IBM Z® Systems Security *Vs.* HPE x86

IBM Z® Systems with pervasive encryption is a major milestone, not only in cybersecurity, but in the IT industry and a significant security differentiator in the global market--as cybersecurity is the number one challenge in enterprises today. The recent announcement of IBM z14 eliminates the labor-intensive, manual encryption processes and secures mission-critical workloads with an industry-leading, pervasive encryption—acclaimed solution. Pervasive encryption provides 100% of the data stored on the mainframe, in a few clicks, without tremendous analysis to determine the data required for encryption.

Deployment Flexibilities On *or* Off Premise. Beginning at the IBM Applications Discovery Dashboard end users optimize graphical visualizations, operational analytic reports for applications; with z/OS Connect™, developers are empowered with critical data and services through RESTful APIs; with Blockchain and IBM Hyperledger technology yields highly secure processes; moreover, IBM Z machine learning to increase visibility while decreasing costs and conserving valuable resources. The new IBM z14 hardware-accelerated encryption resides on each core with a Central Processor Assist for Cryptographic Function™ (CPACF). The pervasive encryption process protects encryption keys with tamper-responsive hardware to invalidate keys at any sign of security issues which can be restored safely. This important capability can also be extended externally from the IBM z14 to storage systems and other cloud servers.

Market

- **Worldwide Data Security.** Very strong double-digit revenue growth from $2.2B 2017 to $12.5B by 2022 with a CAGR of 41.8%. [1]
- **Global Industries.** Vigorous double-digit security growth in verticals. BFSI, Healthcare and Gov. All industries report CAGRs between 37.4% to 40% during 2017 to 2022. [1]
- **IBM Security.** Reported strong 28% year-over-year revenue growth in 2018. After reaching $4.1B in security revenue in 2018, IBM is in the top 10 worldwide by revenues putting IBM in a position to address security enterprise detection and overall requirements. [2]

IT Challenge Questions

- Do you find that encryption has been very difficult and/or expensive to do at scale?
- Have you experienced security incidents with automatic data and code encryption in-flight, at-rest, or tamper-resistance during installation and runtime?
- Have you had limitations with encrypting application data while making application changes?
- Do you have challenges with encryption via governance policy associated with access control?

Use Cases

- IBM Z Systems clients looking for an agile, highly secure, on-premise approach to integrate transactional processes with analytics and fraud detection.
- Client business areas, e.g. customer care that up-sell & cross-sell, supply chain managers and operations, transport platforms, anti-fraud; overall security, privacy and governance are top priorities.
- Insurance claims payments analytics, retail with OLTP across warehouses and distributed systems.
- Manufacturing returning from lower-cost geographies or retaining US-based operations to focus on customer service and constant innovation to decrease costs and remain competitive.

Why Choose IBM Z® Security and IBM® Security Systems?

- **Pervasive encryption enables 100% of the data stored on the mainframe to be encrypted, simply and easily, requiring no further analysis of data.**
- **Unparalleled and highly secure for on or off premise.** Crypto Express6S and Accelerator for SSL transactions for encrypted link between web server and a browser. Java, Node.js or Swift for ease in co-location development. Mobile application to remotely monitor and manage systems from anywhere with push notifications and alerts-giving administrators greater flexibility—on or off their premises.
- **Connecting "systems of record" and "systems of engagement".** Linux platform that can be deployed as a standalone server, or side-by-side with z/OS or z/VSE® or z/TPF for easy integration on a single physical server.

Sources: (1) M&M, "Disaster Recovery as a Service Market", 2017. (2) IBM Annual Reports, 2018.

IBM Z

IBM Z® Systems Security *Vs.* HPE x86

IBM

HPE® is acquiring and investing in partners to drive their security solutions. HPE is executing on services spin-merge with CSC and products spin-merge with MicroFocus®, this is a challenge for clients with critical support management escalations including overlapping products and services. HPE invested in security start-ups, e. g. SafeBreach™, Hexadite™ and Shape Security™. HPE® OneView™ in the past couple of years, inorganically grew their ecosystem to over 20 partners with 30 integrations; thus gaps in overall infrastructure management, sales alignment, support channels are prevalent. The transfer of ArcSight™ SIEM technology and Information and Governance group to Micro Focus poses challenges for security services.

Overview

HPE is coupling container offerings with hybrid cloud deployment solutions. Enhancing those offerings with containerization drives hybrid cloud architectures to improve security to create standardized environments along with ArcSight and Fortify security offerings. HPE's recent partnership of DXC, (CSC) will eventually gain traction in hybrid cloud, however, messaging for Project New Stack and SLAs will be under scrutiny. HPE competes in parts of broader data-centric audit and protection (DCAP) market, where clients demand broader, integrated data protection.

Competitor Weaknesses

- **IT Platform Complexity and x86 Challenges.** An evolving IT environment involving a mix of legacy systems, traditional on-premises infrastructure combined with multiple public and private cloud platforms will drive security containers and microservices adoption-rapidly. However, portability around various legacy architectures, commodity systems (x86) languages and scalability is still a problem. [1]
- HPE's Gen10 servers with Intel's new Xeon™ processor scalable chips 'Skylake' is designed to prevent servers from using compromised firmware code. However, with the new server enhancements, they may or may not really help defend connected enterprise IT systems. Even if the new Gen10 servers protect against firmware breaches, many are still tied into legacy systems that could remain vulnerable. [2]
- Inconsistencies remain in HPE's app development with an unclear future of the Helion Development Platform. Moreover, Intelligent Edge, Aruba networking and security products, dropped 6% y-o-y to $666M. [3]

Key Takeaways

- IBM security is built into every level of the mainframe's structure, including the processor, O/S, communications, storage and applications. Enterprises looking for cloud deployment options for specific security functionality, especially SIEM, SVM, IAM, governance and internet/network fraud prevention, should put IBM on their short list of vendors for consideration. With IBM leading in most security-based Gartner Magic Quadrants, IBM security is poised for global success with clients and business partners. Clients in every industry should consider IBM strategically, as a security provider and trusted advisor given its growing AND proven set of core competencies in security with flagship products such as QRadar, RACF, zSecure and pervasive encryption.
- Whether you're considering an operating system upgrade, platform change or acquiring a new system IBM Z machine, IBM Z Systems Service and Support can help you plan, install, configure, migrate and test the new environment. Deploying a private cloud and/or hybrid cloud requires a roadmap for future growth and plans for cloud expansion—this includes a trusted, highly secure, organic platform—IBM Z Systems and security.

Sources: 1). NCC Group, Whitepaper, "Understanding and Hardening Linux Containers, 2016. 3). HPE Annual Report, 2018.
2). HotHardware, "Intel Skylake, Kaby Lake Processors Vulnerable To USB Port Debugging Exploit Says Researchers", Jan. 10, 2017.

