INSIGHTS | **WHITE PAPER**

Protecting The Edge To Cloud Landscape With An Eye On The Future

While it's known that threat actors escalated both the frequency and severity of their attacks during the COVID-19 pandemic, the risk landscape continues expanding and the statistics prove it. Between October 2022 and September 2023, the number of ransomware attacks surged by over 50% when compared to the preceding 12 months.[2] In the United States, data breaches have reached an all-time high, with a nearly 20% increase in just the first nine months of 2023 compared to the entire year of 2022.[3] If that weren't enough, 1 in 4 people had their health records exposed in the first three quarters of 2023.[4]

A Disturbing Irony

Behind the numbers, however, lies a disturbing irony. In the past, cybercriminals required a range of technical skills to effectively execute an attack. That is no longer the case due to to the increasing availability of malware toolkits and as-a-Service offerings on the dark web. In today's landscape, attackers with simplified skill sets are still plenty capable in pursuing and executing malicious objectives. In contrast, those tasked with safeguarding enterprises are on the opposite end of the spectrum, which is to exhibit a high level of sophistication and expertise.

At a time when so much is demanded by enterprise cybersecurity teams, only 30% of businesses believe they are effectively keeping pace with the changing threat landscape while also closing the IT security gap. [5] Closing this gap is imperative as threat actors will continue to exploit its open vulnerabilities.

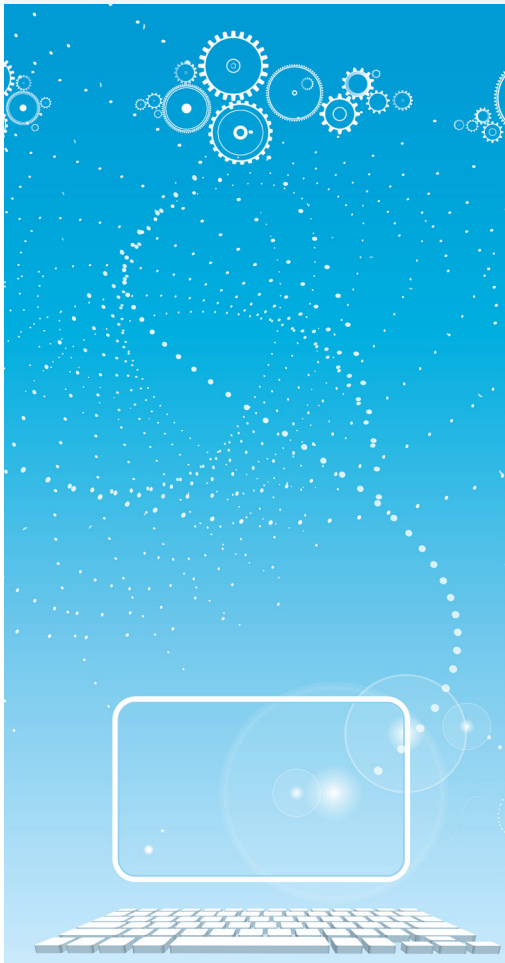
Hybrid's Impact On Cybersecurity

A lead reason for increased cybersecurity risk is the incredible wave of digital transformation that has transpired in recent years. This event has led to a substantial increase in connectivity among users, devices, and data. Consequently, this elevates the overall digital exposure and risk profile of businesses. There are now more touchpoints and attack avenues within an enterprise to secure than ever before.

Another major contributor, however, is the transition to hybrid computing architectures. There are many underlying reasons for this:

DID YOU KNOW?

A new phishing site emerges on the Internet approximately every 20 seconds.[1]



Hewlett Packard Enterprise

- Hybrid environments combine on-premises infrastructure with cloud services from multiple providers, thus increasing greater complexity. This creates more potential vulnerabilities and attack vectors.
- IT and security teams often have varying levels of expertise across different platforms, which can result in misconfigurations, security gaps, inconsistencies, and a lack of adherence to best practice standards.
- Maintaining visibility across hybrid infrastructures presents a genuine challenge, leading to monitoring gaps that may go unnoticed until they result in significant damage from threats.
- Hybrid computing usually includes third-party providers who may introduce security risks, which can subsequently impact their customers.

With the above bullet points in mind, it is no surprise that respondents to a recent survey express doubts about the security of hybrid computing. According to the survey, 75% of respondents rated private cloud as the most secure enterprise architecture with 63% placing on-prem only as the second most secure.[6] The hybrid cloud's three-pronged approach of on-premises, private cloud and public cloud took third place, followed by public cloud only.

HPE's Vision Of Security

In a digitally connected hybrid world, security is a shared responsibility. The weakest link can potentially expose everyone connected. That is why HPE has created a vision to make security an inherent part of all operations as it manages more than two million devices and over one exabyte of data through its expansive HPE GreenLake platform. These numbers offer some point of reference as to why security is such a mammoth responsibility for when so many organizations are relying on a third party. While numbers can paint the gloomy picture of today's vastly increasing risk exposure, they also paint a picture of HPE's commitment to combatting these threats. Here's some of the things HPE achieved in 2022:[7]

- Their enterprise SIEM logged over 2.6 billion events per day, prompting triage, investigation, and resolution by their Security Fusion Center.
- They blocked an average of 1,060 phishing emails received at HPE every day, creating a year-end total of 1 billion blocked email threat vectors.
- The HPE GreenLake edge-to-cloud platform continuously applies more than 2,200 separate security controls to protect customers and their data in real time.
- HPE's Product Security Response Team published 187 security bulletins, covering 334 CVEs across 450 products, including 46 HPE-issued CVEs. All impactful CVEs were remediated according to HPE security policies, and patches were made available to customers.

HPE recognizes that as your hybrid provider, they assume the role of custodian for your data. This commitment to data security permeates their organization, beginning at the highest levels and extending downward to all levels. A testament to this commitment is the fact that over 55,000 employees, (98% of HPE's workforce) undergo annual cybersecurity awareness training. At HPE, security is a responsibility that is shared across the organization. These collaborative efforts contribute to safeguarding their footprint, regardless of its location.

From Siloed To Shared Security

Organizations are beginning to learn that the cloud is not a destination, but an experience. It's an alternative way to finance and consume IT services and it is an experience that HPE GreenLake can bring to your business. With that experience also comes the seasoned security teams that adhere to best practice. The HPE GreenLake edge-to-cloud platform mitigates these risks with a comprehensive secure-by-design approach and a shared security model. Their shared model precisely outlines the security roles and responsibilities for both the cloud consumer and the provider, HPE.

HPE GreenLake takes responsibility for the security of the hybrid cloud platform and the cloud experience it brings. HPE Managed Services offers a comprehensive security portfolio, encompassing monitoring, vulnerability management, secure configuration, and privileged access management, all overseen by a dedicated account security officer responsible for security performance. Customers are responsible for managing the access of

their user base. Once you become an HPE GreenLake customer, their experts collaborate with you to design a solution that meets your business requirements and maintains the security of your environment. This operational, technical, and security support remains consistent throughout the partnership's duration.

New Approaches To Cybersecurity Talent

One of the primary factors contributing to the prevalent security gaps in many organizations today is the noticeable shortage of cybersecurity professionals. It's projected that there will be 3.5 million unfilled cybersecurity jobs by 2025.8 These unfilled positions represent inherent security vulnerabilities. Security-conscious organizations are recognizing the need to transform their approaches to cultivating and hiring cybersecurity talent. Both HPE and WEI are exemplifying this commitment by actively working to attract and nurture new talent to fill these critical roles in the future.

HPE recently launched their Professional Rotation Experience Program (PREP) for recent graduates. PREP is a two-year rotational program offering global exposure to various cybersecurity functions. Participants gain hands-on experience, rotate through different teams every six months, and receive innovative training and development.

Creating Your Own Talent Pipeline

WEI recognizes the importance of expanding the talent pool. To alleviate the challenge of competing for the same talent as everyone else, WEI is actively assisting their customers in establishing their own talent pipelines through the WEI Technical Apprenticeship for Diverse Candidates program. This initiative not only addresses the current talent shortage but also contributes to achieving diversity goals and introducing fresh perspectives within organizations. Candidates undergo thorough assessments and are matched with customers where they can learn under the guidance of experienced engineers. Upon completing their apprenticeships, customers can extend full-time employment offers to the apprentices.

Resilience Through Zero Trust

The HPE GreenLake platform is fortified by a zero-trust architecture that continuously verifies the integrity of hardware, operating systems, platforms, and workloads for ongoing security assurance. For instance, in the context of storage, HPE employs memory encryption and silicon root of trust to protect data in use and firmware. Self-encrypting drives enforce hardware-based encryption, balancing security and performance, while the HPE Trusted Platform Module enhances Microsoft BitLocker for a tamper-resistant environment. As HPE looks to the future, they are making a host of key security initiatives that include:

- Shifting from device-based data protection to self-protecting data.
- Leverage zero trust and SASE to increase the cybersecurity resilience of customer infrastructure.
- Cultivate a security culture into the organization all the way up to the board level that is committed to a strong cybersecurity awareness training program.
- Investing in user behavioral analytics that track user activities over time and detect deviations from established patterns, uncovering potential ongoing attacks.
- Clearly defining the shared security model for cloud operations and understanding the division of responsibilities between customers and providers
- Prioritizing talent acquisition over experience, recognizing that skills can be developed or earned, while talent is more intrinsic.

Talk to WEI today

Cybersecurity and business continuity are intrinsically linked, as robust cybersecurity measures are essential to protect an organization's data and systems, ensuring uninterrupted business operations. In the context of hybrid architectures, partnering with a trusted hybrid or colocation provider with expertise in establishing a zero-trust environment is crucial. Discover how HPE and WEI can assist in designing an infrastructure that meets your business, security, and compliance requirements.

Sources

1. HPE 2023 Cybersecurity 2023
2. Worldwide Ransomware Activity October 2022-September 2023: Europe, North America, and Asia Among Top Targeted Regions, Cyber Threat Intelligence Integration Center, October 31, 2023.
3. H1 2023 Data Breach Analysis: 2023 Data Compromises Are on a Blistering Pace to Set a New Record, Identity Theft Resource Center, June 30, 2023
4. Cyberattacks surge in 2023, as millions fall victim to ransomware: Report, Yahoo News, December 7, 2023
5. The 2022 Study on Closing the IT Security Gap, Ponemon Institute, January 2022
6. From Hybrid Cloud by Accident to Hybrid Cloud by Design, From hybrid cloud by accident to hybrid cloud by design (hpe.com)
7. HPE 2023 Cybersecurity 2023
8. Cybersecurity skills shortage paradox, Cybernews, November 15, 2023

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.