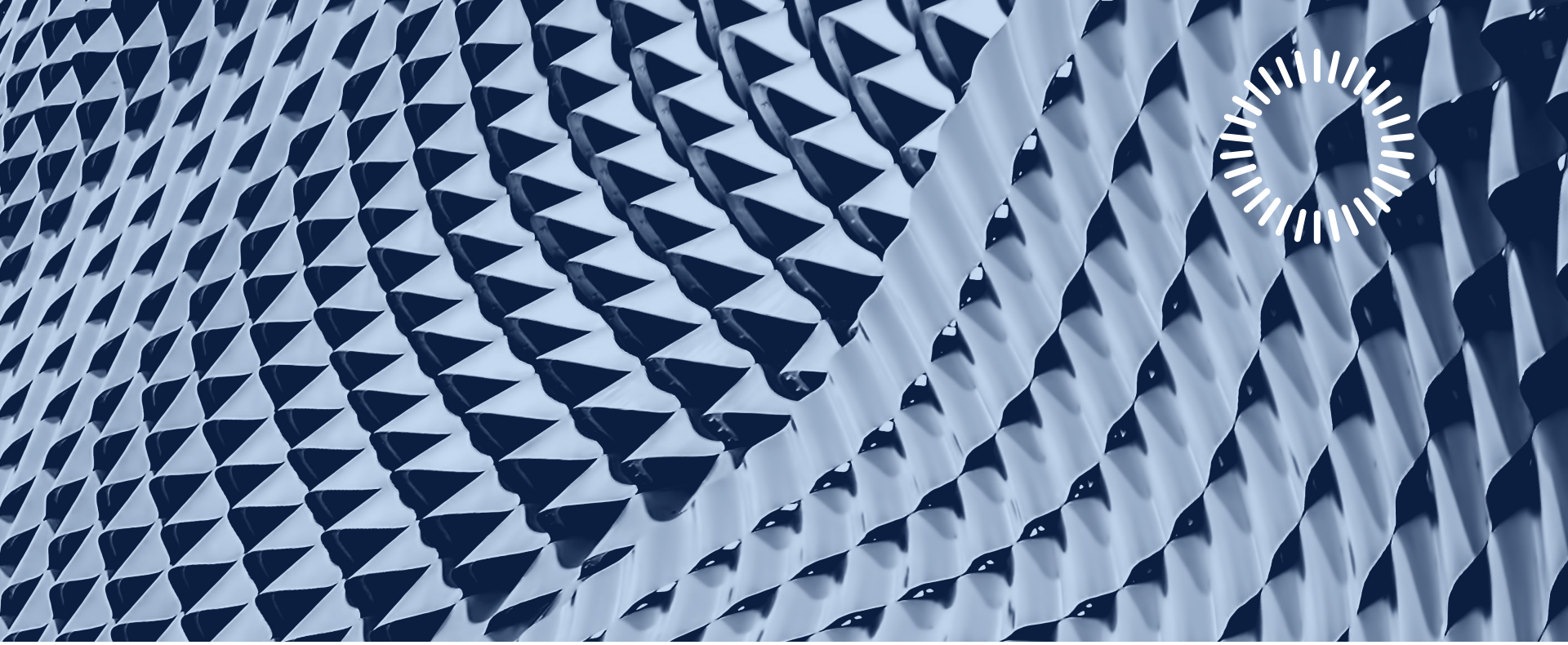
PATCH MANAGEMENT

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.

Patch management can also be combined with other services, such as MDR, to provide a comprehensive, proactive approach to IT security.

US SIGNAL®



Get an in-depth look at your organization's current security posture, and identify IT security vulnerabilities with US Signal's security and risk assessment services. Assessment services can be on a one-time basis or set up as an ongoing engagement.

SERVICES INCLUDE:

- **NIST Cyber Security Framework ("CSF") Assessment**
- **Cyber Security Maturity Assessment**
- **Security Framework Gap Analysis**
- **Phishing-Social Engineering Assessments**
- **Risk Assessments**
- **Ransomware Assessments**

ASSESSMENTS

Build out an effective, best practices-driven security program without having to recruit, hire and maintain a Chief Information Security Officer (CISO).

SERVICES INCLUDE ASSISTANCE WITH:

- **Developing or updating specific policies**
- **Designing and building a security architecture**
- **Managing IT risk against business goals**
- **Securing sensitive data**
- **Developing cybersecurity training and increase cybersecurity awareness**
- **Overseeing specific projects such as vendor risk assessment and compliance initiatives**
- **Creating and implementing a data loss prevention plan**
- **Conducting audit remediation**

VIRTUAL CISO

AUGMENTATION

Utilize US Signal's Security Operations Center (SOC) team to help supplement or replace your current internal security efforts. US Signal can provide a variety of services ranging from advisory services or staff augmentation and task execution.

SERVICES INCLUDE:

- **Vulnerability management program assistance**
- **Daily log review**
- **Incident management**
- **Endpoint security platform management**
- **SIEM management and tuning**
- **Firewall rule analysis**
- **PCI internal segmentation scanning**
- **Best practice configuration reviews**
- **Update of department procedures and playbooks**
- **Security platform implementation**

US SIGNAL®

POLICY + PROCEDURE DEVELOPMENT

Work with US Signal's security experts to develop or refine information security policies and procedures that meet your organization's business objectives, fit within its culture and address current and emerging threats.

TYPICAL SERVICES INCLUDE:

- **Definition of desired future state and your organization's business and regulatory requirements**
- **A comprehensive examination of your unique threat landscape and available security resources**
- **Identification of gaps and deficiencies compared to desired practices and technologies**
- **Development or enhancement of required policies and procedures, driven by best practices and built to meet business objectives**
- **Recommendations for implementation, training, and regular updates**

While US Signal can't eliminate compliance requirements for you, we can help ease the burden. US Signal maintains a well-governed, high-quality IT infrastructure that meets the demands of a wide range of governing agencies. By ensuring the necessary security controls and documented processes are in place and regularly audited, US Signal can help your company meet many of its compliance requirements.

US Signal is audited for compliance with or holds certifications for numerous regulatory requirements and industry standards. Among them:

IN ADDITION, US SIGNAL:

- **Will sign a Business Associate Agreement (BAA)**
- **Will provide audit documentation and other assistance as appropriate**
- **Has an on-staff compliance officer and executive security team**
- **Maintains a full Governance, Risk, and Compliance (GRC) program**
- **Employs a risk-based BC/DR plan and an Incident Response plan with tabletop tests performed annually**
- **Conducts regular employee IT security training**
- **Has a Vendor Due Diligence program**

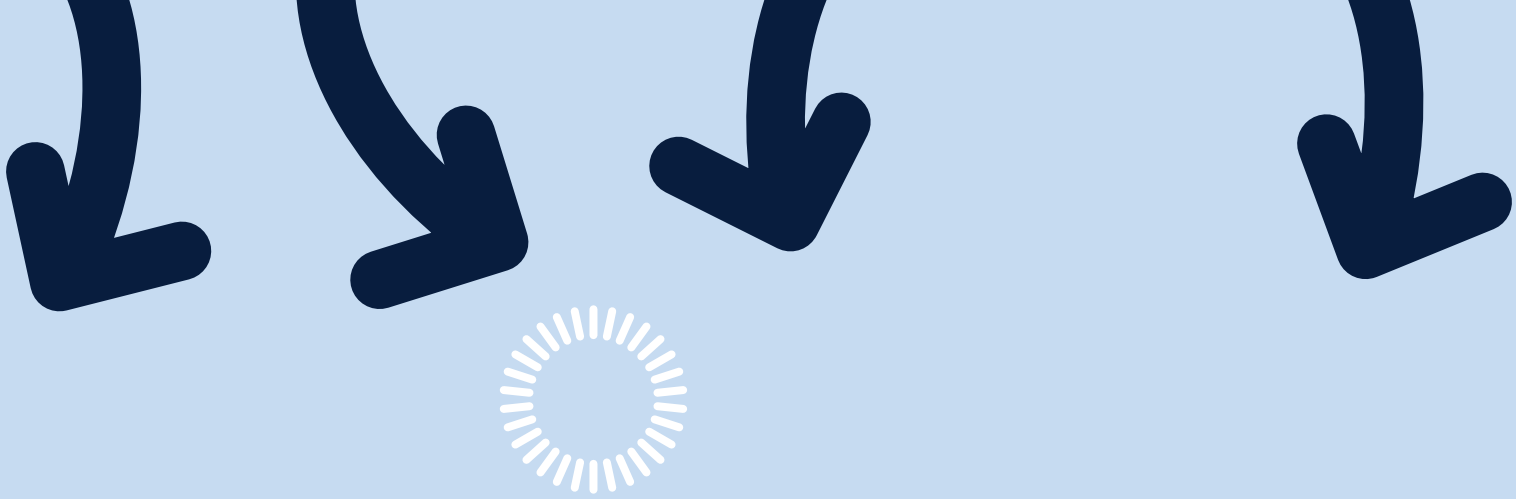
COMPLIANCE

DATA CENTER SECURITY

Along with a secure, robust fiber network, US Signal's data centers are at the core of its services. While security features vary among US Signal's eight Midwest-based data centers, they generally include:

- **Vehicle intrusion prevention (selected facilities)**
- **Internal and external camera coverage at all entry points with appropriate lighting**
- **24/7 monitored pan-tilt zoom and fixed-focus cameras with surveillance footage archived for one year off-site**
- **Biometric iris scanners or user-assigned proximity access cards (varies by facility) with the data centrally analyzed, correlated, and archived by US Signal's log rhythm SIEM platform**
- **Interlocking access control vestibule to enter the building and a second access control vestibule to enter the data center floor (selected facilities)**
- **Required visitor login and badge when inside a US Signal facility, along with escort by a US Signal employee or authorized colocation customer**
- **Locks on all cages and cabinets**
- **Intrusion alarms and motion detectors**
- **Fire suppression and fire alarm systems**
- **24/7 monitoring and alarms for HVAC, water detection, humidity, temperature, power outage, and generator operations with immediate alert response**

US SIGNAL®



US Signal employs leading-edge security technologies to ensure all aspects of its operations are protected. That includes:

THAT INCLUDES:

- **Redundant firewall clusters that are diversely located for the corporate infrastructure with full threat management capabilities**
- **Host-based intrusion detection, passive network detection, firewall-based IPS, net flow monitoring, DNS security, and centrally monitored**
- **Antivirus are used to help provide multiple layers of defense**
- **Two-factor authentication**
- **An endpoint protection platform that includes workstation encryption in addition to the ability to address advanced threats such as malware and ransomware**
- **SIEM platform for centralized log collection to monitor deployed enterprise, cloud, and service provider technology to identify, correlate, and remediate any potential security incidents**

SECURITY TECHNOLOGIES

PROCESSES + POLICIES

In addition, US Signal employs a variety of data center operations and security best practices to bolster security.

AMONG THEM:

+ **A vulnerability and patch management program to ensure security vulnerabilities are identified, scored, and remediated**
+ **Multiple third-party threat intelligence services to help make risk-based decisions and prioritize patching and vulnerability management**
+ **All new systems and any systems with significant changes scanned before going into the production environment**
+ **An internal audit organization utilizing CISA certified staff with ISO-19011 as the reference architecture for the planning, conducting, and reporting of the internal audit program**
+ **A vendor due diligence program**
+ **Risk-based business continuity and disaster recovery (BC/DR) plan that includes multiple live tests each year, follow-up action item review, and reporting**
+ **Multi-faceted, frequent employee training in all US Signal policies, including for information security and data protection**

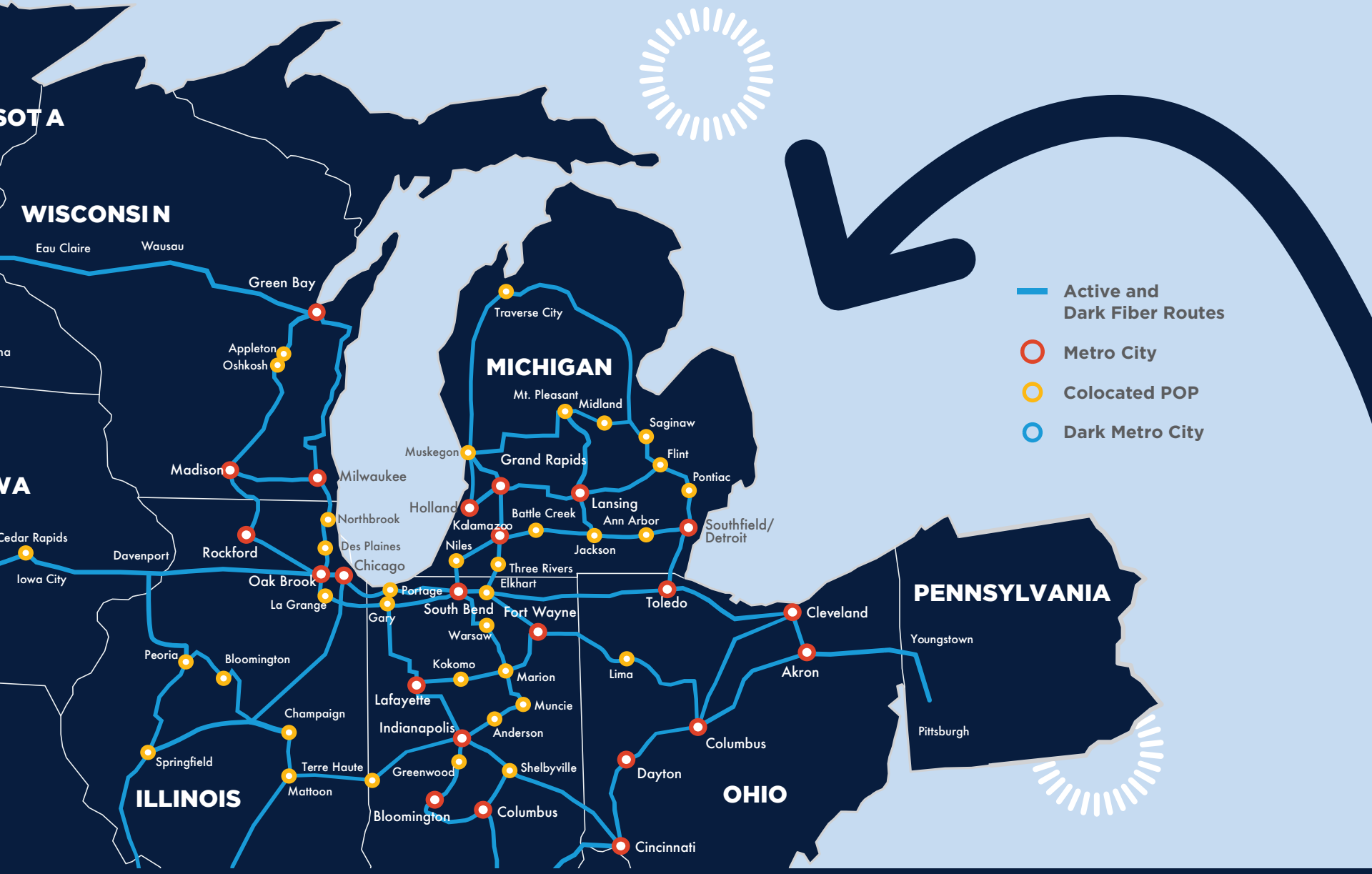
There's also a full range of policies in place to further ensure top-notch security, such as:

+ **Access to US Signal systems based on the employee position to ensure only the access needed for the position is granted**
+ **Shared accounts prohibited, administrator-level account use is limited, and all administrator accounts are monitored for anomaly by US Signal's SIEM**
+ **Employee termination procedures are in place to remove logical and physical access**
+ **US Signal-owned assets recovered at the time of employee separation from US Signal**
+ **All access changes tracked and documented within US Signal's IT trouble ticket system, providing an audit trail for access activity**

US SIGNAL®

BOOST YOUR SECURITY

Work with US Signal's security experts to develop or refine information security policies and procedures that meet your organization's business objectives, fit within its culture and address current and emerging threats.



www.ussignal.com | 866.274.4625

US SIGNAL®