Enterprise IT in the age of sophisticated cyberattacks

Highly publicized and devastating data breaches have brought security to the forefront of many executives' attention today. This has resulted in security budgets growing across organizations. But, at least in part, increased spending and technological change has introduced new complexities and risks that threaten IT security. A 2019 Forrester survey of security professionals found that "fewer than a quarter" are "completely satisfied with their security portfolios in supporting them to develop advanced threat intelligence capabilities; increase productivity of security staff; extract insight from data; and drive efficiencies."[1]

Chief among security professionals' concerns is the growing number and sophistication of attacks, which exposes more aspects of today's businesses than ever before. Vulnerabilities in the hardware and firmware levels may not have been points of great concern in the not-too-distant past; now, however, they find themselves prime targets.

Threats, meanwhile, will continue to multiply as IT architectures evolve. In many ways, the cyber security challenges your business must overcome today can be distilled down to two empirical truths: The IT stack is expanding and—as a direct result—hackers are broadening their horizons.

The realities of the current threat landscape

Organizations today rely on their security systems to prevent threats to intellectual property, sensitive corporate information, sensitive personal information, and privacy. How they strategically approach IT security is an imperative.

Often, this is achieved by adopting a business-, compliance- or monetary-driven approach. While this approach holds value, alone it does not provide adequate protection for business processes against the increasing number of IT systems risks. It possibly overlooks key cross-discipline aspects as well.

The ideal course of action involves planning and assessment to identify risks across key areas related to security. IBM Power Systems™ and the POWER9 processor offer a holistic, multilayered approach for your security strategy to ensure your organization is secure and compliant. This multilayered approach includes

- Hardware
- Firmware
- Hypervisor
- Operating system
- PowerSC

Adopting a holistic security approach enables your organization to meet the demands of four realities currently affecting the security landscape.

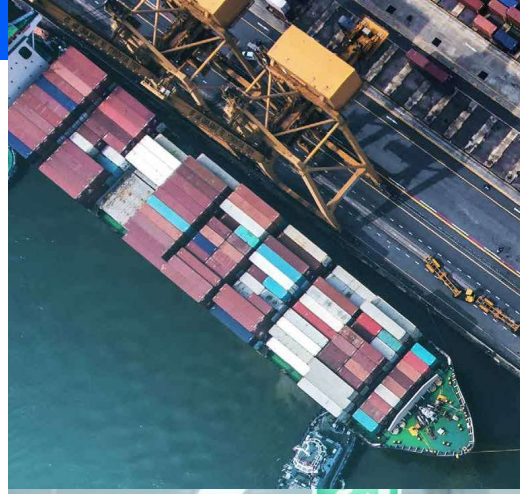
Hackers are growing more sophisticated. The more an organization moves outside the limitations of traditional on-premises data centers, the more space cyberattackers have to think outside the box. Their methods are no longer contained to the network level, leading to broadened horizons and more capable attacks.

More business is being conducted on mobile and edge devices. Data within an organization can now be stored and accessed by employees from practically anywhere—across servers, hybrid cloud environments and numerous mobile and edge devices. This inextricable crisscrossing of server and device is the byproduct of ongoing digital transformation—but it creates a whole new attack vector ready to be exploited.

Tighter regulation is affecting risk profiles. The processes being put in place to help ensure regulatory compliance can also lead to unintended risk exposure. And the EU's GDPR is merely one recent development of a growing trend: Governing entities are paying much closer attention to how your organization uses data. But they also add layers of complexity to the daily operations of your business.

Employees are vulnerabilities waiting to happen. Your workforce will always pose some level of risk—no matter what security controls you put in place or how well you handle vulnerabilities. The hard work you put into securing end points and adhering to compliance can be rendered moot by an unintentional mistake or a clever malicious attack. Meanwhile, many organizations struggle to find and retain competent security staff, and they find themselves stuck with a perpetual skills shortage.

The volume, variety and velocity of today's cyber threats are only going to multiply as IT architectures continue to evolve and adapt to the changing tides of technology, work culture and compliance. And that means your security strategy must also evolve to reach beyond the network level.



A holistic, multi-layered approach to security is required

Building security into every level of your stack is achievable by implementing various third-party vendor security solutions. However, that approach compounds the complexity that already exists—and introduces even more vulnerabilities and points of exposure into your network. Your best recourse is to take a multi-layered, holistic approach, one that secures all of your organization's data and systems while also minimizing complexity.

With that in mind, IBM created the IBM Security Framework to help ensure that every IT security aspect can be properly addressed when using a holistic approach to business-driven security.

The IBM Security Framework focuses on:

1. **Infrastructure**—Safeguard against sophisticated attacks with insight into users, content and applications.
2. **Advanced security and threat research**—Gain knowledge of vulnerabilities and attack methodologies and apply that insight via protection technologies.
3. **People**—Manage and extend enterprise identity across security domains with comprehensive identity intelligence.
4. **Data**—Secure the privacy and integrity of your organization's most trusted assets.
5. **Applications**—Reduce the cost of developing more secure applications.
6. **Security intelligence and analytics**—Optimize security with additional context, automation and integration.

Learn more about the IBM Security Framework and how you can drill down even further with the IBM Security Blueprint.

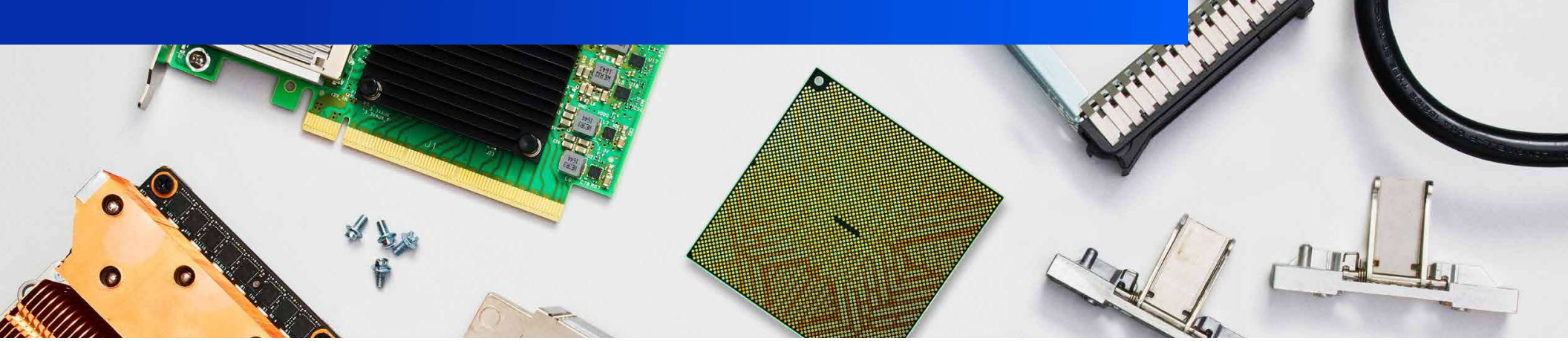
How IBM Power Systems and POWER9 secure the stack

With IBM Power Systems, you get comprehensive end-to-end security that tightly integrates across the entire stack—from processor and firmware, to OS and hypervisors, to apps and network resources, all the way to security system management.

Hardware, firmware, and hypervisor

24 cryptographic engines

The POWER9 processor holds twice as many cryptographic engines as its POWER8® predecessor. You can encrypt data at rest or in motion at double the speed or faster across all layers of the stack.



On-chip accelerators

POWER9 boasts on-chip accelerators that compress and decompress GZIP files much faster than software. You can quickly compress and encrypt entire VMs and securely move them across the network.

Secure boot on POWER9

Secure boot protects system integrity by verifying and validating all firmware components via digital signatures. All firmware released by IBM is digitally signed and verifiable. You can also install your own firmware and replace the hierarchy of public keys needed for verification.

Trusted boot and Trusted Platform Module (TPM)

The trusted boot feature in POWER9 allows for the inspection and remote verification (attestation) of all firmware components on your server. The trusted boot feature uses the TPM, which serves as the Root of Trust (RoT) for measuring the software stack. Verification is signed by the TPM itself, so you know the firmware hasn't been tampered with in any way.

IBM PowerVM® enterprise hypervisor

IBM PowerVM has an excellent security track record when compared against major competitors, so you can confidently secure your virtual machines (VMs) and cloud environments.

Operating system

IBM Power Systems offers leading security capabilities for a wide range of operating systems like IBM AIX®, IBM i and Linux®. Features vary depending on the OS, but examples of these capabilities include being able to:

- Assign administrative functions typically reserved for the root user without compromising security
- Encrypt file-level data through individual key stores
- Gain greater control over the commands and functions available to users, along with control over what objects they can access
- Log access to an object in the security audit journal by using system values and the object auditing values for users and objects
- Carry encryption across an entire drive, first encrypting an object and then writing out in the encrypted form
- Measure and verify every file before it runs or opens for the requesting user

Workloads, VMs and containers

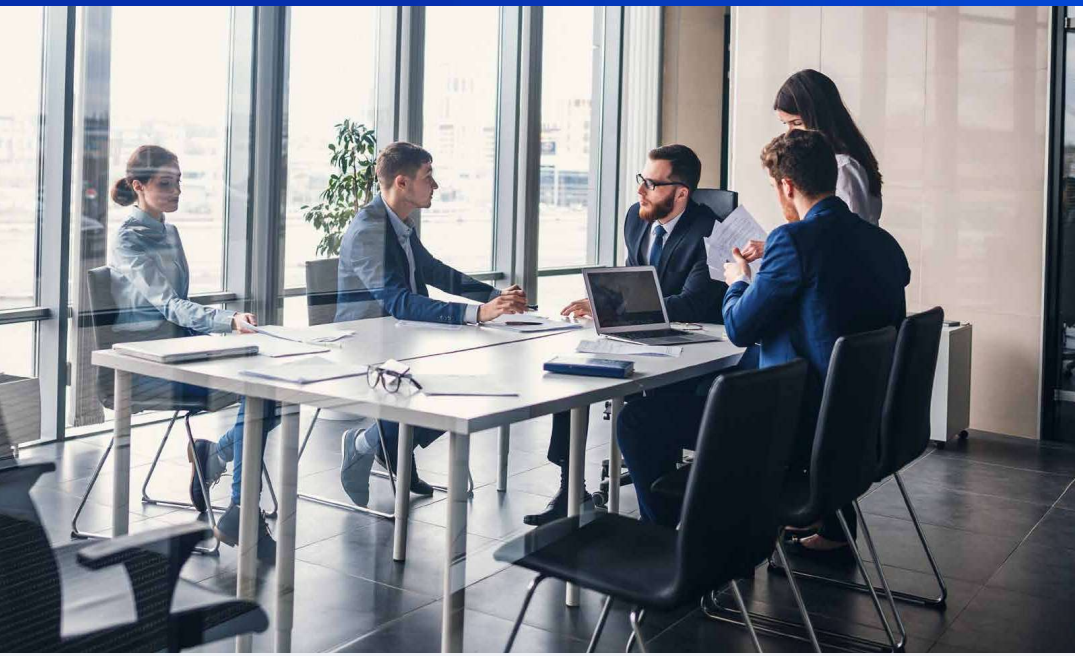
Workloads are no longer restricted to on-premises data centers; they're continually moving to virtualized and cloud environments. This means that many organizations are adopting containers to deploy new and existing applications across hybrid infrastructures. These increasingly dynamic environments and workloads require equally versatile security capabilities.

Live Partition Mobility (LPM)

IBM Power Systems lets you secure data in motion. LPM protects VMs through encryption when you need to migrate from one system to another. If you have virtualized on-premises data centers and/or hybrid cloud environments, this capability is critical.

Protected Execution Facility

The Protected Execution Facility is one example of how IBM Power Systems protects this level of the stack. It's a POWER9 feature that encrypts and runs your VMs in secure memory, meaning a compromised hypervisor will not have access. Additionally, in a cloud environment, malicious insiders or administrators with access to the VM will not have access to the workloads running in the secure memory. The decryption process only happens on a verified system.



The most powerful approach to security is a streamlined one

As the capabilities of hackers become even more sophisticated and technological evolution introduces new vulnerabilities into today's businesses, integrating a multi-layered, holistic security solution that doesn't add to your organizational complexity is key. IBM Power Systems protects every level of your stack with the tightly integrated, in-depth solutions of a single vendor. A security strategy that relies on a multitude of components from multiple vendors introduces complexities that can ultimately prove costly—in more ways than one.

Security from a single vendor provides natural advantages that simplify and strengthen your security strategy. Building on three decades of security leadership, IBM Power Systems brings with it extensive partnerships with other organizations in and outside of IBM that further deepen and broaden its security expertise. These partnerships enable IBM Power Systems to tap into an even bigger community of security professionals and ensure that issues can be identified quickly and addressed with confidence. And with the backing of the IBM Security and IBM Research business units, along with the PowerSC portfolio, POWER9 servers thwart multiple threats, including insider attacks, from top to bottom.

Streamline your security across the entire stack with a holistic, multi-layered approach—and keep your business secure.

To learn more about how POWER9 servers can help secure your infrastructure, contact your IBM representative or IBM Business Partner.

1. "Complexity In Cybersecurity Report 2019: How Reducing Complexity Leads To Better Security Outcomes," Forrester Research, Inc., May 2019

© Copyright IBM Corporation 2019. U.S.

IBM Systems, 11501 Burnet Road, Austin, Texas 78758

Government Users Restricted Rights—Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
NOTE: IBM web pages might contain other proprietary notices and copyright information that should be observed.

IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml.

33028633USEN-00