A multilayered approach to security with IBM Power

Essential infrastructure for a zero trust approach

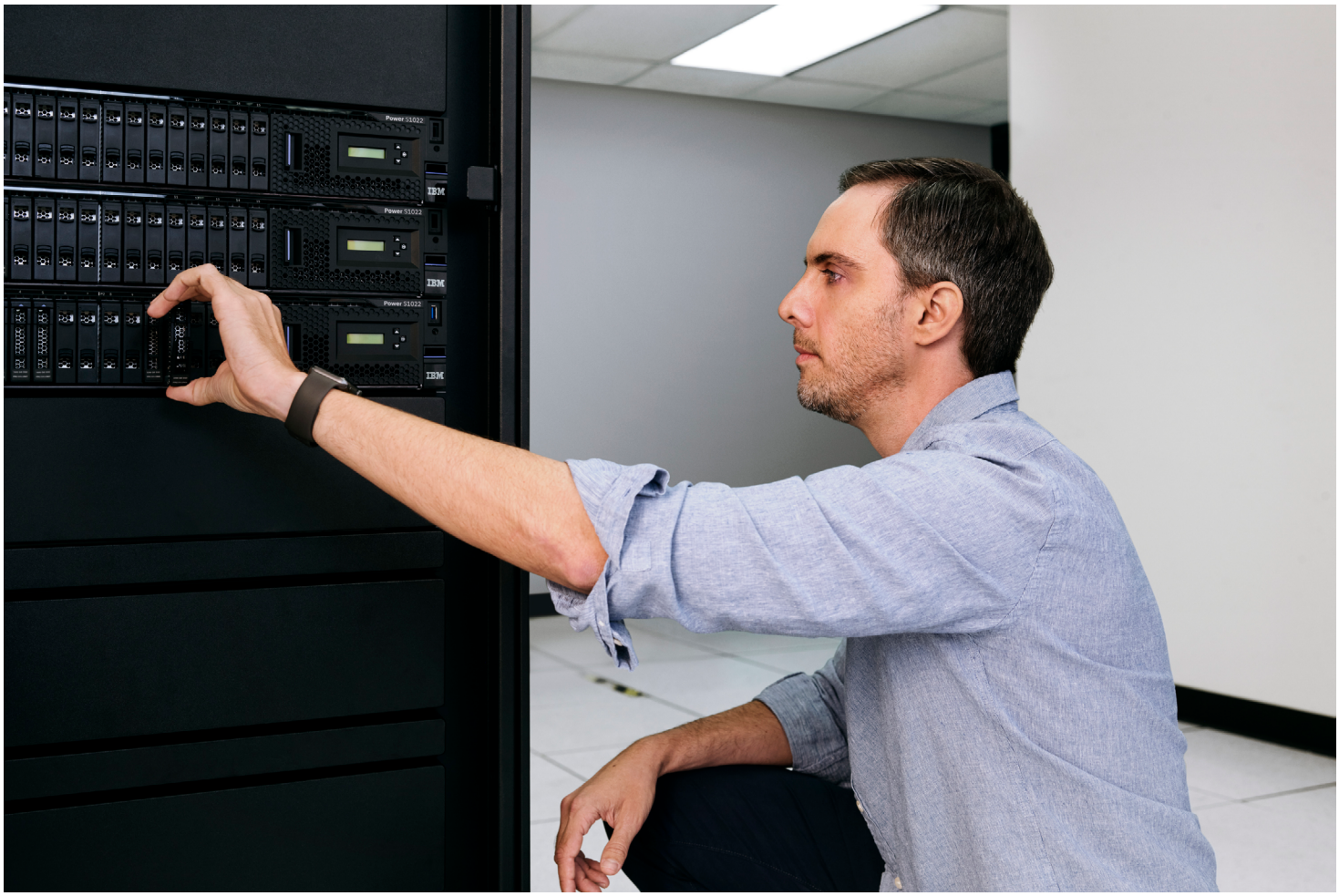


Table of contents

Enterprise IT in the age of sophisticated cyberattacks

Today’s IT landscape

Since the beginning of the COVID-19 pandemic, a staggering number of devastating data breaches have been recorded. The average cost of a data breach is now USD 4.24 million, up 10% from last year’s reported USD 3.86 million. This is the largest increase that the industry has witnessed in the last seven years[1], making security a top concern. Improving your security strategy and enabling your business to move quickly, safely and securely in this always-on world is the focus for many executives today, resulting in increased security budgets. However, increased spending and technological change introduces new complexities and risks that continue to threaten IT security. One of security professionals’ top concerns is the growing number of sophisticated attack vectors which continue to e xpose 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’re prime targets in today’s threat landscape.

In many ways, the cybersecurity challenges your business must overcome today can be distilled down to two empirical truths:

- The IT stack is expanding and hackers are broadening their horizons.
- Organizations must stay ahead of future threats to protect their platforms with the highest level of security to safeguard their hybrid cloud infrastructure.

USD 4.24 M

The average cost of a data breach is now **USD 4.24 million, up 10%** from last year’s reported USD 3.86 million.

The realities of the current threat landscape

A holistic approach

Enterprises rely on their security systems to prevent current and future threats to intellectual property, sensitive corporate information, customer data and workload privacy.

How professionals strategically approach IT security is imperative to prevent data breaches and cyberattacks. Not only can security vulnerabilities lead to downtime, but they are costly to any organization. Ransomware attacks pose the largest threat, costing enterprises USD 4.62 million per attack on average[1]. The IBM® Power® platform's integrity can reduce the risk of ransomware by implementing endpoint detection and response (EDR), and zero trust concepts such as continuous multifactor authentication (MFA).

Adopting a business-driven, compliance-driven or monetary-driven approach alone cannot provide adequate protection for business processes against the increasing number of IT systems risks. Solitary approaches can overlook key cross-discipline aspects of an efficient and integrated security strategy. The ideal course of action involves planning and assessment to identify risks across key areas related to security. IBM Power technology and IBM® Power10 processor-based systems offer a holistic, zero trust, multilayered approach for your security strategy to ensure your organization is secure and compliant. This multilayered approach includes:

- Hardware
- Operating system
- Firmware
- IBM® PowerSC 2.0 technology
- Hypervisor

Adopting a holistic security approach can enable your organization to meet the demands of the threats affecting the security landscape.

Hackers are growing more sophisticated

The more an organization moves outside the limitations of traditional on-premises data centers and transition to hybrid cloud or multicloud environments, the more space cyberattackers have to think outside the box. Implementing least privilege and augmenting perimeter-based controls will help to manage the increased number of threats. Their methods of the past are no longer contained at the network level, leading to broadened horizons and more capable attacks.

Security is vital as data access increases

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 and modernization. As a result, this accessibly creates a plethora of attack vectors 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. General Data Protection Regulation (GDPR) is merely one such recent development of a growing trend. Governing entities are paying much closer attention to how organizations use data. Yet they also add layers of complexity to the daily business operations.

Employees are vulnerabilities waiting to happen

Employees' compromised credentials are at fault for 20% of all data breaches last year[1]. Aside from login information, phishing scams and email compromise are other ways employees unknowingly put company information at risk. Your workforce will always pose some level of risk — no matter what security controls you put in place or how well you handle vulnerabilities. In the era of cybercrime, it is imperative to train employees on these common security threats and have a reporting system in place. The hard work you put into securing endpoints and adhering to compliance can be rendered moot by a mistake or a clever malicious attack.

Meanwhile, many organizations struggle to find and retain competent cybersecurity staff, and they find themselves stuck with a perpetual skills shortage. To combat such skill shortages, organizations can implement simplified security management that automates operations, compliance, patching and monitoring. Benefit from end-to-end security designed to protect with additional endpoint detection without the additional resources.

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

A zero trust strategy is essential

A holistic approach

Implementing zero trust concepts can help organizations address security in an often-complex IT environment. IT professionals struggle with visibility and control across hybrid cloud and multicloud landscapes. Zero trust manages the risks by shifting to a more comprehensive strategy that restricts access controls while not impacting performance or user experience. Building security into every level of your stack can be achievable by implementing various third-party vendor security solutions. However, that approach worsens the complexity that already exists — and introduces even more vulnerabilities and points of exposure into your network. Your best recourse is to take a multilayered, zero trust approach. This secures all of your organization's data and systems, while also minimizing complexity. With that in mind, the IBM® Information Security Framework helps ensure that every IT security aspect can be properly addressed when using a holistic approach to business-driven security.

The IBM Information 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.
7. Zero trust philosophy – Connect and protect the right users to the right data while protecting your organization.

Learn more about IBM Security Framework (PDF, 25.2 MB) and how you can drill down even further.

How IBM Power technology secures the stack

Explore IBM Power

With IBM Power technology, you can increase cyber resiliency and manage risks with comprehensive end-to-end security that 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

On-chip accelerators
The IBM Power10 processor chip is designed to enhance side-channel mitigation performance and is equipped with improved CPU isolation from service processors. This 7nm processor is designed to deliver up to a 3x increase in capacity resulting in greater performance[2].

End-to-end encryption
The transparent memory encryption of IBM Power solutions is engineered to enable end-to-end security that meets the demanding security standards enterprises face today. It is also designed to support crypto acceleration, quantum-safe cryptography, and full homomorphic encryption to guard against future threats. The accelerated encryption for the newest IBM Power system model has 2.5x faster Advanced Encryption Standard (AES) crypto performance per core than that of IBM Power E980 technology[3]. Organizations can benefit from transparent memory encryption with no additional management setup.

EDR software
The increase in external threats makes endpoint security critical when it comes to protecting customer data and digital assets. By detecting any potential threats at the endpoint, organizations can act quickly and resolve incidents without disrupting business continuity. An integrated approach eliminates complications and secures your organization from even the most dangerous attacks.

2.5x

The accelerated encryption for the newest IBM Power system model has **2.5x faster Advanced Encryption Standard (AES) crypto performance per core** than that of IBM Power E980 technology[3].

Enabling principles such as multifactor authentication and least privilege bring added protection by securing all APIs, endpoints, data and hybrid cloud resources.

Zero trust principles
Organizations are evolving to adopt zero trust principles to help manage these growing threats. Enabling principles such as multifactor authentication and least privilege bring added protection by securing all APIs, endpoints, data and hybrid cloud resources.

The IBM zero trust framework brings this concept to life.

- **Gather insights** – Understand users, data and resources to create the security policies needed to ensure complete protection.
- **Protection** – Protect the organization by quickly and consistently validating context and enforcing policies.
- **Detection and response** – Resolve security violations with minimal impact to business operations.
- **Analyze and improve** – Continually improve security posture by adjusting policies and practices to make more informed decisions.

By implementing zero trust principles, businesses can innovate and scale, safely.

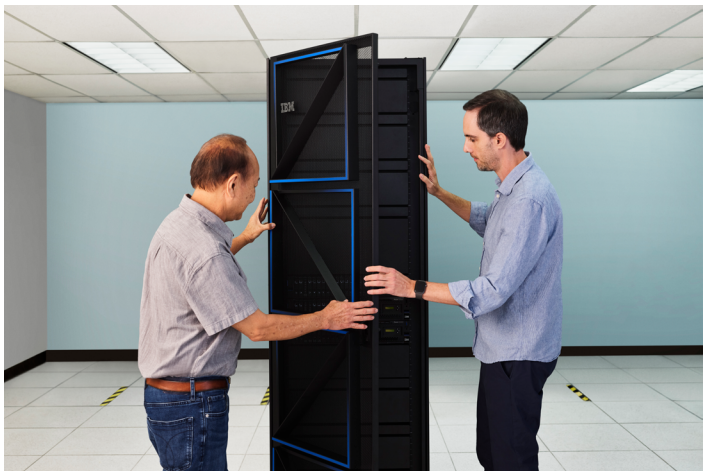
Secure boot on IBM Power10 solutions
Secure boot is designed to protect system integrity by verifying and validating all firmware components via digital signatures. All firmware released by IBM is digitally signed and verified as part of the boot process. All IBM Power systems come with a trusted platform module that accumulates measurements of all firmware components loaded on a server allowing for their inspection and remote verification.

IBM PowerVM enterprise hypervisor
IBM PowerVM® enterprise hypervisor 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®. EDR for IBM Power technology can provide additional security for VM workloads, ensuring complete protection at every endpoint within the network. For systems that rely on passwords to be secure, the AIX and Linux operating systems utilize IBM PowerSC multifactor authentication (MFA) that require additional levels of authentication for all users, protecting against password cracking malware. The 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 opens for the requesting user



Workloads, VMs and containers

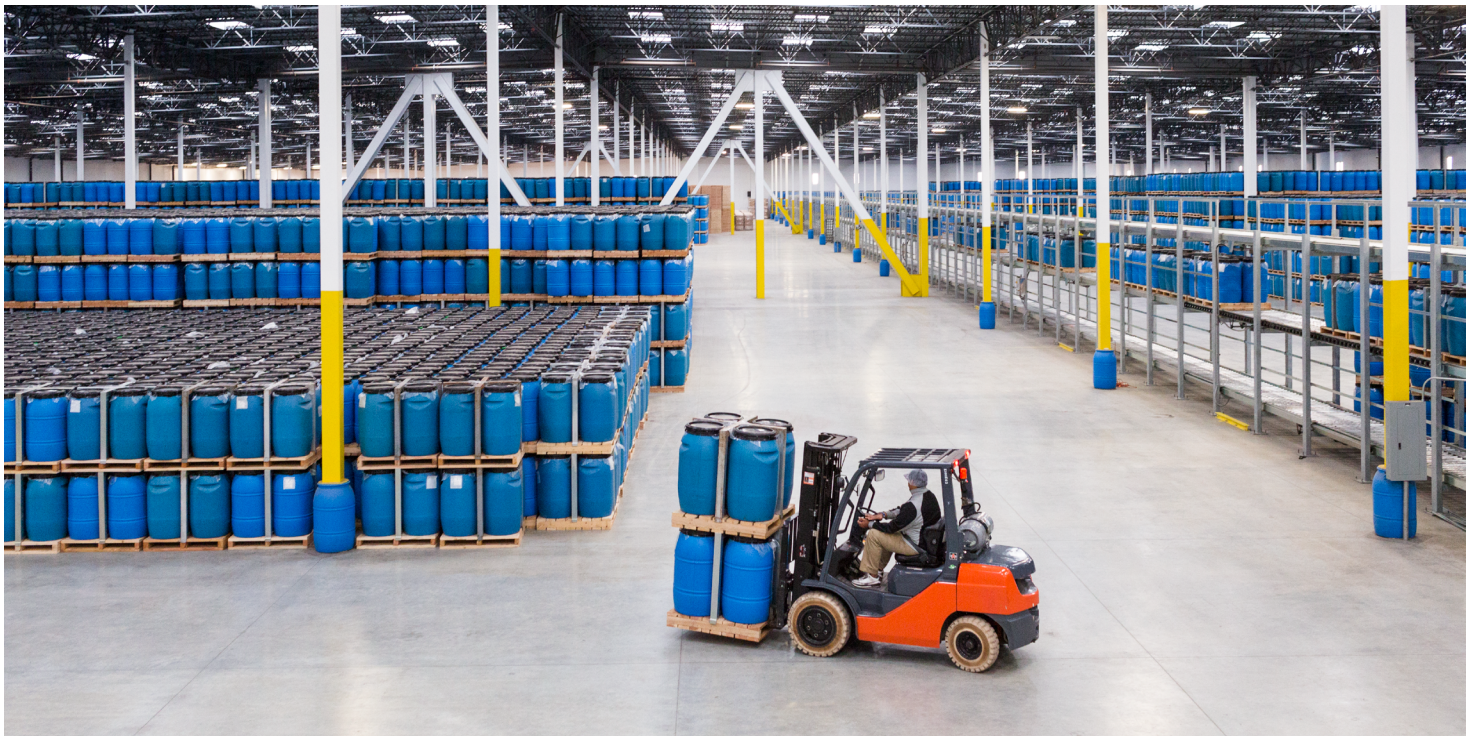
Workloads are no longer restricted to on premises data centers; they're continually moving to virtualized hybrid cloud and multicloud environments. As an example, many organizations are adopting containers to deploy new and existing applications across hybrid infrastructures.

These increasingly dynamic environments and workloads require equally versatile security capabilities. IBM Power solutions can meet security needs by preserving workload privacy with cryptographic algorithm acceleration, secure key storage and CPU support for post quantum cryptography and fully homomorphic encryption (FHE) cryptographic algorithms.

To address the unique security requirements of containerized deployments, IBM has also partnered with independent software vendors (ISVs) like Aqua Security, who builds with IBM Power technology and Red Hat® OpenShift® Container Platform to further secure containers throughout their lifecycle.

IBM Power servers are designed to protect data from on premises to cloud with end-to-end memory encryption and accelerated cryptographic performance. The policies that are embedded for cloud native workloads including VMs, containers and serverless functions are built to support Red Hat OpenShift and IBM Power customers when integrating their security and compliance requirements for application modernization.

Live Partition Mobility (LPM)
IBM Power technology 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, hybrid cloud environments or both, this capability is critical.



Integrated security products on IBM Power solutions

IBM PowerSC 2.0 technology

IBM® PowerSC 2.0 technology is an integrated portfolio offering for enterprise security and compliance in cloud and virtual environments. It lives on top of your stack while providing a web-based UI for managing the security features of IBM Power technology that reside from the lowest level up solutions.

With its simplification and automation capabilities, IBM PowerSC 2.0 technology can reduce time, cost and risk by streamlining compliance monitoring and enforcement. This solution can support audit processes and allows customers to achieve compliance certifications more efficiently. It can also reduce security risks by increasing visibility across the stack.

Features of IBM PowerSC 2.0 Standard Edition

Multifactor authentication (MFA) technology
MFA is now integrated into IBM PowerSC 2.0 solutions. This simplifies the deployment of MFA mechanisms following the zero trust principle of “Never trust, always verify.” This approach supports alternative factors for users to login with RSA SecurID-based authentication and certificate authentication options including common access card (CAC) and personal identification verification (PIV) cards. IBM PowerSC MFA raises assurance levels of systems by requiring extra authentication factors for users.

IBM PowerSC 2.0 technology can reduce time, cost and risk

EDR capabilities
IBM PowerSC 2.0 solutions introduces EDR for Linux on IBM Power workloads, offering the latest, industry standard capabilities for managing endpoint security, including, intrusion detection and prevention, log inspection and analysis, anomaly detection and incident response.

Compliance automation
The IBM Power family comes with prebuilt profiles that support a myriad of industry standards. You can customize these profiles and merge them with enterprise rules without having to touch Extensible Markup Language (XML).

Real-time compliance
Detects and alerts you when someone opens or interacts with security-critical files.

Trusted network connect
Alerts you when a VM is not at the prescribed patch level. It also notifies you when fixes become available.

Trusted boot
Allows for the inspection and remote verification of the integrity of all the software components running on AIX logical partitions.

Trusted firewall
Protects and routes internal network traffic between the AIX, IBM i and Linux operating systems.

Trusted logging
Creates centralized audit logs, which are easy to backup, archive and manage.

Preconfigured reporting and interactive timeline
The IBM PowerSC Standard Edition supports auditing with five preconfigured reports. You also have an interactive timeline to see the life and events of a VM.

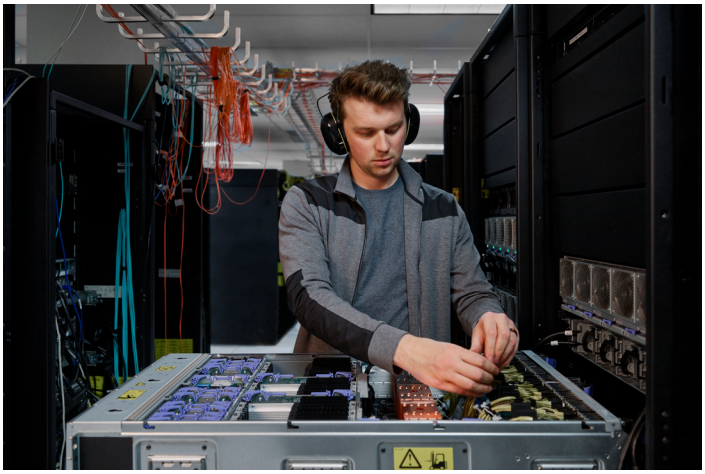
Learn how to simplify management of IT security and compliance with IBM PowerSC in Cloud and Virtualized environments

The most powerful approach to security is a seamlessly integrated one

Seamless integration

As cybercriminals continue to advance their methods and technological evolution introduces new vulnerabilities into today's businesses, integrating a multilayered, zero trust, security solution that doesn't add to your organizational complexity is key. IBM Power solutions can protect every level of your stack from edge to cloud to core with the tightly integrated, in-depth solutions of a single vendor. Working with multiple vendors introduces complexities that can ultimately prove to be costly — in more ways than one. IBM Power technology supports end-to-end encryption at the processor level without impacting performance. Integrating your infrastructure brings every layer of the stack into focus.

Security from a single vendor can provide natural advantages that simplify and strengthen your security strategy. Building on three decades of security leadership, IBM Power technology brings with it extensive partnerships with other organizations in and outside of IBM that further deepen and broaden its security expertise. These partnerships can enable IBM Power technology 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 2.0 portfolio, Power10 servers can thwart multiple threats, including insider attacks, from top to bottom.



Schedule a consultation to explore the potential of IBM Power solutions

Contact us →

Notes
1. Cost of a Data Breach Report 2021, IBM Security, July 2021 (PDF, 3.6 MB)
2. 3X performance is based upon pre-silicon engineering analysis of Integer, Enterprise and Floating Point environments on a POWER10 dual socket server offering with 2×30-core modules vs POWER9 dual socket server offering with 2×12-core modules; both modules have the same energy level. 2 10-20X AI inferencing improvement is based upon pre-silicon engineering analysis of various workloads (Linpack. Resnet-50 FP32, Resnet-50 BFloat16, and Resnet-50 INT8) on a POWER10 dual socket server offering with 2×30-core modules vs POWER9 dual socket server offering with 2×12-core modules.
3. AES-256 in both GCM and XTS modes runs about 2.5 times faster per core when comparing IBM Power10 E1080 (15-core modules) vs. IBM POWER9 E980 (12-core modules) according to preliminary measurements obtained on RHEL Linux 8.4 and the OpenSSL 1.1.1g library

IBM Cloud
IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
June 2022