

Fundamentals for building a robust cybersecurity strategy

Get ahead of ever-evolving cyber threats with a foundational security approach that addresses your entire IT environment.

By **Anne Taylor**, independent technology and business writer

Cyber threats are increasing in complexity and volume. Bad actors are escalating their attacks with sophisticated techniques. A recent article on [CSO](#) highlighted some of the emerging threats, including:

- A Russian hacking group called Midnight Blizzard, which uses Microsoft Teams to carry out phishing attacks
- Data poisoning, where hackers corrupt data being used to train machine- or deep-learning models
- AI-based threats, such as bad actors launching malware packages into generative AI environments used by software developers

It's no wonder that 88% of IT security leaders believe their organizations are falling short in addressing cyber risks, according to Foundry's 2023 Security Priorities [study](#).

Most IT and security professionals already recognize that incidents are a matter of when, not if, and that they need a proactive strategy. But what should that approach include? How can you protect your organization against constantly evolving attacks when it's challenging to keep pace with what's being launched today?

There are three fundamentals that provide the basis for a robust cybersecurity strategy: education, trust, and a full-stack security approach.

Fundamental #1: Know the risks

It is easy to understand why cybersecurity and vulnerability alerts get missed. They come from dozens if not hundreds of security tools and applications. In addition to alert fatigue, the Foundry security study found that companies are struggling to address cyber risks due to:

- Difficulty convincing all or parts of their organization of risk severity
- Insufficient investment in budget, people, and technologies to address risks
- Challenges in finding, acquiring, or retaining the necessary security expertise

To be sure, these are tall hurdles. Yet, overcoming them is crucial. The global costs of cybercrime — including data destruction, fraud, theft of intellectual property, business disruption, reputational harm, restoration efforts, and more — are expected to reach \$10.5 trillion by [2025](#), according to Cybersecurity Ventures¹.

If your organization is among the 88% falling short in addressing cyber risks, Moor Insights & Strategy² [suggests](#) starting with a cyber environment assessment. Ideally, that would be conducted by an objective third party that doesn't have a stake in the results. It should give you a basis for a risk discussion with your executive team and provide a checklist of weaknesses and vulnerabilities to fix.

In terms of filling expertise gaps, there are several avenues to pursue, including working with managed services providers and retraining IT professionals who demonstrate a natural curiosity toward cybersecurity. An end-to-end stack with built-in cybersecurity functionality also goes a long way toward alleviating the burden on overstretched security teams.

Fundamental #2 - Trust is a critical ingredient

Zero trust (ZT) practices and technologies lay the foundation for baked-in security; 49% are using these technologies and another 32% are researching ZT solutions, services, and models, according to Foundry's Security Priorities study.

That said, a great deal of focus so far has been placed on securing applications and networks — making sure the right people have access to the right resources. However, it's also critical to extend trust throughout devices and computing platforms, including servers and cloud infrastructure.

There are standards and operating frameworks that can help you embed zero trust in your IT environment. For example, the National Institute of Standards and Technology Cybersecurity [Framework](#), a collaboration between industry and government, offers guidelines, standards, and best practices toward protecting critical infrastructure.

Other ZT resources include the Cybersecurity and Infrastructure Security Agency Zero Trust Maturity [Model](#), which can be used to guide toward identifying security gaps and measuring effectiveness. Another resource is the Department of Defense Zero Trust [Strategy](#), which provides advice toward implementing stringent security practices.

Moor Insights also recommends conducting an audit of your infrastructure. Attacks are increasingly targeting firmware, [such as](#) the remote installation of malware that can launch at device boot up. A June 2023 [report](#) from Moor recommends:

- Understanding which generation of servers are deployed in your organization and what levels of protection they provide
- Assessing whether the CPUs in your servers are vulnerable to side-channel attacks

¹ [Cybercrime To Cost the World \\$10.5 Trillion Annually By 2025 \(cybersecurityventures.com\)](#)

² [Moor Insights and Strategy: Zero Trust - Five Steps for Enterprise IT \(hpe.com\)](#)

- Determining if your server provider has built-in protections at the hardware and firmware levels

Finally, it's critical to trust your vendors. They should instill confidence that they too are taking a proactive approach to security.

Fundamental #3 - Full-stack security, from silicon to software

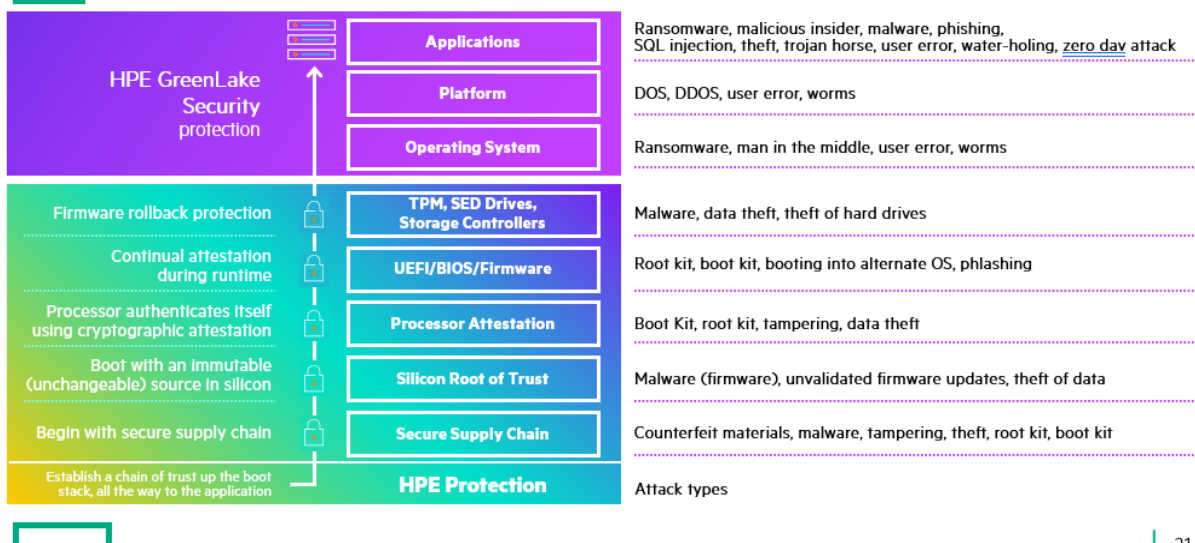
[HPE ProLiant Gen11](#) servers have been built for end-to-end proactive security. The latest generation helps defend your organization against existing cyber threats, while also providing constant security advancements for ongoing protection — from silicon to software, from factory to cloud, and from generation to generation.

“The HPE ProLiant Gen11 servers offer trusted security by design,” said Cole Humphreys, Global Server Security Product Manager at HPE. “It starts with the architecture, which includes a silicon root of trust with an embedded lights-out (iLO) chip that can detect during the server boot-up process whether any layer has been compromised or tampered with.”

In addition, HPE ProLiant servers have security protections built in throughout the layers for all attack types.

HPE hardware-based security is critical for enterprises

Your security is only as strong as the layer below the point of attack



| 21

Full-stack security is supported by innovations from within the HPE trusted partner ecosystem. For example, Intel is a Tier 1 HPE partner and together the two companies share “an uncompromising focus to deliver infrastructure that can be trusted, as well as features that provide easier security management,” [said](#) Humphreys.

HPE and Intel take a fundamental approach to security. HPE ProLiant next-gen servers are built with 4th Gen and 5th Gen Intel® Xeon® Scalable processors and security features such as Intel® Control-Flow Enforcement Technology (Intel® CET).

Intel CET is designed to mitigate an attack that Mike Ferron-Jones, Product Manager, Data Center Security Technologies at Intel calls an “evil genius.” In a recent [interview](#), he said the capability is “designed to look for existing bits of server code that it can execute in a particular order to achieve a malicious outcome, such as opening a command prompt. Intel CET disrupts those control mechanisms to prevent [compromises] from taking effect so the software behaves as the developer intended.”

It is these innovations that boost the business value of Gen11 servers, enabling customers to obtain “the combined security investments from HPE and Intel, from the ground up and including support,” Humphreys added.

The bottom line

Education, trusted security, and a full-stack approach are must-have fundamentals for a robust and proactive security strategy that delivers confidence to the business and data protection.

Find out more by visiting [HPE ProLiant](#)

Meet Guest Blogger, Anne Taylor



Anne is an independent technology and business writer with 20+ years of experience. She strategizes and creates content – including blogs, webinars, white papers, research surveys, and infographics – across a wide range of companies and industries. Her background is in both journalism and content marketing.