HUGHES®
An EchoStar Company

CYBERSECURITY PRACTICES FOR EVERY TYPE OF ENTERPRISE

INTRODUCTION

In a recap of Cybersecurity Trends & Statistics for 2023, Forbes Magazine noted ominously that there is “more treachery and risk ahead as attack surface and hacker capabilities grow.” Every company, large or small, the author stressed, is now a reachable target with its brand, reputation, and revenue pipeline at risk from a breach.

So how does a business––particularly a small to medium sized enterprise––contend with sizeable cyber risks and threats?

Today’s cybersecurity options go far beyond the firewall to ensure that businesses can withstand the evolution of cybercrime–in other words, keep up with how quickly attackers’ capabilities change and grow. These solutions take a more proactive approach to threat detection and response and reduce the time and resources required to manage threats. Ultimately, they enable enterprises to focus on their core business objectives.

In this ebook, we look at cybersecurity from every angle and every perspective. We explore strategies and technologies, like Managed Detection and Response (MDR) and Zero Trust; provide tips for enterprises of all sizes; and summarize the advantages of using a multi-vendor Managed Security Services Provider (MSSP) to protect the network.

MDR, EDR, and XDR… What's the Difference?

There are a variety of mitigation techniques and technologies, including Managed Detection and Response (MDR), Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR). Each can function both independently and collectively to prevent cybersecurity breaches.

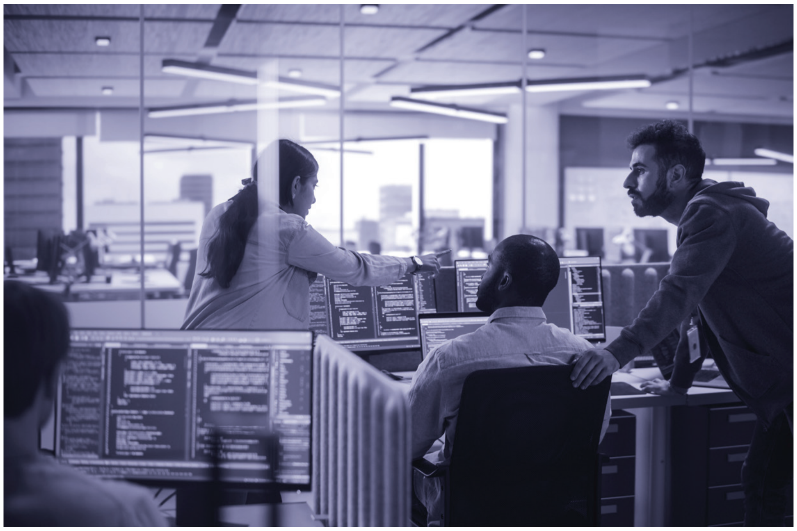
Here's how:

- MDR service provides a business with a team of experts who use advanced analytics and machine learning (ML) algorithms to actively monitor the network. The team monitors cloud environments, network traffic and endpoints; identifies potential security threats; and takes action to mitigate those risks. The goal is to detect and respond to threats swiftly, before they can cause harm. Small to medium sized businesses unable to hire and retain cyber professionals to support MDR or whose team struggles to keep up with monitoring activities, can have MDR implemented by a Managed Security Service Provider (MSSP) equipped with a 24/7 Security Operations Center, or SOC.

- EDR focuses specifically on endpoint devices and is a core component of MDR. In fact, no MDR solution is complete without EDR. Endpoint devices on a network include all the servers, desktops, laptops, smartphones, cameras, scanners, and other devices. EDR uses advanced analytics and ML to detect and respond to threats in real-time, providing in-depth visibility into endpoint activities and threats that may evade traditional antivirus solutions. EDR still requires manual intervention (typically from a team of SOC analysts) to investigate and remediate threats.

- XDR can be seen as another version of MDR that relies more on artificial intelligence (AI) and ML and less on a hands-on approach. Advanced threat hunting typically reduces the need for human intervention and the "managing" of threats.

One of the significant advantages of MDR and XDR solutions is that they integrate data from multiple sources, providing a more comprehensive view of security across the entire organization. This integration of data allows security teams to detect and respond to threats that may have gone undetected using other methods. It also helps to reduce the number of false positives and negatives, leading to faster and more accurate detection and response.



Understanding the Zero Trust Strategy

Zero Trust is a security framework requiring all users, whether in or outside an organization's network, to be authenticated before being granted access to applications and data. The intent behind Zero Trust is to no longer assume that the network is the ultimate source of trust. Rather, just because someone or something is on the network doesn't mean they can be trusted: even the network itself cannot be trusted.

But what does it mean to be "trusted?" And what characteristics denote that something or someone is not worthy of trust? These are the big questions under consideration right now.

With Zero Trust, only a person's validated identity determines access. If the security structure is based on identity, then access can be granted wherever the user may be. If there is question or doubt, more identity confirmation tests can be applied to increase confidence.

Over the last few years, we've all been introduced to Zero Trust strategies by banking and financial apps that apply multi-factor authentication, including biometrics (the use of our faces or fingerprints for identity verification), location, patterns of use and more. Military and government organizations have additional verification options at the ready. They can leverage backend credentials such as device information, time zones, tokens (like Common Access Cards and others) and IP addresses––details that come together to build an even higher degree of trust and confirm "you are who you say you are."

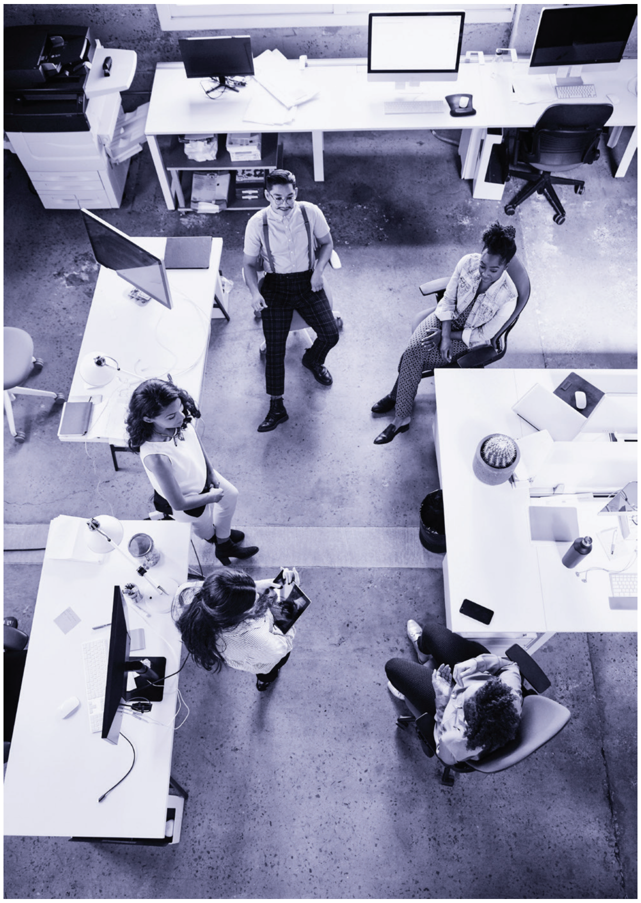
Yet, deploying Zero Trust across dynamic, global environments has far reaching implications. While Zero Trust ensures security, it also creates friction––which can affect time and efficiency. Any identity verification solution deployed cannot be so cumbersome that it impedes mission readiness or prompts users to circumvent the process altogether.

All of this is to say, Zero Trust is a philosophy that provides a structure, but not a checklist. As such, it is not bound by a specific technology; it offers inherent flexibility to accommodate innovation and change.

Tips for Every Organization

While there are many different approaches to network security, every enterprise—regardless of size, shape or structure—will likely find one or more of the following tips worthwhile.

- **Strike a balance between "Security" and "Access."** Network security, by its very nature, adds friction to the user experience. It slows things down. Think of the extra time it takes for an authorization code to filter into your email with two-factor authentication. Unfortunately, too much friction can prompt employees to find workarounds or for customers to abandon the sales process altogether. For those reasons, businesses need to carefully consider the balance between protecting their networks and providing a relatively positive (or merely neutral) experience when it comes to accessing the network.



- **Train employees on good security practices and hygiene.** Network security is only as "good" and effective as peoples' behaviors and actions––that includes those of C-suite executives as well as frontline employees. In fact, in Cybersecurity's Greatest Insider Threat Is In The C-Suite, Forbes noted that 78% of IT leaders say the C-Suite is the most likely to be targeted by phishing attacks. Providing purposeful security training to every employee and subcontractor can mitigate those risks.

- **Join InfraGard**, a partnership between the Federal Bureau of Investigation (FBI) and members of the private and public sectors. InfraGard provides education, information and workshops on emerging technologies and threats so enterprises can stay well-informed. Members include business executives, entrepreneurs, lawyers, security personnel, military and government officials, IT professionals, academia and state and local law enforcement—all dedicated to contributing industry-specific insight and advancing national security.

- **Scrutinize the Point of Sale (POS) system.** POS systems have evolved far beyond transaction engines. Today, they integrate with innovative third-party through APIs, like the online order and delivery platforms, and with back-office software and enterprise applications. They can be connected to smart devices, like product scanners, speakers, cameras and lighting. Many also support the digital guest experience, be it mobile app ordering or having tablets at tables. Regardless of the specifics, every device and endpoint on the POS increases breach risk for an enterprise––which means each of these endpoints need to be protected to reduce these risks.

- **Recognize that technology innovation can also be adopted by hackers.** The cybersecurity threat landscape changes at warp speed. As an example, there is a groundswell of attention on how artificial intelligence (AI) is being used for nefarious activities, like the creation of deepfakes––which become more realistic each year. One prediction is that by 2025, deepfake AI "people" will enter the workforce. Having fakes or frauds in the workplace means enterprises will be at significantly higher risk for a breach initiated from inside the network. How might a business protect itself? Perhaps by having new remote workers go in person to a facility for a background check.

Why a Multi-vendor MSSP?

In cybersecurity, there are many situations where no single technology provider can meet all the needs for secure, high-performance and reliable infrastructure. Some solutions may provide outstanding threat analysis, while others provide more robust WAN optimization or high-availability solutions. Even simpler single-source architectures can be challenging for some IT groups to deploy and maintain at scale.

As a result, some enterprises resort to fixed, universal access policies to secure their networks. While that approach may provide stability due to static configurations, it can disrupt the customer and employee on-site experience. In other cases, enterprises may compromise their solution selection, choosing what they can support within their internal operational limitations rather than what they know they need. A better option is to partner with an MSSP, like Hughes, that has access to multiple market-leading technologies.

Best-of-Breed Implementations

By collaborating with the right multi-vendor MSSP, enterprise customers can implement mixed best-of-breed solutions and dramatically expand their access to proven cybersecurity technologies.

For example, in two recent deployments, Hughes found that satisfying the customer's demanding business and operational requirements required blending multiple solutions together -- instead of serving the customer with a single vendor solution, we used a combination of technologies from multiple vendors to achieve the ideal solution.

Leverage Existing Tech Investments

As cybersecurity threats continue to evolve, solution requirements must also evolve. Enterprise customers may need to transition between solutions to satisfy these new requirements. Multi-vendor MSSPs with experience managing both legacy cybersecurity solutions and new innovative technologies can expertly facilitate the operational transition from old to new. In large, distributed networks with equipment on different depreciation schedules, a multi-vendor MSSP can also provide managed services on the legacy equipment until it fully depreciates to maximize the value of the customer's prior investment.

Access to an Ecosystem of Cybersecurity Resources

The field of cybersecurity is one of constant innovation based on unrelenting creativity from bad actors and cybersecurity solution providers. Multi-vendor MSSPs have a unique insider's view into these aggregate innovation cycles due to their partnerships with the numerous technology vendors they support. This multi-dimensional perspective means the multi-vendor MSSP has the advantage of expanded market insight to accurately assess the current state and future direction of cybersecurity technology.

As enterprises become ever more digitally dependent, and hackers pose an existential threat, businesses must employ every available tool and strategy to mount an adequate defense. The multi-vendor MSSP can provide the ability to blend best-of-breed solutions, leverage existing tech debt, and access an entire ecosystem of cybersecurity resources.

Next Steps?

Wondering what your next steps might be? An MSSP can evaluate your security needs and recommend the best-fit solution to improve your cybersecurity posture and ensure that your business is protected under any circumstance. Even if you have an in-house IT team, an MSSP can complement your existing resources to improve security and enable growth. As Forbes outlined, being cyber-aware is part of the process of risk management and security; looking at the cyber-threat landscape and understanding your options enables you to see how to position the enterprise to keep pace with evolving risks and threats.

Every Path. Every Cloud. Everywhere.

A vulnerability anywhere is a risk everywhere. Hughes delivers managed cybersecurity designed to defend everywhere our clients go and every way their network grows. We plug the gaps traditional cybersecurity vendors don’t, defending every transport type, including satellite, cellular, microwave and the connections highly distributed enterprises depend on.

Hughes has been recognized in the 2022 Gartner® Magic Quadrant™ for Managed Network Services and Frost Radar: NA Managed Services reports.

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

HUGHES®
An EchoStar Company

www.hughes.com

11717 Exploration Lane
Germantown, MD 20876 USA