Hewlett Packard Enterprise

eGuide

360-DEGREE SECURITY WHERE AND WHEN YOU NEED IT

Secure on all sides

HPE's silicon-to-cloud security accelerates outcomes for a distributed world

Enterprises of today are faced with an unprecedented set of challenges when trying to secure their data sets across increasingly complex distributed IT environments. In fact every 11 seconds[1] a business falls prey to a ransomware attack. Our industry is at a critical juncture—to establish new ways for enterprises reclaim their security and help to address how to secure the vast and fluid digital supply chain from edge to cloud.

Today enterprises are struggling with more advanced and persistent threats such as ransomware and malware that targets the low levels of the IT infrastructure, beyond the reaches of their end point security software solutions. With cyber attackers increasing their aggressiveness, their scale and budgets, they are creating an increasingly sophisticated marketplace for new exploits to occur.

To address the security challenges across highly distributed IT environments HPE's approach begins at the foundation—in the supply chain and rooted in the silicon with enhanced zero trust enabled 360-degree security for Compute. HPE's zero trust security architecture and secure lifecycle is initiated deep in the silicon during manufacturing and concludes with a safeguarded, end-of-life decommissioning, to create the **world's most secure industry-standard server portfolio**.[2] Right now around the world, you can find the HPE-exclusive silicon root of trust technology in over two million active servers.

1. Cybersecurity Ventures Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021
2. Based on external security firm conducting cyber security penetration testing of HPE Gen10 servers and three leading server competitors, September 2019

Click on the arrows in this eGuide to jump to the particular section you want to see.

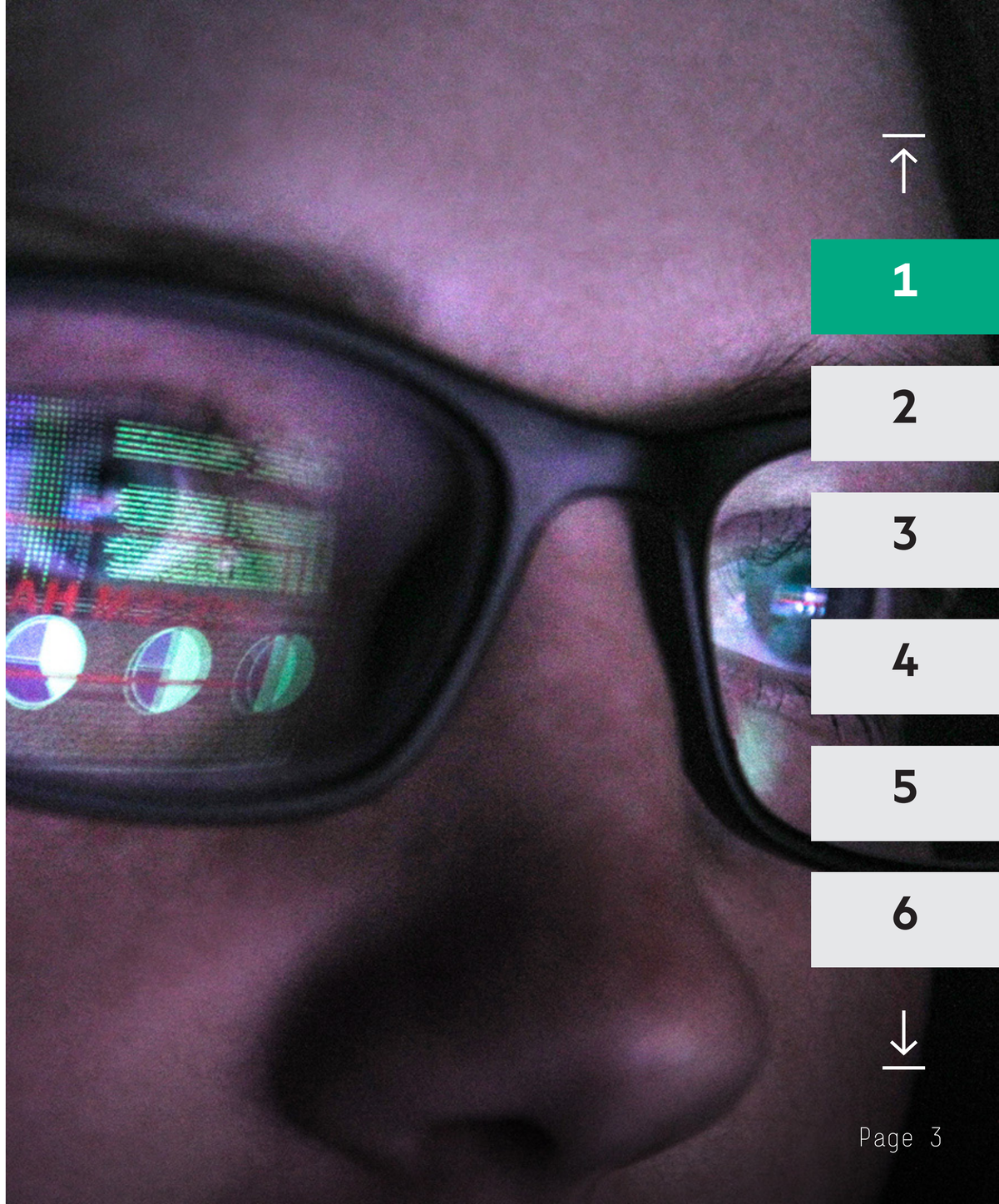
1. An ever-evolving landscape

Threats advance alongside technology

Today, IT professionals no longer question if, but rather, when an organization will become the subject of a cyberattack. Cybercriminals will strike wherever they find weaknesses or opportunities, hacking into firmware in everything from home appliances to data center servers. And security threats seemingly advance at the same rate as technology, resulting in a perpetually moving and evolving target.

Nearly 60% of IT professionals agree “it is difficult to protect complex and dynamically changing attack surfaces” and “the inability to integrate security solutions is the reason why data breaches are still happening.”[3] Clearly, it can be difficult for even the most security-conscious IT organizations to stay on top of the latest developments in cybersecurity.

Attackers inevitably find ways to take advantage of new technology trends as they gain footing in the market. From mobile and cloud computing to connected devices and the IoT, the more promise a technology holds for business, the more desirable it is to exploit. They still operate in the most basic ways too—using email phishing scams, stealing USB storage devices, or carelessly guarded passwords.



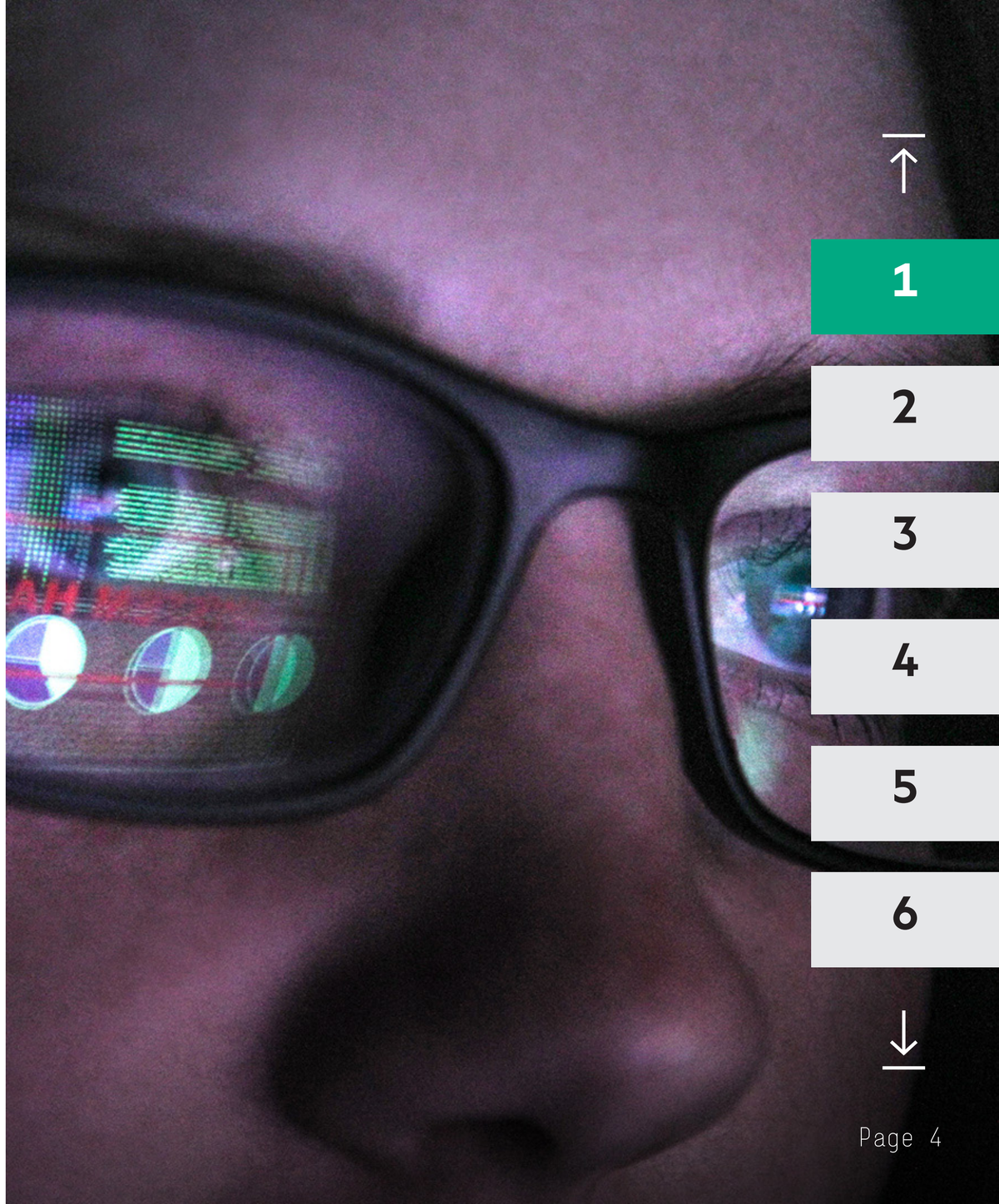
3. “Supply chain cyber attacks to ‘quadruple’,” cips.org, 2021

An ever-evolving landscape →

The dominating trend of 2021, though, is the supply chain attack. The European Union Agency for Cybersecurity (ENISA) cautions in its report “Threat Landscape for Supply Chain Attacks” that cyber-attacks are anticipated to quadruple from 2020. These less opportune crimes are more difficult to execute, but come with a bigger payoff for the adversaries.

Unfortunately, more than half of IT professionals feel they’re unable to keep up with the onslaught of alerts, and their security teams lack visibility into all devices connected to the IT infrastructure. In addition, they report “it is hard to protect the expanding and blurring IT perimeter with IoT, BYOD, mobile and cloud.”[4]

Yet, effective threat managers simply cannot risk responding to the unique vulnerabilities of each tech trend, because shifting their attention means opening their organizations to further attacks. IT professionals can’t stop attackers from trying their hardest, but they can employ better models and methods to prevent breaches from occurring.



4. “Closing the IT Security Gaps 2020 Global Study,” Ponemon Institute, 2020

2. The foundation for silicon-to-cloud security

Zero trust enabled architecture safeguards infrastructure

You need security that goes beyond the firewall and software to protect the heart of your infrastructure, starting with the supply chain. From materials suppliers to logistics and transportation services, and production and assembly to warehousing and distribution, HPE suppliers are required to comply with company policies, as well as ISO standards and the Defense Federal Acquisition Regulation Supplement.

HPE Supply Chain compliance is assured through risk-based security audits, program monitoring, inspections of electronic parts, component traceability, and material control processes. Taking this already secure supply chain methodology to the next level is the HPE Trusted Supply Chain—manufactured in highly secured US HPE facilities that feature hardened data protection during manufacturing process in support of customers spanning industries including federal, public sector, banking and financial services, and healthcare organizations, that require highly secure products sourced in the US. It also addresses customer demands for an additional supply base to increase resiliency and identify and reduce risk in the midst of COVID-19 that has impacted supply chains globally.

"Consider an industry-standard rack server is built from up to

10,000 components.

Further, consider the chain of custody of that server before it reaches a datacenter. The opportunity for the server to become compromised is a real threat that should concern every IT professional."

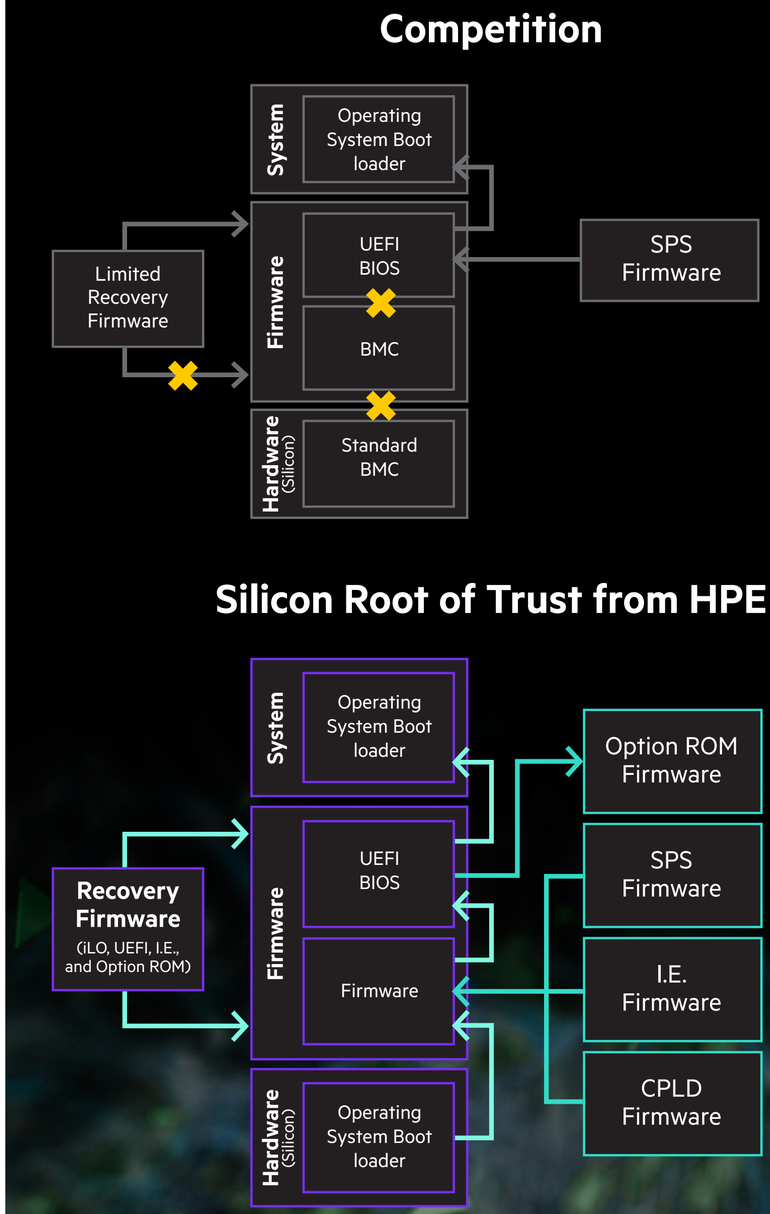
"Closing the IT Security Gaps 2020 Global Study," Ponemon Institute, 2020

The foundation for silicon to cloud security →

At the silicon level, three HPE security innovations—platform certificates, the **Silicon Root of Trust from HPE**, and product cryptographic identity (iDevID)—work together, providing intersecting security and ultimately, peace of mind. And, HPE has created security measures for when the time comes to retire or repurpose infrastructure.

Platform Certificates are based on hardware manifest of the server upon the completion of the manufacturing, and prior to shipping, providing assurance that the integrity of the system throughout the supply chain lifecycle has not been compromised and is intact upon arrival to the customer site and prior to the server being connected to the network. Additionally, a **Server Configuration Lock** can be engaged, ensuring that any changes made will render the server unbootable without authorization. According to cybersecurity solution experts, "industries that require Zero Trust architectures will benefit from [HPE's] new Platform Verification Process, that ensures that systems have not been altered at any point since leaving the factory and prior to connecting to mission critical networks such as government networks critical infrastructure."[5]

Industry-standard HPE Gen10 Plus servers also include the **Cyber Catalyst by Marsh**[SM]-designated Silicon Root of Trust from HPE built directly into the hardware itself. This binds all the essential firmware—UEFI BIOS, complex programmable logic device, innovation engine, and management engine—into the silicon before the server is even built. iDevID authenticates this HPE-exclusive "immutable digital fingerprint" on the **HPE iLO** chip to allow remote management and monitoring features, touch-free. Virtually impossible to alter, this chipset provides an



5. "HPE is Elevating Supply Chain Security," InfusionPoints, LLC., 2021

The foundation for silicon to cloud security →

unprecedented level of hardware security that enables firmware to be authenticated as far back as the supply chain, providing a secure startup process.

When the server boots up, the firmware looks for the unique fingerprint buried in the silicon to see if it matches the firmware fingerprint. Once the silicon fingerprint is verified, the rest of the essential firmware—over 4 million lines of code—is authorized to boot and scan itself.

If at any point, a hacker has inserted a virus or compromised code, the runtime firmware verification capability will detect it and the customer will immediately be alerted. If a breach is detected, customers have three options: the server can be recovered to the last known good state of firmware, restored to factory settings, or taken offline so security teams can perform forensics.

When it's time to retire or repurpose servers, HPE provides a National Institute of Standards and Technology (NIST)-level crypto-erase. One-button secure erase enables customers to easily erase all user data with confidence that no data can be recovered for nefarious purposes—to easily repurpose and redeploy servers. In addition, **HPE Pointnext Services** offers asset recovery services to ensure the retirement of infrastructure is both secure and environmentally safe.

"HPE's approach to driving hands-free security for the lifecycle of infrastructure should make its servers a 'must consider' for companies of all sizes.

Simply put, HPE's intersecting security should increase IT administrators' peace of mind as they embark on digital transformation projects, knowing that the vast amounts of data generated and stored from the edge to the cloud are secure."[6]

Matt Kimball, Senior Analyst
Moor Insights and Strategy

6. "Zero Trust is a Lifecycle Effort," Moor Insights & Strategy, 2021

Staying ahead of threats

HPE continues to adapt and invest in new technologies

InfusionPoints, an independent cybersecurity solutions expert, was invited to evaluate the innovative new security technologies in HPE Gen10 Plus servers.

"The need for assurance of the provenance, security, and trustworthiness of hardware, firmware, and software running today's workloads is fundamental to protecting against modern threats. HPE is continuing to innovate and lead in building security features into their ecosystem that provide for this level of security."[7]

The third-party experts provided further context in a second report, stating that "HPE started building the foundation of Zero Trust capabilities with the release of the HPE-exclusive silicon root of trust in 2017 with HPE Gen10 servers which we thoroughly tested at the time." They found that Silicon Root of Trust from HPE provided validation and recovery capabilities for the server UEFI and HPE iLO—and extended to provide validation to component firmware. "With HPE ProLiant Gen10 Plus servers, HPE continues to add Zero Trust enabling features into their inter-generation products."[7]

InfusionPoints' experts remind that the authentication of devices isn't much different from the authentication of human users: Authentication credentials are only as good as the credential issuer, and how tightly they prove the identity of an entity before binding that entity to an authentication credential.[6]

Enter the HPE server platform certificate and iDevID in addition to the Trusted Platform Module (TPM). As a supporter of the Trusted Computing Group (TCG), HPE has worked to ensure an open-standards-based TCG compliant implementation of platform certificates. And, within the United States, these systems will be manufactured leveraging the HPE Trusted Supply Chain program which gives customers stronger validations with hardened security features directly enabled within the factory by vetted HPE employees in highly secure facilities on US soil.[8]

The report concludes that "as supply-chain attacks continue and adversaries pivot to new tactics, seeing HPE's approach to staying one step ahead should allow consumers to rest easy knowing HPE has their interest."

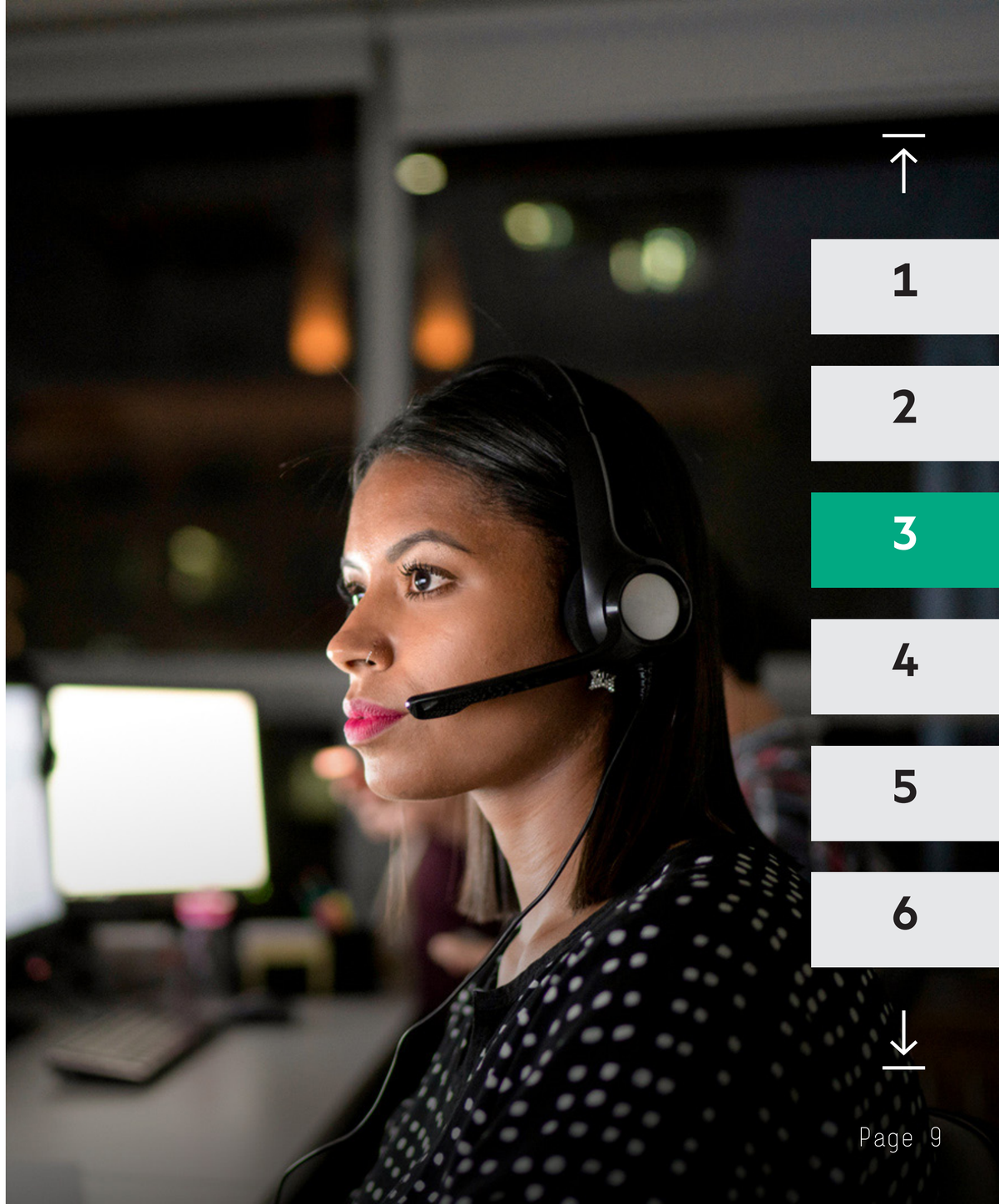
7. "Device Identity and Component Attestation comes to HPE Gen10 Plus Servers," InfusionPoints, LLC., 2021
8. "HPE is Elevating Supply Chain Security," InfusionPoints, LLC., 2021

3. Safeguards for any business

Deep security regardless of industry or business size

Only HPE Gen10 Plus servers can provide enterprises, government entities, or small-to-medium businesses with the highest levels of protection against firmware attacks, and the HPE Gen10 Plus product line offers a zero trust enabled architecture that starts in the supply chain an extends a cryptographically attested with an immutable chain of trust to the silicon and beyond—regardless of the server line you purchase.

For enterprise and government agencies, we offer **HPE ProLiant** rackmount servers, **HPE Synergy** compute modules, and **HPE Apollo Systems** high-density and high-performance computing (HPC) servers. For smaller businesses and remote branch offices, the **HPE ProLiant ML series** tower servers offer the same Silicon Root of Trust from HPE as the more powerful servers.



Safeguards for any business →

GOVERNMENT

HPE advances in security are of even more interest to the government sector. In the **Executive Order** issued by the Biden Administration dated May 12, 2021, Zero Trust security models are touted repeatedly as the best practice government agencies must adhere to. Further mentioned are cloud services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).[9]

By offering a flexible range of configurations, HPE Gen10 Plus servers can be deployed as part of a private cloud, anchor VM delivery, facilitate secure container environments, store database applications, and process Big Data transactions in nearly any Federal IT environment.

Plus, HPE iLO 5 technology offers four different levels of security, based on customer needs and industry regulation. HPE Gen10 Plus Servers ship in production mode but can be upgraded to high-security mode for increased encryption sophistication, Federal Information Processing Standards (FIPS) mode for federal processing standards, and Commercial National Security Algorithm (CNSA) mode, which offers the highest level of cryptographic algorithms that meet standards set by the National Security Agency.

RETAIL

In today's online marketplaces, more than 90% of login attempts at retail sites are automated attacks initiated by hackers. More than 1.8bn usernames and passwords were stolen in 2020, thanks to 117 credential spills, up from 77 in 2019.[10]

And it's not just about stealing passwords. At the enterprise level, retailers are doing a lot more than processing transactions online—they're moving products around the world and sourcing new and existing materials with sophisticated enterprise resource planning (ERP) systems while trying to protect crucial employee and customer information.

9. "Executive Order on Improving the Nation's Cybersecurity," whitehouse.gov, 2021
10. "6 Things Every Small Business Needs to Know About Ransomware Attacks," inc.com, 2021

Safeguards for any business →

MANUFACTURING AND DISTRIBUTION

At every touch point—each factory, transfer, warehouse, and delivery—there exists some opportunity for bad actors to make unwanted modifications to products on their way to the end user. It's a pervasive problem.

HPE has overcome this by securing its supply chain through delivery using iDevID, platform certificates and the Silicon Root of Trust from HPE. These secure solutions, embedded into the silicon of Gen10 Plus Servers, has given major logistics and delivery services enough confidence to deploy HPE servers in their data centers.

SMALL AND MID-SIZED BUSINESSES

While security breaches can cause nuisance, fines, and loyalty issues for the enterprise, those same threats can have devastating effects on small and medium-sized business (SMB). In fact, most SMBs don't survive a breach—60% go out of business after six months. It doesn't help that 50 to 70% of ransomware attacks target small businesses. Worse, about 80% of victims get hit a second time.[11]

By building firmware validation directly into our silicon, HPE is trying to make security as fundamental as possible, and that's good news for SMBs who often lack IT budgets and staff to fight the security battle day to day.

11. 2021 Credential Stuffing Report," f5.com, 2021

4. Securing your data everywhere

Data at rest, in motion, at execution

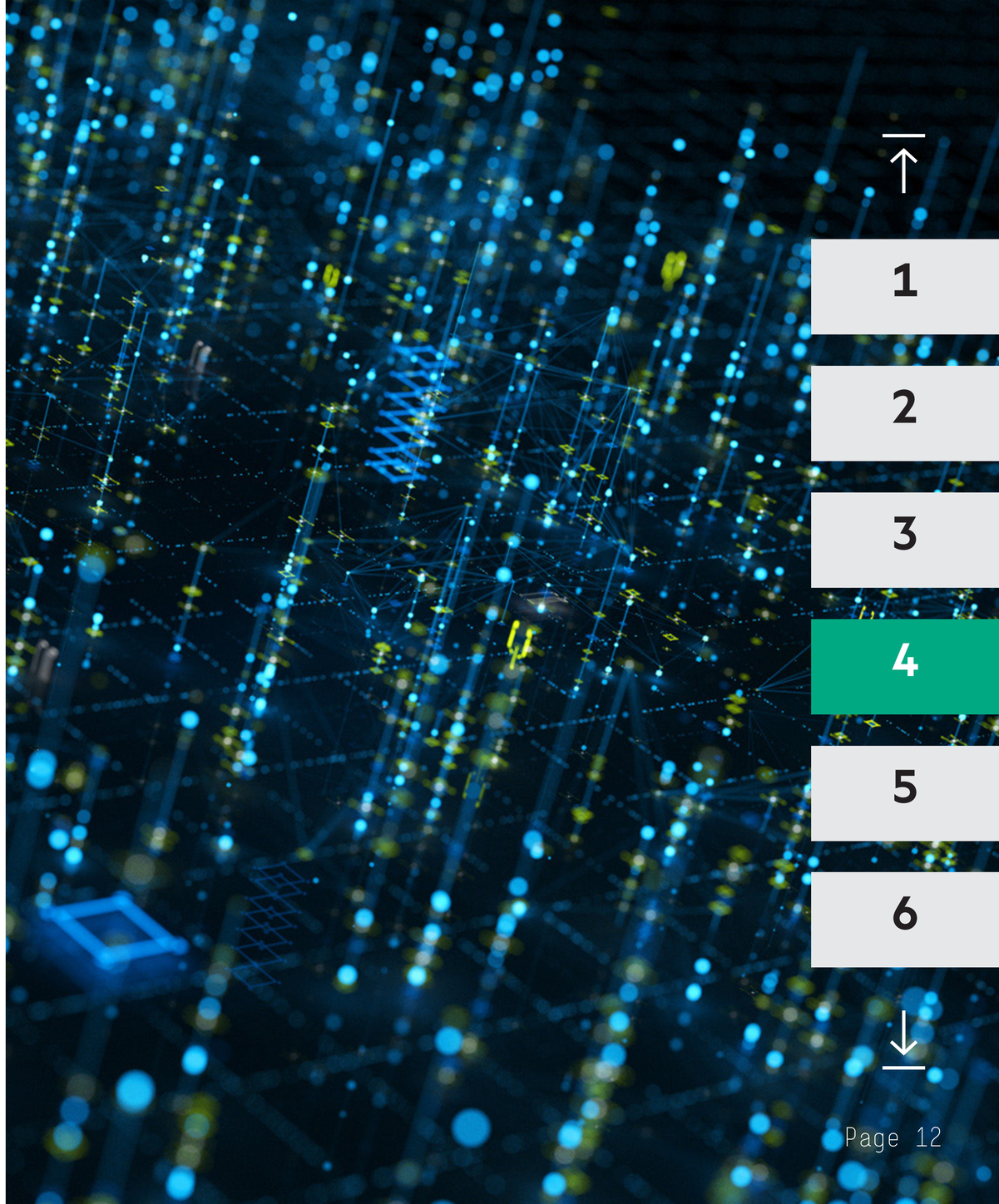
The protection of customer information and other sensitive data tend to be the most concerning issues for IT professionals. HPE provides a set of solutions to address data security at various stages: data at rest, data in motion, and data in execution.

DATA AT REST

HPE servers with Utimaco ESKM provides a complete **solution for unifying and automating an organization's encryption controls** by securely creating, protecting, serving, controlling, and auditing access to business- and compliance-critical encryption keys for when data is transferred from data at rest in a storage or local server to another node within WAN. HPE ProLiant DL360/DL380 Gen10 Plus is designed as a fully integrated solution and is a Federal Information Processing Standards (FIPS) 140-2 validated secure server appliance.

DATA AT MOTION

The HPE ProLiant server with the Pensando distributed services card provides **data in motion security solutions**, and a host of other advanced features. As opposed to a significant part of the servers' CPU power being used for network services management purposes, this solution poses virtually no impact on the host server CPU. Providing business agility, IT simplification, and a lower TCO, this HPE solution is available as a capital expenditure (CAPEX) as well as an operational expenditure (OPEX) deployment model through HPE GreenLake.



Securing your data everywhere →

DATA AT EXECUTION

This **solution** leverages HPE ProLiant DL380T Trusted Supply Chain Server with Intel® Ice Lake SGX processors to deliver a single pane for managing secure enclaves across the SGX-based confidential compute nodes within the data center. Fortanix Confidential Computing Manager helps orchestrate critical security policies such as identity verification, data access control, and code attestation for enclaves that are required for confidential computing.

And HPE ProLiant rack servers with XYPRO Technology's XYGATE SecurityOne (XS1) offer a **unified security management and data analytics platform**, which includes real-time risk management, threat detection, vulnerability assessment, compliance reporting, and integrity monitoring using a modern browser-based interface for end-to-end ZERO Trust security. XS1 actively detects security threats by combing through data in real-time and intelligently highlighting the actionable incidents that need immediate attention.

The protection of customer information and other sensitive data tend to be the most concerning issues for IT professionals. HPE provides a set of solutions to address data security at various stages: data at rest, data in motion, and data in execution.

Project Aurora

Enabling HPE's edge-to-cloud zero trust security architecture

Project Aurora extends our Silicon Root of Trust from HPE to deliver a complete security architecture with new embedded and integrated security solutions starting at the silicon level. Ignited in the supply chain, it establishes an immutable chain of trust up through the infrastructure, operating system (OS), software platform and workloads without requiring signatures, significant performance trade-offs, or lock-in.

With Project Aurora, you can prevent and detect compromise in the hardware and software components of a remotely managed HPE system through standardized continual measurement, attestation, and verification of everything. It helps you transform security from a barrier to an innovation acceleration—from silicon to your workloads.

This continuous attestation will enable HPE to quickly detect advanced threats in seconds—minimizing data loss and authorized encryption (and corruption) of valuable data and intellectual property.

5. Protecting forward

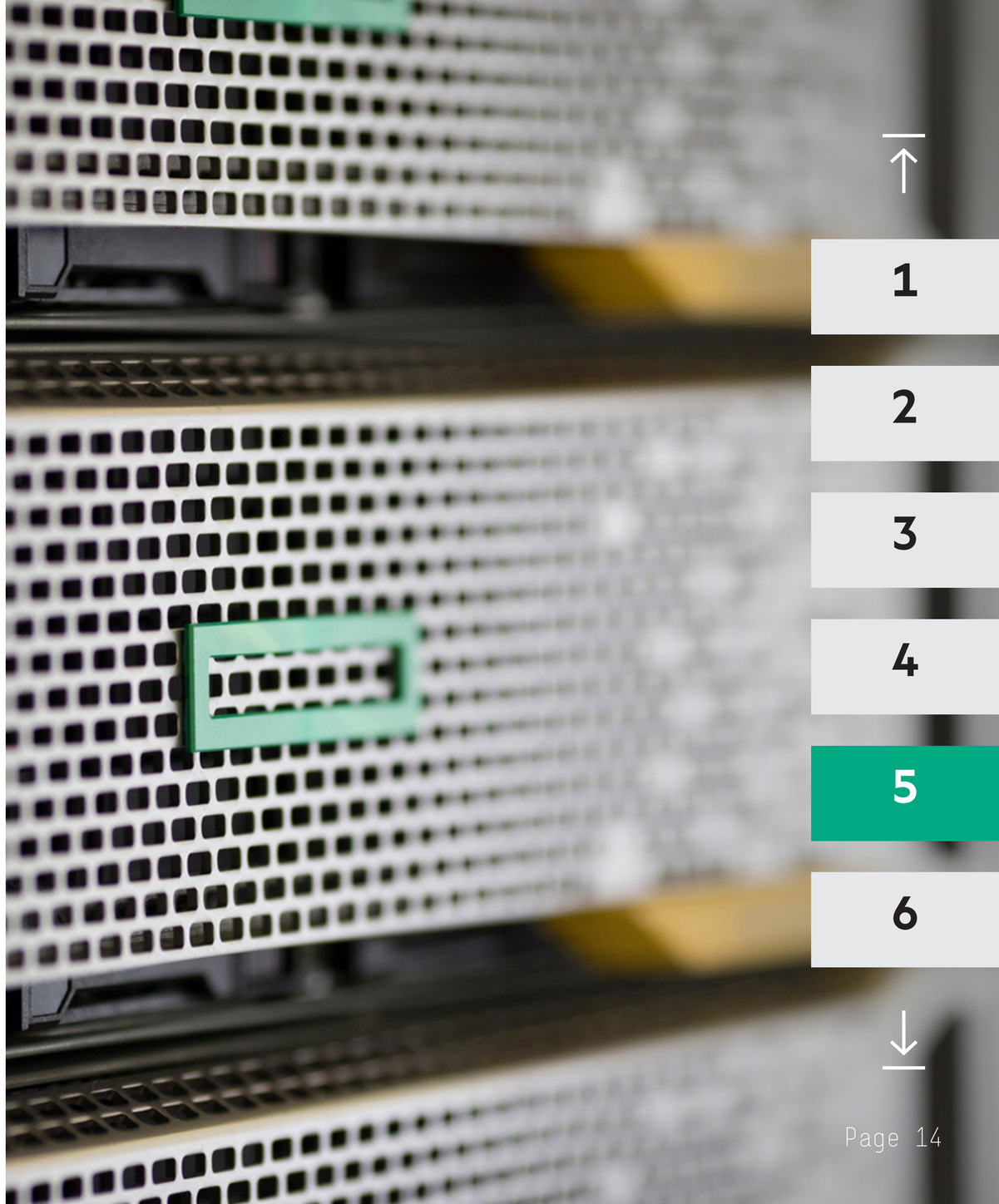
Recently, attacks to data and systems are steadily increasing, in number and complexity, shifting from network perimeter, software, and applications to the physical platform itself. Yet, network firewalls, antivirus scanning, and even security monitoring tools are lacking, because they fail to detect firmware tampering.

While these threats are constantly evolving, HPE remains the only manufacturer of industry-standard servers with security two generations ahead of the competition. Building this trust starts with an uncompromised and trusted supply chain, acting as the first line of defense and ensuring security before your infrastructure arrives. During the life of your HPE Gen10 Plus Servers—equipped with a server-specific digital fingerprint and automated security including early detection and recovery—over 4 million lines of firmware will be protected from malware, malicious code, and ransomware. And when it's time to retire or repurpose old infrastructure, you're protected too: The safeguarded removal of passwords, configuration settings, and data is simple.

HPE's commitment to increasing security across all three critical pillars of the environment—protect, detect, and recover—provides confidence from the firmware up.

Need assistance with security? HPE Pointnext Services offers best-in-class design and implementation services to further extend and complement the built-in features in HPE Gen10 Plus Servers.

Protect the future of your business, with HPE.



6. Resources

Web Page
HPE Security

Training Game
Escape Room

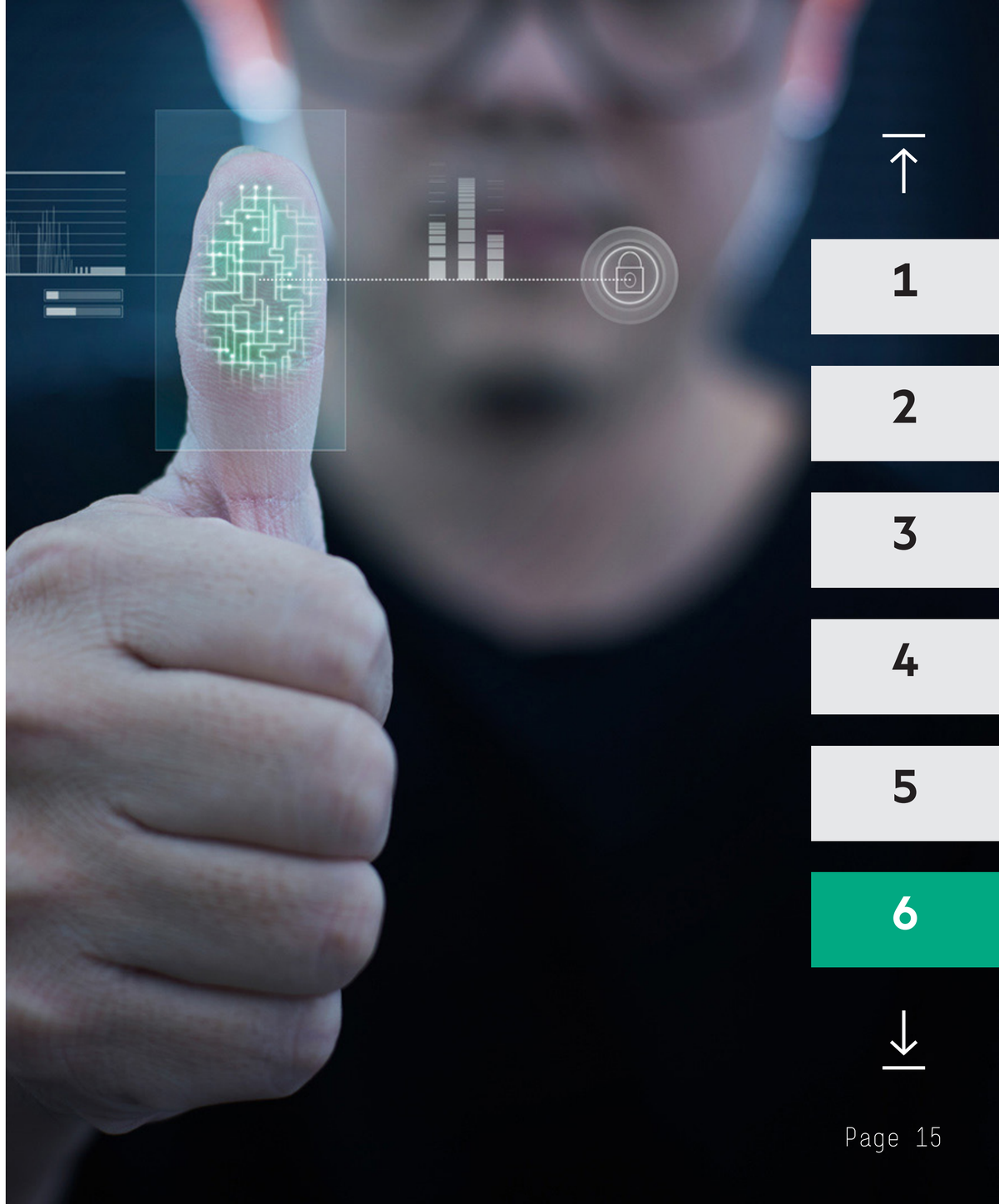
Brochure
Mitigating Risk with Managed Security from HPE Greenlake Management Services

Analyst Reports
- **Closing the IT Security Gaps 2020 Global Study by the Ponemon Institute**
- **HPE is Elevating Supply Chain Security by InfusionPoints CyberSecurity Solutions**
- **Device Identify and Component Attestation comes to HPE Gen10 Plus Servers by InfusionPoints CyberSecurity Solutions**

White papers
- **Zero Trust is a Lifecycle Effort**
- **HPE Enables Zero Trust Architecture with Project Aurora**

Video
Just the Facts: HPE Security

Reference Guide
Gen10 and Gen10 Plus Security



Get 360-degree security where and when you need it

Learn more at
www.hpe.com/security/compute

Make the right security decision.
Click here to chat with our experts.

Chat **Email** **Call**

Get updates

a50005077enw, S-August 2022

Hewlett Packard Enterprise