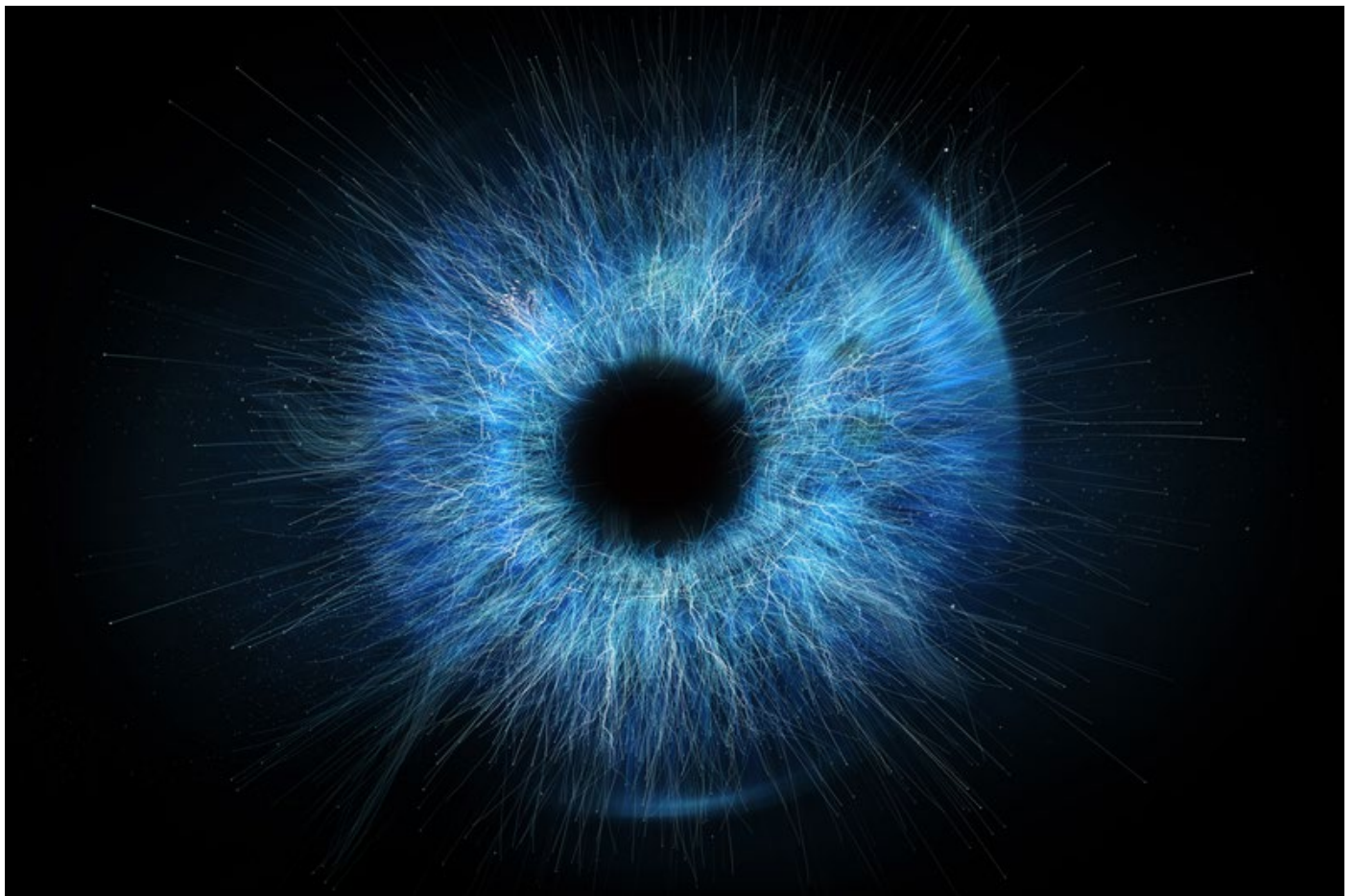📅 April 13, 2021

Cybercrime pays, and companies are writing big checks

Cybercrime is one of the world's largest industries and defending against it is one of the largest IT spends companies make these days. HPE's 360-degree view of security is meeting that challenge.

By Gary Craze, HPE ProLiant Servers Product Marketing Manager, Hewlett Packard Enterprise

When we think of large, global industries, there are very few in the massive realm of trillions of dollars. The global healthcare industry, the global education market, the global construction industry… each claiming roughly ten trillion dollars per year.

Thus, it might surprise some people to learn that cybercrime ranks up in that lofty group as one of the world's largest industries. It's expected to reach over $10 trillion dollars by 2025. And it's not content with its status either. Cybercrime is one of the fastest growing industries at roughly 15% each year. [1]

Two out of three companies expect that their greatest IT spending category will be on fortifying their cyber defenses, with an expected 3.5 million roles in companies dedicated to cyber protection. [2,3]

The vast amount of money and armies of people needed to fight cybercrime becomes apparent when looking at all the challenges companies, and individuals, need to address.

- Persistent malware and ransomware attacks
- Social engineering and phishing attacks
- Cyber syndicates and state attacks from organized crime and rogue nations
- Growing use of artificial intelligence and machine learning to supercharge attacks
- Growing financial, regulatory and privacy laws companies have to meet

In the end, roughly two out of three companies indicate that they struggle to protect against complex and dynamically changing attacks. Their lack of integration and the complexity of their security solutions are creating gaps in their cyber defenses. Ultimately, most companies confess they lack confidence that they can detect an inside attack before a breakout occurs. [4]

Increasingly complicating things for companies is the fact that attacks can begin both before and after IT infrastructure is actually in the possession of the company. It raises concerns about the security of the IT infrastructure from their suppliers, as well as the safety and integrity of their critical data beyond end of the life of the infrastructure.

Now, more than ever, companies need better assurances of the security of their IT infrastructure across the entire span of its life.

Taking a 360-degree view to security

HPE accepted the challenge when we built the ProLiant Gen10 series of "The World's Most Secure Industry Standard Servers", creating the foundation of what today is a holistic, 360-degree view to security that begins in the manufacturing supply chain, provides industry-leading security throughout the operational life of the servers, and concludes with a safeguarded, end-of-life decommissioning or repurposing of a company's servers.

Today, HPE's 360-degree view to security continues to grow across the entire lifespan of a server.

HPE's Trusted Supply Chain, which ensures security before a customer's infrastructure even arrives at their facility, continues to expand with offerings such as new servers that include advanced security features that are built by vetted HPE employees in highly secure U.S. facilities.

For customers' day-to-day operational security needs, HPE set the standard with our Silicon Root of Trust which creates a digital fingerprint in the silicon of the server itself, protecting against attacks against the very core of a server.

This digital fingerprint protects over 4 million lines of firmware from malware and ransomware and helps defend your infrastructure from malicious code with early detection and automated recovery of a security-compromised server.

Taking security to the next level

But HPE isn't content with just locking down the core of a server.

Extending the Silicon Root of Trust beyond the core, HPE is taking a "Zero Trust Architecture" approach to the entire system, extending the Silicon Root of Trust concept across the platform.

Using new approaches such as "product cryptographic identity," or Device Identity Certificates, HPE can extend that root of trust out to other devices in the system. With the expansion of the root of trust across the devices in the server, an additional approach known as "configuration validation," or Platform Certificate, can be used to ensure the entire server configuration can be securely locked down.

Beyond the physical elements of a server, HPE's security vision extends into operating systems and applications, working closely with our partners to leverage new technologies that help safeguard application integrity and data privacy as the need for secure, confidential computing grows.

Ultimately, these new security approaches of Device Identity, Platform Certificates, and confidential computing are driving the ability for companies to reach new levels of secure, zero-touch provisioning, helping them to securely accelerate the deployment of their infrastructure.

Bringing "security as a service" to companies

Even with increasing awareness of all these security risks, and an associated increase in security and compliance-related spending, managing IT security still presents an array of challenges for some companies, including skills gaps, siloed tools, complexity, and lack of automation. And these challenges only grow when you consider outsourcing operations to a third-party service provider, because while operations can be outsourced, the organizational risks of security and compliance failure can't be.

This is where managed security from HPE GreenLake Management services comes in—part of a complete security, risk, and compliance portfolio.

Managed security enhances the customer environment by offering services that include security monitoring, privileged access management, vulnerability management, and security hardening with the attention and accountability of an account security officer.

This broad portfolio of managed security services delivers security expertise and experience, simplified processes, and a holistic management solution—all aimed at reducing organizational risk.

HPE's 360-degree view of security meets the challenge

Trusted supply chains, secure manufacturing, industry-leading operational security, and a broad portfolio of managed security services: It all combines to make HPE's 360-degree view to security vision squarely aligned on the challenges customers face today.

In the end, beyond ensuring the integrity of both company and customer data and infrastructure, it's all about telling cyber criminals that their paycheck has been revoked.

Ready for more?

Discover more about HPE's 360-degree view to security.

Learn More About HPE SMB Solutions

[1] Cybersecurity Ventures, Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021

[2] Enterprise Strategy Group, 2021 Technology Trends to watch

[3] Gartner, Rethink the Security and Risk Strategy, Tom Scholtz 2020

[4] HPE and Ponemon Institute Global Study 2020: Closing the IT Security Gaps

Hewlett Packard Enterprise

a00117984enw, April 2021