ZERO TRUST – FIVE STEPS FOR ENTERPRISE IT

SITUATION ANALYSIS

Although enterprise organizations are spending more on securing their most precious assets, they are more vulnerable than ever. Every day seems to bring a new cybersecurity headline, and every IT professional knows the real and present danger under which they work. Hackers are more emboldened than ever, and their job has never been easier.

Zero trust is a term that has lost some meaning due to overuse and misuse. However, the concept of an environment that operates on the least trust principle at the lowest possible levels is critical to establishing robust security. In terms of infrastructure, that means security that begins in silicon with design and materials sourcing.

Companies like HPE have worked from this design principle long before zero trust was a catchphrase. This brief will discuss enterprise IT challenges and how HPE has built a security-first culture into its product design and manufacturing, enabling IT to protect its assets proactively.

THE THREAT LANDSCAPE IS EVER CHANGING AND NEVER AS EXPECTED

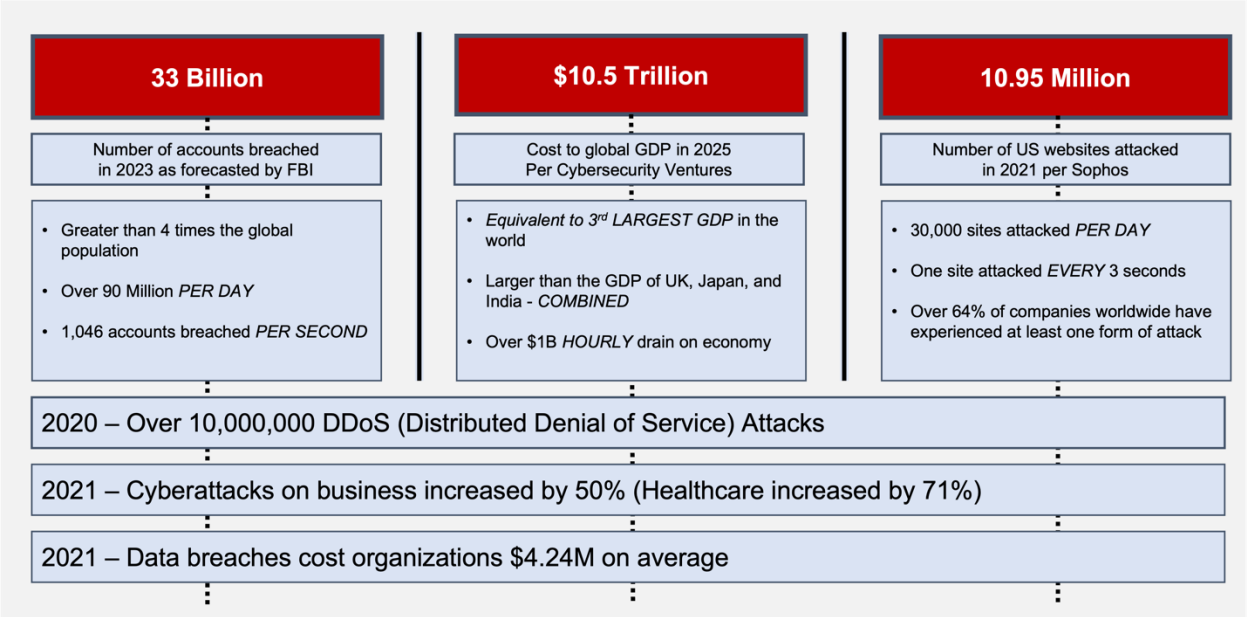
Cybercrime is a thriving business – not simply thriving but significant. In 2015, cybercrime cost the global GDP roughly $3 trillion. In 2022 that number doubled to $6 trillion. And by 2025? That number is anticipated to hit $10.5 trillion. A number so large almost seems impossible to grasp. To make that a little easier, consider this – in 2025, cybercrime will cost the global GDP $332,952 *per second.*

If these numbers seem staggering, consider the following:

- 30,000 websites attacked per day – equals an attack approximately every second
- The edge not only opens a new attack surface for hackers, but the nature of the edge introduces a whole new set of attack vectors.
- Like the edge, the cloud opens a new attack vector for enterprise IT. In 2022, some 45% of the cyberattacks originated in the cloud. This open and distributed

environment, driven by APIs that connect data and applications and open-source software, is a breeding ground for attacks.

FIGURE 1: THE DEVASTATING EFFECTS OF CYBERCRIME[1,2,3]



Source: Moor Insights & Strategy

While most understand money as a motivator for hackers, geopolitics is also another major driver of hacking. From a geopolitics perspective, nation-states dedicate budgets and resources to attacking adversaries and rivals. No other cyberattack epitomizes the geopolitical more than the 2020 US federal government data breach known as the "SolarWinds attack." This cyberattack, which lasted 8-9 months, found vulnerabilities across the software supply chain, including Microsoft, VMware, and security giant Palo Alto.

On a global basis, the average cost of a cyber breach is over $4 million. In the US, that figure jumps to $9 million. While this number is significant, the cost to reputation is perhaps more damaging for some. And smaller organizations (a new target for hackers) may never recover.

Cyberattacks are occurring at an unprecedented rate across more attack surfaces and attack vectors by nation-states, organized hacking efforts, and the unaffiliated. Hacking

[1] https://www.netscout.com/blog/asert/crossing-10-million-mark-ddos-attacks-
[2] https://www.cybersecurityintelligence.com/blog/corporate-cyber-attacks-up-50-last-year-6069.html
[3] https://www.ibm.com/downloads/cas/OJDVQGRY

has never been more vibrant or straightforward. It is its own industry, complete with as-a-Service offerings. Finding the latest rootkit is as simple as installing the Tor browser and searching the dark web.

AI Introduces Complexity and Simplicity

One must also recognize the impact of AI on cybersecurity. While there is much focus on how cybersecurity firms incorporate deep analytics and AI into products, bad actors are also using AI to create more sophisticated tools. Does this become a zero-sum game?

The other impact of AI is driving down the technical barriers some may have faced in using ransomware. Generative AI can create a Python script to perform virtually any function in seconds. It doesn't take much imagination to think about how one could use this tool to create a sophisticated DDoS or phishing attack against the unsuspecting. For example, AI/ML is being used in DDoS attacks. Using a self-learning algorithm, these automated attacks can intelligently guess what security solutions are in use and create an attack approach that exploits the weaknesses of the identified solution.

This may seem a bit hyperbolic, but unfortunately, it's not. The trends and growth Moor Insights & Strategy (MI&S) has seen on the threat landscape validate what we all feel. And the future shows no signs of easing or even stabilizing.

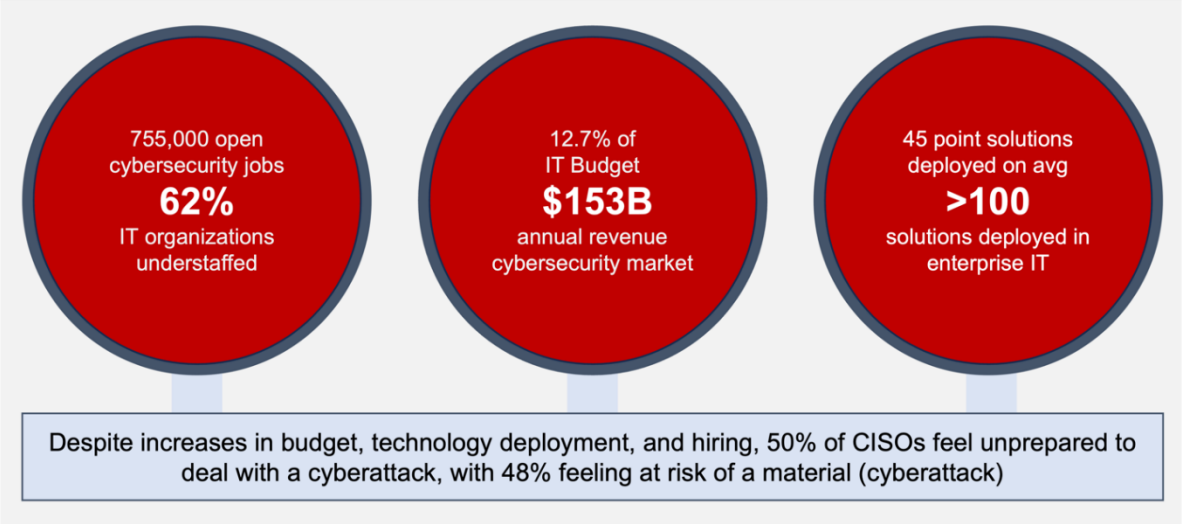
Enterprise Is More Challenged Than Ever

More Can Equal Less

In response to the ever-increasing threats, virtually every IT organization that MI&S speaks with continues to increase its cybersecurity budget – a trend that has continued for several years. In 2022, the industry saw enterprise IT allocate 12.7% of its budget to cybersecurity, resulting in a market that generated about $153 billion in revenue and is expected to grow at a 13.8% CAGR, reaching nearly $425 billion by 2030.

This budget is being spent directly responding to the ever-evolving, seemingly ever-nascent threat landscape. Enterprise IT organizations have deployed 45-point security solutions on average to combat these threats, with some reaching well over 100.

FIGURE 2: IT INVESTMENTS NOT PAYING OFF[4,5]



Source: Moor Insights & Strategy

On the human capital front, enterprise IT is equally aggressive. At the time of writing this report there are over 775,000 cybersecurity job openings in the US alone, and 68 cybersecurity professionals for every 100 jobs. In many cases, those 68 cybersecurity professionals are relatively new to the IT job market as universities and technical institutions stand up security certification programs and churn out professionals like a factory assembly line.

Despite these record investments in security, attacks are rising, the cost per attack is growing, and our most precious assets – data and infrastructure – are at risk.

In the area of cybersecurity, more is not necessarily better. Enterprise IT doesn't need more protection – it needs *better* protection. It needs security that is integrated, end-to-end and top-to-bottom. And this protection only sometimes comes about through more investment. Instead, it comes about through *smarter* investments – and from taking a step back and reorienting toward the correct to true north.

Achieving a fully secure environment is easier than we think. Sometimes the best tack is a clean-sheet mindset. MI&S believes many IT organizations can benefit from taking the proverbial step back and looking at security more holistically.

[4] https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020

[5] https://www.techrepublic.com/article/half-of-global-cisos-feel-their-organization-is-unprepared-to-deal-with-cyberattacks/

THE PATH TO A TRUSTED ENVIRONMENT

FIVE THINGS TO START YOUR JOURNEY

Zero trust isn't achieved overnight. Given the depth of this challenge, starting on the path to achieving zero trust can seem daunting and near impossible. How does an IT organization choose the right tools and integration points to ensure an air-gapped environment? Here are five things that MI&S recommends every IT organization do to get on the path to zero trust.

1. **Assess your current cyber environment** – Bring in a third party with no vested interest in the outcome to perform an unbiased assessment of your environment. Perform planned and unplanned vulnerability testing through red team/blue team exercises. Root out the weaknesses and test for susceptibility to AI-driven attacks.

   Perform a cost/function analysis. In other words, understand your spending and the real-world value of your investment. Look for redundancies in function and gaps in coverage. And try to reduce the number of cybersecurity vendors. The fewer the vendors, the simpler the deployments and the tighter the integration.

2. **Understand the standards** – Perhaps unlike any other market, cybersecurity has seen a considerable coalescing of industry players, practitioners, and regulators for better outcomes. While there are many resources available to enterprise IT, MI&S has found the following to be extremely helpful in aiding the journey to zero trust:
   a. National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 1.1. This framework for implementing standards, procedures, and technology in achieving zero trust has become a trusted source for companies and governments worldwide. Download the NIST CSF1.1 here. Note that CSF v2.0 is in draft form and can be accessed here.
   b. Cloud Security Alliance (CSA) Guidance 4.0. This document is a must-have for enterprise IT organizations in the cloud – or those beginning the cloud journey. This crowd-sourced document brings about best practices from organizations undertaking cloud projects – real-world feedback and guidance from real-world use cases. View the CSA Guidance 4.0 here.
   c. Cybersecurity & Infrastructure Security Agency (CISA) Zero Trust Maturity Model (ZTMM) v2.0. How does an IT organization go about starting its zero-trust journey? How does management measure effectiveness, gaps,

and focus areas? The CISA ZTMM v2.0 is a great starting point, taking what was previously referenced as a "clean sheet" approach to achieving zero trust. Read and download the document here.

d. Department of Defense (DoD) Zero Trust Strategy and Roadmap. Released in November of 2022, this resource helps explain how the agency with perhaps the most stringent security requirements – the DoD – is achieving zero trust. Further, this site provides enterprise IT with pointers and many other valuable resources to implement and maintain a zero-trust posture. View the DoD CIO library here.

3. **Establish and enforce practices, policies, and processes** – The US military thrives through structure and discipline. A big part of this success is establishing and enforcing standard operating procedures (SOPs). These SOPs are reinforced frequently, ensuring people follow the right processes when enforcing an objective.

   Cybersecurity is no different. Enterprise IT organizations looking to achieve military-grade security must be militaristic in approach. Establish best practices around security as it applies to IT and business users. Enforce those practices through policy. And test those practices through some of the activities described previously (e.g., red team/blue team).

4. **Audit your infrastructure** – Cybersecurity begins at the lowest levels of your environment. Some say you are only as secure as the point below the point of attack. In the case of your environment and application stacks, this starts with infrastructure. What generation of servers are deployed? Are the CPUs deployed vulnerable to side-channel attacks? Does your server vendor build in protection and resiliency at the hardware and firmware level?

   Any organization can take a significant first step toward hardware security with a simple audit – whether with a standard inventory tool or simply a spreadsheet used to track servers and infrastructure across the datacenter.

5. **Work with the right partners** – While this may seem like a given, it's essential to understand that not all IT solutions companies take the same approach to driving security in their products. The example of SolarWinds proves that multiple vendors (including security companies) were caught with significant vulnerabilities.

a. The same applies to hardware vendors. For example, while all server vendors claim to deliver best-in-class hardware-based security, they each have a unique approach. And while some vendors are relatively new to emphasizing secure computing, others (like HPE) have been designing security at the lowest levels since before security became a maniacal focus of IT. Some would argue that HPE made the server security market.

HPE'S HISTORY OF HARDWARE-BASED SECURITY

MI&S has been tracking HPE's approach to hardware-based server security since the company first introduced silicon root of trust to the market with the launch of the ProLiant Gen10 portfolio in 2017 (read our coverage here). It is important to note that the company was the first to market in developing this low-level protection that can detect changes to drivers and firmware immediately – enabling security professionals to prevent months-long exploitation by low-level rootkit attacks. And shortly after the release of silicon root of trust, the company released tools within iLO to enable IT administrators to quickly restore servers to a last known good state in the event of an attack.

With the launch of Gen10 Plus, HPE deepened ProLiant's security profile with capabilities such as TPM 2.0 as a standard offering, attestation via platform certificates, and zero-trust provisioning via iDevID.

But perhaps the biggest security announcement was neither hardware nor software. Rather, it was HPE's secure supply chain initiative, whereby the company began secure manufacturing. Customers requiring greater assurances of security can acquire servers built by a manufacturing team that has gone through extensive background checks, in facilities that met the scrutiny of the US government.

Gen11 saw HPE continue to drive security from the lowest levels of silicon to the application stack. This generation of ProLiant saw TPM, platform certificates, and IDevID standard on all servers, as well as a broadening of the company's secure manufacturing capabilities. And one of the highlights of Gen11 was the release of HPE GreenLake for Compute Operations Management. Additionally, HPE included expanded component attestation through the secure protocol and data model (SPDM) specification.

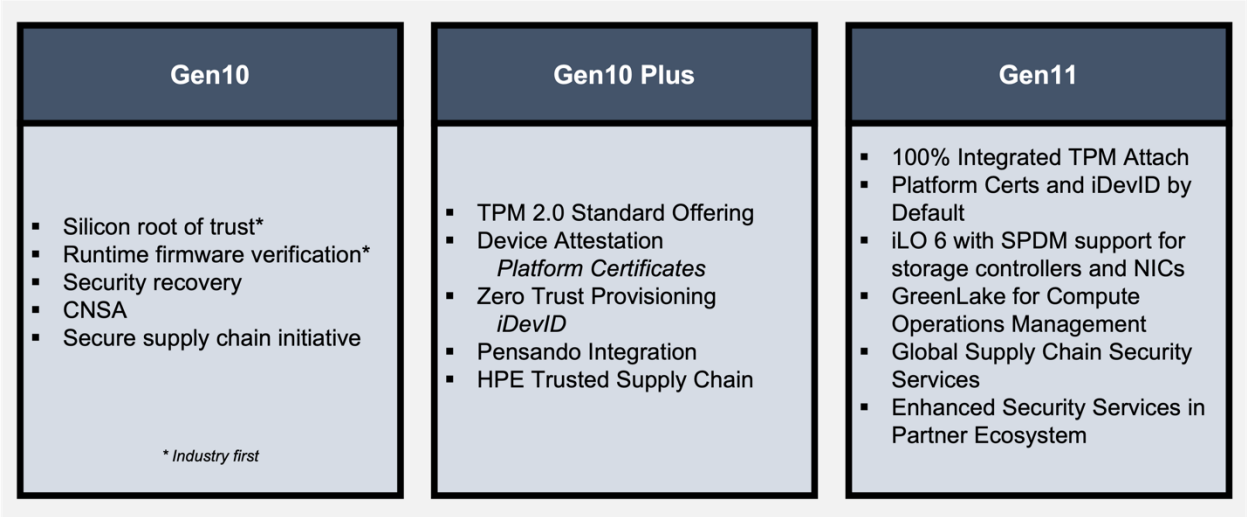
FIGURE 3: COMPUTE OPS MANAGEMENT SECURITY CAPABILITIES

GreenLake Compute Ops Management Security Capability	GreenLake Compute Ops Management Functionality
Risk Assessment	Continuous review of applications for risk and threat analysis
Vulnerability Protections	Constant human review of CVE list for constant exploit landscape and mitigations
Architecture Security	Microservices architecture isolates security issues
API Gateway | CloudFront	API Gateway protects against external attacks CloudFront integrates with web application firewall – providing another layer of security
Role Based Access Control	Precise levels of access
Multi Factor Authentication	Software based authentication, further securing access
mTLS Authentication	Used to secure all on premises communications
AES 256 Encryption	Highest levels of encrypting data
Multi-Tenancy	Customer data stored separately, securely

Source: Moor Insights & Strategy

But this has just been the beginning for HPE. The company has continued to innovate in security and has established security as both a design philosophy and design point. Secure computing has been at the center of the company's design focus, leading to features and capabilities that need to be more stable in the threat landscape. Put more plainly, the company isn't simply dropping components on a motherboard or in a chassis – it is looking generations out when considering platform design.

FIGURE 4: HPE LEGACY OF SECURITY-CENTRIC INNOVATION



Source Moor Insights & Strategy

The best demonstration of how deeply security has become rooted in the HPE culture is how the company has approached ProLiant. It is evident in the entire lifecycle – from sourcing materials and components to securing manufacturing and validation and attestation all the way through to secure recycling. Security is multi-planar at HPE – through the life of the server and from the lowest levels of silicon through the application stack. Because of this, MI&S believes HPE and its ProLiant lineup should be a serious consideration for any security-conscious IT organization.

SUMMARY

The message is simple for those waiting for this wildly unpredictable (and increasingly dangerous) cybersecurity landscape to normalize. Don't hold your breath. Although there already seems to be a daily cyber headline, with some high-profile organization or government entity being exploited, expect this only to worsen. Bad actors span nation-states to lone wolves, and access to the technology and tools to bring the most prominent organizations to their knees is only a click away on the dark web.

While the external factors facing enterprise IT are quite dangerous, what IT can control can appear equally frightening. Despite increasing budgets and more resources, IT organizations are more vulnerable than ever. In some cases, more is less, and this can be especially true in cybersecurity. Enterprise IT doesn't need more tools or more professionals who lack the real-world experience to be effective. Put differently, enterprise IT must get back to basics when it comes to cybersecurity.

What enterprise IT can control is how it approaches securing its environment. MI&S believes that many organizations can benefit from a clean-sheet approach. Step back from the day-to-day and reimagine cybersecurity – the organizational approach and operations. Understand best practices around establishing and maintaining a zero-trust environment. Continuously test and look for vulnerabilities. Becoming militaristic in approaching security – stringent standards with no compromise – is the only way to keep the bad actors at bay.

And choose the right partner for your hardware security needs. While all server vendors have security features and capabilities, not all servers are designed with a zero-trust mindset. Because of HPE's proven track record in staying ahead of the threat landscape, MI&S sees the company as a cornerstone of the zero-trust enterprise.

For more information, here.

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTOR
Matt Kimball, Vice President and Principal Analyst, Datacenter Compute and Storage

PUBLISHER
Patrick Moorhead, CEO, Founder, and Chief Analyst at Moor Insights & Strategy

INQUIRIES
Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS
This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name, author's title, and "Moor Insights & Strategy." Non-press and non-analysts must receive prior written permission from Moor Insights & Strategy for any citations.

LICENSING

DISCLOSURES
Hewlett Packard Enterprise commissioned this paper. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER
The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators, not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of this document's publication date. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.