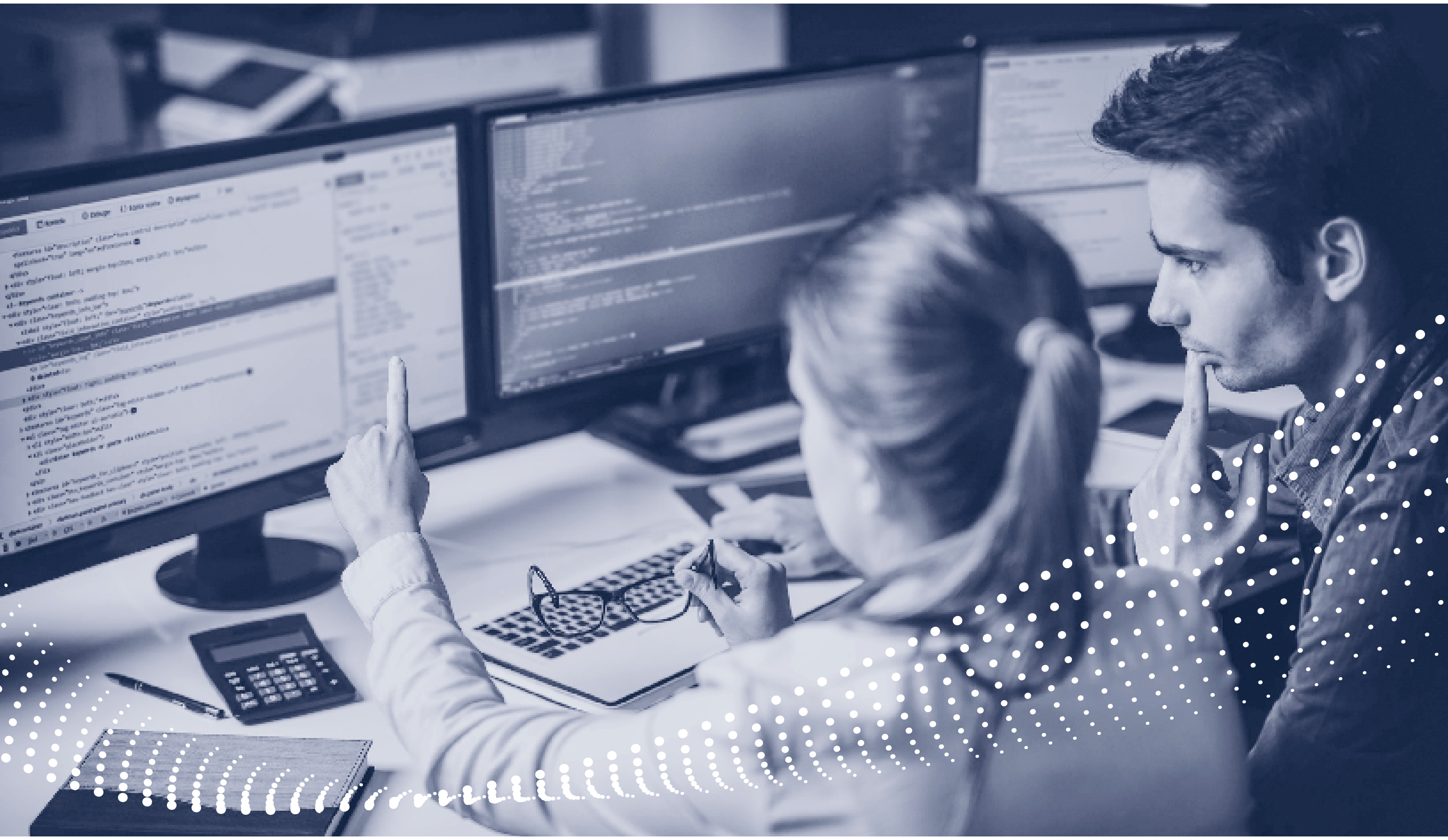
TechTarget | Custom Media
White Paper

HUGHES®
An EchoStar Company

TAKING INITIATIVE IN CYBERSECURITY

An MNSP with the full security stack can keep you a step ahead of the bad actors.



INTRODUCTION

Cybersecurity is a top priority for most companies, yet successful attacks continue unabated. The reason comes down to strategy: Many companies are stuck playing reactive defense, a losing battle against adversaries that are inventive and relentless. To take the initiative, many organizations are turning to a managed network service provider (MNSP) capable of delivering the entire cybersecurity stack, including people, processes and technology.

Cybersecurity challenges

Supply-chain attacks, in which routine software updates are seeded with malware, are the latest in a wave of threats that include phishing, social engineering and internet of things (IoT)-based denial-of-service attacks. Ransomware attacks, which can be initiated through multiple vectors, regularly generate hefty payments from businesses and government agencies to unlock precious data.

As organizations implement digital business initiatives that enlarge their attack surface, protecting data becomes more difficult. Cloud-based applications, IoT data and the surge of remote workers in the recent COVID-19 pandemic—all pose distinct cybersecurity challenges, making piecemeal cybersecurity measures increasingly untenable.

The constant morphing of threats into more numerous and sophisticated forms in the hands of hackers and cybercriminals with plenty of knowledge and patience, presents businesses with still more difficulty. As the bar is raised by bad actors, organizations must enlarge their expertise to keep pace. Specialists with up-to-date knowledge of threats and how to thwart them are indispensable in any cyberdefense strategy, but these experts are hard to find, expensive to hire and difficult to keep. According to ZipRecruiter, a cybersecurity specialist in the U. S. is paid on average $111,052 annually.[1] According to CyberSeek, the U.S. has 464,420 unfilled cybersecurity positions, out of a total cybersecurity workforce of 956,341.[2] Globally, there are an estimated 3.5 million unfilled cybersecurity jobs.[3] With such a talent shortage, playing defense against adversaries with extensive expertise and dogged persistence is unlikely to succeed.

Taking the initiative

IT leaders should implement an integrated and automated defense. They should set aside ad hoc, disconnected countermeasures in favor of a strategy that links clear cybersecurity goals with workable tactics to achieve them. Focus should be on these four areas:

1. **Superior customer experience.** In the era of e-business, customers expect a responsive, feature-rich website that is always available. Product data must be timely and accessible; transactions must execute rapidly and reliably; above all, the data of the customers themselves must be protected.
2. **Compliance.** Financial services firms and retailers are used to implementing technology and processes the meet PCI-DSS guidelines; healthcare organizations must protect patient information in conformance with HIPAA rules. With the advent of GDPR requirements, any organization doing business in Europe must protect the personally identifiable information (PII) of EU citizens. Numerous state regulations, such as the California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), and the Virginia Consumer Data Protection Act (CDPA), are leading indicators for a future federal law safeguarding consumer PII.
3. **Employee productivity.** Cybersecurity measures must be seamless to employees and implemented with top-down governance. Otherwise, barriers to data access, slow performance, or complex processes are likely to be bypassed by employees and executives by standing up new systems and services without telling cybersecurity staff.
4. **Controlling cost.** Every cybersecurity initiative must balance the risks posed by threats with the corporate mission and budget requirements of an organization. Cybersecurity measures must be economical as well as effective so that an organization can attain its profitability objectives.
5. **Evolving defense posture.** Cybersecurity defense must stay ahead of continually evolving threats. The new PCI DSS v4.0, which is expected to be released in mid-2021, will enable Qualified Security Assessors to take a more flexible, risk-based approach in evaluating the compliance of security controls and will specifically focus on authentication and encryption, while imposing stricter requirements for monitoring and testing.

[1] "Cyber Security Specialist Salary," ZipRecruiter.com, April 22, 2021.

[2] "Cybersecurity Supply/Demand Heat Map," CyberSeek.org, 2021.

[3] "Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021," Cybercrime Magazine, Oct. 24, 2019.

Choosing the right MNSP: Multi-layered protection

The people, processes and technology delivered by a full-stack MNSP such as Hughes includes multiple layers that work together to blunt the most sophisticated attacks.

- **Skilled cybersecurity specialists.** A large, established MNSP such as Hughes is much better able to hire and retain the cybersecurity talent required to keep pace with evolving threats. Specialists with specific areas of expertise are assigned to customers with corresponding needs. Thanks to greater scale, a large MNSP can spread its cost over multiple customers -- and apply knowledge gained while protecting one customer to the protection of others.

- **Zero-trust expertise.** Zero-trust cybersecurity strategies have attracted significant mindshare in recent years. Yet not all organizations are a good fit for zero-trust, which can be complex to implement. A zero-trust approach assumes that the network perimeter has been penetrated, and even trusted employees and business partners might have been compromised. Zero-trust implementation requires micro-segmentation of network and data center infrastructure, end-point security including multi-factor authentication and highly granular access permissions. Zero-trust also includes security automation and orchestration involving a diverse array of complementary cybersecurity tools, managed from a single pane of glass. Zero-trust methods and technologies must be implemented with care so as not to inhibit employees' access to the data and applications they need to work productively.

- **Ransomware avoidance and recovery.** Although ransomware attacks are ubiquitous, careful maintenance of complete, accessible backups can protect an organization from joining the long list of victims. By deploying agents to end-user systems whether on-site or remote, organizations can initiate regular backups, whether locally, at a central site, or at a remote backup facility. An MNSP can assist in implementing backup technology, by allocating sufficient network bandwidth to backup traffic and by implementing post-attack recovery procedures. EDR technology detects applications performing cryptographic functions on a file system, blocks them and allows the encryption to be reverted.

- **Managed firewall services.** The firewall is a cornerstone of cybersecurity in the era of the internet. Next-generation firewalls encompass an increasing array of unified threat management (UTM) capabilities, including:
    - **Intrusion detection systems (IDS) and Intrusion prevention systems (IPS).** IDS and IPS work together to monitor a network for malicious activity, report intrusions to a central point of administration and respond to detected intrusions by taking action via the firewall to stop the attack and prevent future intrusions.
    - **Content filtering.** The ability to identify and isolate specific types of content, such as obscene images and gaming apps that might contain malware.
    - **Unified management.** An MNSP may provide a single point for an administrator to manage multiple cyber defense tools, including those from different vendors.
- **Artificial Intelligence (AI), Machine Learning (ML).** AI and ML tools can recognize recurring patterns in data to detect anomalies and predict where breaches might occur in the future. AI and ML lighten the analytical workload of cybersecurity staff while shifting an organization's cybersecurity stance from reactive to pro-active.
- **Security Information and Event Management (SIEM).** A SIEM provides a central point to aggregate and view cybersecurity information. A SIEM is an integral part of **managed detection and response (MDR)** services, which unite threat intelligence, analytics and expert knowledge. The MDR is an overall managed response service based on alerts that are curated by the SIEM utilizing AI. **Endpoint detection and response (EDR)** tools monitor and collect endpoint data, subjecting it to rules-based response and analysis. The SIEM analyzes data from these and other sources to spot possible breaches and rank events in order of importance.
- **Best-of-breed technology.** By acquiring and combining industry-leading technology from strategic partners, an MNSP such as Hughes takes on responsibility for selection and integration that would otherwise fall to overworked cybersecurity staff.

> Because organizations are faced with a broad range of threats targeting many different points of their infrastructure, a cybersecurity strategy must be comprehensive. A single vulnerability, no matter how small, can be exploited to jeopardize an entire company as well as its customers and trading partners.

Conclusion

Because organizations are faced with a broad range of threats targeting many different points of their infrastructure, a cybersecurity strategy must be comprehensive. A single vulnerability, no matter how small, can be exploited to jeopardize an entire company as well as its customers and trading partners. However, implementing multiple point products places an unwanted burden on an organization's cybersecurity staff to deploy, maintain and manage, often leading to finger-pointing between the staff and various vendors.

To emerge from a legacy defensive posture and take the cybersecurity initiative, it makes sense to choose an MNSP such as Hughes that delivers the entire security stack, implementing multi-layered technologies to provide seamless protection. With 50 years of experience, Hughes delivers a comprehensive managed cybersecurity solution to over 300,000 enterprise locations globally that is integrated with connectivity and business network technologies to achieve maximum data protection.

For more information, please refer to
https://business.hughes.com/sd-wan-networking/managed-security

HUGHES®
An EchoStar Company

11717 Exploration Lane
Germantown, MD 20876 USA

For additional information, please call 1-888-440-7126 or visit business.hughes.com.

This content was commissioned by Hughes and produced by TechTarget Inc.