HUGHES®
An EchoStar Company

SOLUTIONSHEET

Securing Enterprise Networks Today

With the Right Mix of Hughes Services, Support and Protection, Your Network's Security Can Become a Key Competitive Advantage

Every day there are an estimated 2,200 attempted cyberattacks—one every 39 seconds.[1] These attacks come with a hefty price tag. They prompt fines and penalties. They cause customers to lose trust. They damage a company's reputation. In fact, one in four Americans won't do business with data-breached companies.[2]

The result? According to Cybercrime Magazine, 60 percent of small companies go out of business within six months of falling victim to a data breach or cyber attack.[3]

So it's no wonder cybersecurity is top-of-mind for businesses of every type—from enterprises running distributed networks to small operations that rely on the internet for revenue. In mitigating cyber threats, leaders across such functions as IT, security and operations, must walk a very fine line: protect the business against bad actors and malware without greatly constraining business operations. Additionally, businesses must be ever vigilant. Cybersecurity is a constant effort; it's not a "one and done" proposition.

The good news is that for enterprises willing to take initiative in the battle against inventive and relentless adversaries, Hughes can guide the way to the right mix of services, support and protection to mitigate top cybersecurity risks and give the business a competitive edge.

What Are Your Cybersecurity Pain Points?

While all organizations are at risk for cyberattacks, individual vulnerabilities and pain points differ widely. Enterprises also typically encounter multiple challenges.

You may recognize your own enterprise in these scenarios:

- **Size** — The large distributed enterprise with multiple locations may find it difficult to manage and monitor activities at individual sites. For example, a franchise operation may have a store manager who installs a new connected device, like a camera, that creates vulnerabilities for the entire network.
- **Lack of resources** — The small to medium sized business with few resources and no IT team may focus on getting new employees set up with their equipment, usernames and passwords, and troubleshooting network issues, but may not have the expertise, tools or time to keep up with today's aggressively evolving threat landscape.
- **Connected devices** — Regardless of whether it's installing a new digital screen or deploying mobile tablets company wide, each time an enterprise increases the number of devices joining the network, the threat landscape expands.
- **Network service providers** — A regional or national enterprise that relies on a variety (even hundreds) of different service providers and vendors to support its network, may struggle to know whether all of them are keeping their own networks secure.
- **Third-party providers** — An organization that works with a variety of third-parties—either service providers or 1099 contractors—who collaborate online and in the Cloud, may inadvertently create a distributed network containing multiple vulnerabilities.

1 www.nstec.com/network-security/cybersecurity/how-often-cybersecurity-attacks-occur/
2 https://www.zdnet.com/article/one-in-four-americans-wont-do-business-with-data-breached-companies/
3 https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/#:~:text=In%20fact%2C%2060%20per-cent%20of,data%20breach%20or%20cyber%20attack

- **Remote workers** — An enterprise that supports remote workers or a hybrid environment must be able to ensure its network is safe and secure, regardless of where employees access it.
- **Cloud-based operations** — The business with Cloud-based operations, or that is considering a full shift to the Cloud, must be able to confirm that all interactions, data, personally identifiable information (PII), intellectual property, and daily transactions remain safe and secure. A business may not understand how to fully protect itself in this new paradigm.
- **IT team stretched too thin** — IT and security teams often find themselves overwhelmed by keeping pace with highly sophisticated and everchanging cyber-attacks, like ransomware. Understanding the latest security technologies as well as hiring and retaining in-demand professionals compound the problem. An enterprise with an IT team that gets bogged down with security activities may find itself unable to focus on other equally important digital initiatives to benefit the business.
- **The breached business** — The organization that has already suffered a data breach may find it hard to recover from lost sales, opportunities, and trust, as well as a tarnished brand.

What Can You Do?

Assuming your enterprise is facing one or more of these pain points, how should you proceed? First, think about network security in three layers: people, process, and technology.

Your People: While your people are critical to ensuring network security, they can also increase your risk. They may click on phishing emails, or give hackers the opportunity to access back office systems. Once that happens and ransomware is installed, hackers can shut down your business until the ransom is paid. Teach your employees about how to identify and avoid such attacks. Then, repeat (and update) training so they can stay vigilant and informed.

Your Processes: Next is process. Review all operational procedures. Who has direct or remote access to back office and Point-of-Sale (POS) systems? Do employees insert thumb drives or media devices into workstations? Who installs cameras or other Internet of Things (IoT) devices to the network? Many businesses are vulnerable because they haven't defined or enforced security-minded processes.

Your Technology: Finally, consider your technology profile. We've gone from simple, closed, private networks that process credit card transactions and conduct overnight polling of daily sales, to open networks with an array of Cloud applications and IoT-enabled services. Moving from a closed to open environment requires a much broader portfolio of network security services, for example transitioning from basic firewalls to Unified Threat Management (UTM). Today, it's essential to have anti-malware, Intrusion Detection Services (IDS), Intrusion Prevention Services (IPS), Web content filtering, and in many cases Security Information and Event Management or SIEM services. It's no longer enough to just detect attacks, you must also be able to respond to them in near real-time.

Use Cybersecurity Frameworks to Guide Your Efforts

When you understand the need to safeguard all three layers, you can then use a cybersecurity framework to dictate routine activities. The National Institutes of Science & Technology (NIST) has developed a framework that every organization, of any size, should consult.

1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

The NIST Cybersecurity Framework

Are You PCI-Compliant?

Another important framework for any retailer or business processing credit card transactions is to ensure Payment Card Industry (PCI) compliance which governs the protection of payment data. In the event of a breach, if your network is not PCI compliant, you will be responsible for any resulting losses. PCI was designed with 6 goals in mind:

Goal 1: Build and maintain a secure network.

Goal 2: Protect cardholder data.

Goal 3: Maintain a vulnerability management program.

Goal 4: Implement strong access control measures.

Goal 5: Regularly monitor and test networks.

Goal 6: Maintain an information security policy.

Together, these goals provide the structure for how to keep transactions and customer data secure. While achieving PCI compliance is a good starting point, it's not a final destination. As threats evolve, you must continue to do all you can to protect your business.

What Are Your Options?

Seeking solutions requires you to assess whether your organization has the skills, resources, and expertise in-house to adequately secure your network and protect the business. Not just as it exists today, but also tomorrow and 5 years from now—no matter the threat landscape or the number of employees and connected devices you may have.

Some enterprises invest in and build their own dedicated Security Operations Center (SOC). For many however, that strategy is cost-prohibitive because it involves millions of dollars to stand up and operate annually. That's where a Managed Security Service Provider (MSSP) like Hughes can help. An MSSP provides outsourced monitoring and management of security devices and systems, along with managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services.

By considering the three layers, a proper framework, and existing resources and capabilities, you can then explore the level of support you may need from an MSSP.

How Can Hughes Help?

As an MSSP, Hughes can augment your existing IT/security staff by providing expertise, resources, capabilities, and technologies to improve your security operations and enable your team to stay atop emerging threats. Hughes also runs a robust security operations center (SOC) to protect our customers' networks. The Hughes SOC has a full array of best-of-breed cybersecurity technologies, including detection and response, antivirus, anti-malware, and sandboxing.

Given the scarcity of cybersecurity experts in the market, Hughes is more likely to have a deep bench of expertise and a wider range of highly skilled professionals than a commercial enterprise can maintain. The fact is, while AI, ML and automation are important defense weapons, knowledgeable humans are essential. They study alerts and make important decisions to protect the network.

Key Hughes MSSP Advantages:

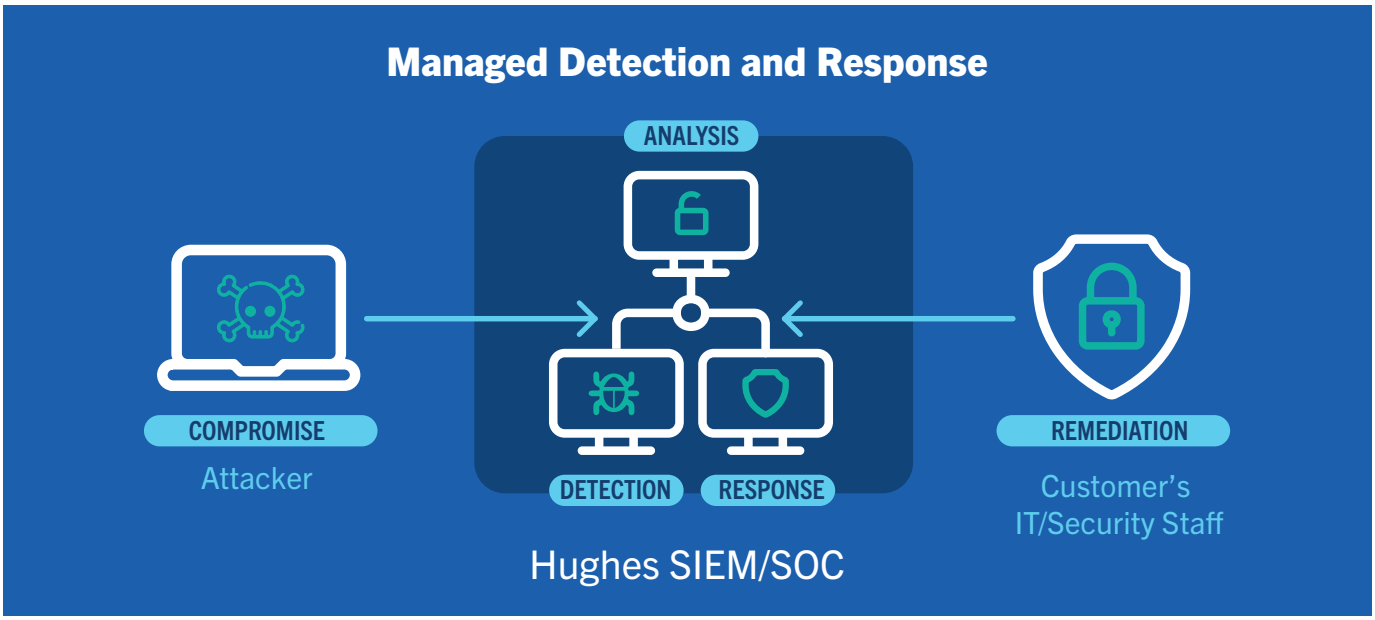
- Enables you to take advantage of industry-leading security technology, processes, and experts without the costly investment
- Ensures you stay protected against the latest threats
- Protects your business if attackers ever get past your firewall or antivirus tools
- Complements your IT/Security team capabilities
- Reduces alert-fatigue and false positives
- Supports compliance and reporting efforts
- Delivers peace of mind from knowing our next-generation SOC is ISO-certified
- Allows you to leverage over four decades of managed services expertise delivered to Fortune 1000 companies

The Cornerstone of Our Offerings: the Hughes MDR Service

The Hughes Managed Detection and Response (MDR) service keeps cybercriminals at bay with proactive intervention, real-time incident response, and threat containment. You can enjoy peace of mind knowing that Hughes deploys the right technology, processes, and people to help you prevent, detect and respond to cyber threats across your enterprise network and endpoint devices.

By 2025, 50% of organizations will be using MDR services for threat monitoring, detection, and response functions that offer threat containment and mitigation capabilities.

Gartner: Market Guide for Managed Detection and Response Services, October 2021



Further Strengthening Your Security Posture

Hughes also offers additional services to further strengthen your security capabilities and posture.

Managed Firewall Service: Designed specifically to help retailers meet stringent and ever-changing Payment Card Industry (PCI) requirements. Our firewall serves as the key component for allowing in "good" traffic and filtering out "bad" traffic to the network. Often, enterprises fail to conduct proper configuration changes and update security policies, both of which can lead to firewall breaches. With Hughes Managed Firewall Service, we proactively administer the required firewall security policies and procedures and update these policies consistently and dynamically. Hughes service experts also leverage firewall security and administer LAN segmentation to better protect a network.

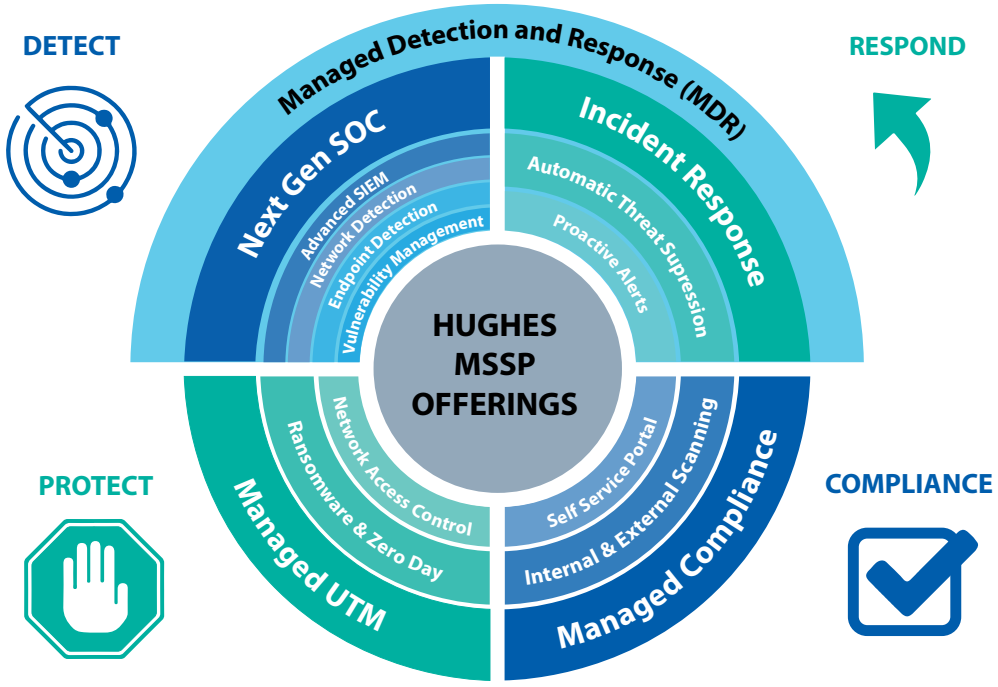
Managed Content Filtering: The coverage and benefits of our standard service with strategic control over the end user Internet experience. With content filtering, an enterprise can reduce the legal liabilities associated with its Guest Wi-Fi services by blocking access to objectionable or copyrighted content. An enterprise may also improve employee productivity by limiting access to nonbusiness related sites or by blocking access to bandwidth-intensive content, such as streaming media. In addition to supporting site-specific access control policies, Hughes also supports filtering based on the type of Web content. A customer may also provide a list of sites to be accessed and blocked. Hughes routinely reports on those sites that have been blocked and those being accessed most often. These reports are stored on the Hughes Network Management Portal (NMP), which is easy for customers to access so they can stay informed regarding content filtering or request changes. With Hughes' Managed Content Filtering, you can gain improved network protection through total control over guest and employee Internet access.

Managed Unified Threat Management (UTM) Service: Adds intrusion detection capabilities as well as antivirus/antimalware to our managed content filtering services. As with all Hughes Security service options, Managed UTM delivers a fully managed security offering that is integrated across an organization's entire network to guard against threats. The intrusion detection system monitors data packets and generates an alarm when suspicious attacks are detected, enabling swifter response times. The antivirus/ antimalware system also generates alarms when malformed packets are detected on the network. Managed UTM Services can also be customized, delivering scalability and reliability along with flexible reporting capabilities, with reports being posted on the Hughes Network Management Portal. Ultimately, it's a cost-effective solution for managing all phases and aspects of security: network deployment, configuration, network operations, and fault management.

Managed Security Information and Event Management (SIEM): An add-on to our Managed UTM service, this option provides a Web-based security dashboard and daily security log reviews for critical and high severity events that could be malicious in nature or require action to correct a weakness. This level of service also includes the option for Endpoint Detection and Response (EDR) agents that can help protect and monitor activity on endpoints such as corporate laptops or mobile devices. With this powerful tool, the customer's SOC team can now react more quickly to important security events, perform root cause analysis, and better plot a path forward through mitigation remediation of threats. Paired with the HughesON 24/7/365 intelligent security alerts and a daily security report compiled by a Hughes Security Analyst, the Managed SIEM Service brings the power of an expensive fully fledged on-prem SIEM platforms without the cost or hassle.

Managed SIEM with Incident Response (IR): Building on the Managed SIEM Service, Managed SIEM with IR adds a unique SLA-based Incident Response capability, providing support via the Hughes Security Operation Center (SOC). This SOC as a Service (SOCaaS) model delivers expertise in security, networking, operating environments and storage technologies, as well as advanced skills in consulting, integration, and managed services. These can be applied to augment existing security capabilities; create customized security services to meet specific or emerging demands; and perform day-to-day operational tasks to further reduce risks, such as analyzing and reporting on potential threat activity 24/7/365. At the center of this service is also the Hughes On-Demand Remote Network Lock-Down tool, which allows a customer to promptly request a temporary lockdown of any network segment, as a mitigation measure against further dissemination of a suspected or identified threat in the customer's internal network. With Incident Response service, the customer can expedite their mitigation measures and reduce overall exposure.

Get Started with Hughes



As a global leader in Managed Network Services, Hughes cybersecurity offerings are designed to not only protect your network, but also your business. Our experts are eager to learn about your current security pain points and your goals. We can then assess your needs and propose the right mix of services and support to mitigate cybersecurity risks—so your network is no longer a liability but a competitive edge.

Managed SASE

As businesses continue to adopt cloud and edge computing, traditional security models are being challenged. The history of security architecture in enterprises was built around the data center, with a well-defined perimeter and the firewall as the most important central security control point. But with the rise of cloud computing and the migration of workloads outside the data center, the role of the firewall has become less important. Enterprises are now subscribing to more than 800 software-as-a-service (SaaS) applications, and the COVID-19 pandemic has accelerated the trend of working from anywhere. As a result, more people, devices, applications, services, and data are leaving the confines of the enterprise data center.

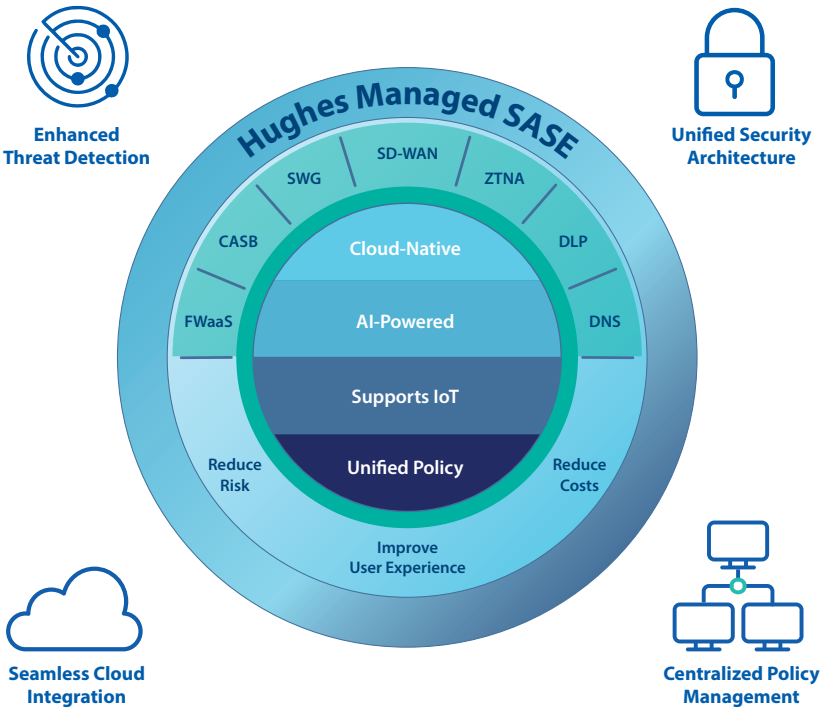
In the pre-cloud era, securing the network was the most important aspect of enterprise security, and the data center was a single location where a company housed its valuable digital assets. However, in the cloud era, the data center is no longer the center of enterprise security, and the fastest growing threats are in the cloud, not in the data center.

The result is that enterprises need to shift their security focus from securing the network to securing the data and following it wherever it goes.

The limitations of point products are also becoming more apparent. In the traditional security model, businesses adopted security designed to thwart individual threats or categories of threats as they emerged. However, in the cloud era, there are too many threats of different types to keep up with using point products. Instead, security needs to be integrated and follow the data, and security tools need to work together to provide a cohesive security solution.

This is where Secure Access Service Edge (SASE) comes into play. SASE is a security architecture that provides services at the edge of the network—closer to where the data and users are located. SASE brings security closer to the data, which is critical in a cloud-first world where the data is no longer confined to the enterprise data center. With SASE, security services are delivered as a cloud-native service, which means that they are scalable, flexible, and easy to manage.

SASE is a comprehensive approach to cloud-based security that takes into account the unique challenges and opportunities presented by the cloud. Proper SASE differentiates between corporate, personal, and third-party applications or services; and uses that awareness to initiate the appropriate connections necessary to protect each application or service in accordance with policy. This approach assesses context, adjusting access based on factors such as device, location, and behavior, and imposes policies to prevent data from being lost or leaked. It also offers continuous monitoring and can trigger alerts or advisories when necessary.



SASE is powered by shared services, which allows all high-level security functions, including Data Loss Prevention (DLP), threat awareness and neutralization, Digital Experience Management (DEM), and others, to tap any or all of the services and techniques that are part of SASE. These shared services include shared context, which includes a massive collection of metadata that identifies the person, device, and location as well as the destination website, application, or service, and its activities. This contextual landscape informs of the actions taken and policies enforced by all SASE elements.

Another important shared service is continuous adaptive trust, which allows data and application access to be flexible based on changing requirements and contexts. Proper SASE aligns the amount of trust with the value of the assets being accessed, guided by the vast wealth of contextual signals available and the organization's appetite for risk as dictated by policy. This approach is a significant departure from the thousands of rules that typically populate firewalls.

Policy-based administration is also a key shared service that enables organizations to establish the boundaries of their risk tolerance and clearly define expected security outcomes. This framework allows SASE components to control activities and data across all applications, application categories, and web services.

The capabilities of SASE are many and varied. The most important key components agreed upon by experts and are included in Hughes Managed SASE:

- Firewall-as-a-Service (FWaaS)
- Cloud Access Security Broker (CASB)
- Secure Web Gateways (SWG)
- Zero Trust Network Access (ZTNA)
- Software Defined Wide-Area Network (SD-WAN)

SASE aims to enable people and businesses to connect and work as quickly and securely as possible by functioning everywhere, which means that it can follow data, applications, and people that have moved to the cloud. SASE addresses cloud-enabled threats and data risks for personal instances of managed applications, thousands of shadow IT applications, and cloud services.

ZTNA is a key component of SASE that enforces the premise that no one is blindly trusted and allowed to access company assets until they've been validated as legitimate and authorized. It supports the implementation of least privilege access, which selectively grants access only to resources that people or groups of people require, nothing more. By giving ZTNA adaptive access capability, SASE boosts ZTNA and harmonizes policy administration and decision with other SSE components while still maintaining distributed policy enforcement.

SASE is a comprehensive approach to cloud-based security that offers many benefits to organizations. By using shared services to power high-level security functions and providing continuous monitoring, policy-based administration, and adaptive access capability, SASE can help organizations stay ahead of cloud-based threats and protect their sensitive data and applications.

Call for a free consultation: 888-440-7126 or learn more at www.Hughes.com/cybersecurity

HUGHES
An EchoStar Company
11717 Exploration Lane Germantown, MD 20876 USA
www.hughes.com