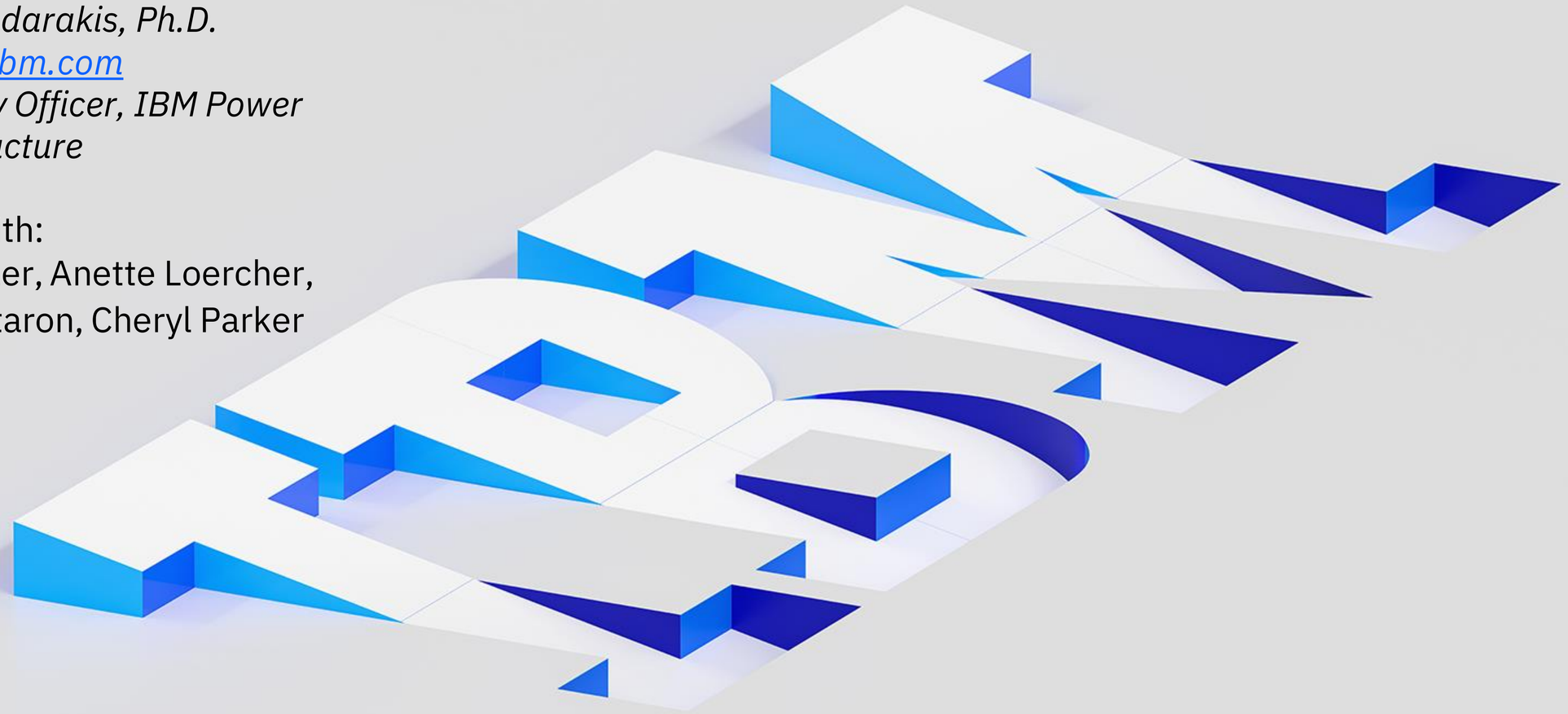
Security for SAP on IBM Power

Dimitrios Pendarakis, Ph.D.
dimitris@us.ibm.com
Chief Security Officer, IBM Power
IBM Infrastructure

Joint work with:
Ramy Buechler, Anette Loercher,
Laurent Montaron, Cheryl Parker



What is at Stake?
Key findings from IBM’s Cost of a Data Breach Report 2023

Average cost of a data breach reached a record high in 2023, but security investments at organizations are divided

USD 4.45 million
Average cost of a data breach

USD 10.93 million
Average cost of a breach in healthcare, the highest for 13 years in a row

51%
Organizations that planned to increase security investments as a result of a breach, with top investments in incident response (IR) planning and testing, employee training, and threat detection and response

Costs were highest and breaches took longer to contain when breached data was stored across multiple environments

39%
Amount of breached data stored across multiple types of environments including public, private and hybrid clouds and on premises

USD 750,000
Amount of higher breach costs when breached data was stored across multiple environments versus on premises only

292 days
Breach response time when data was stored across multiple environments, 15 days longer than the overall average for containing a breach

How do these findings apply to SAP Deployments?

SAP Application Security
What is the value to clients?

SAP systems are mission-critical applications and a primary target for threat actors that try to exploit vulnerabilities and threats

Companies need to demonstrate compliance in their SAP systems with financial regulations that request access and data protection controls

85%

Percentage of the Forbes 500 companies that run SAP

65%

SAP clients had a breach in the past 24 months

$9.44M

Average total cost of a data breach in the US in 2022

26%

Percentage of 2022 vulnerabilities with known exploits

- Source: 1. IBM Cost of a Data Breach Report 2022: United States
- Source: 2. SAP.com
- Source: 3. IBM Security X-Force Threat Intelligence Index 2023

Why is Security for SAP systems so important?

"Myth Busters" for SAP …

- As a commercial product SAP brings Security by default
- When implementing standard functionality, without customizations, SAP is secured by default

Unfortunately, it is not so simple

SAP brings Security features … but that doesn't mean it is secure by default. These features need to be properly setup and configured …

- **Access Management**: Extensive Options → Potential Open Doors
- **Custom Code**: SAP runs on top of a development framework
- **Configuration**: Hundreds of security parameters
- **Multiple Interfaces**: On-premise, private and public cloud systems
- **Integration** with other systems, including non-SAP
- **Compliance** with corporate security requirements
- **Fines**: what is the cost of non-compliance with external regulations

Market starts to understand the risk exposure

Concerns of Forbes-500 CIO's & CISO's

92% indicated an SAP breach would be **serious, very serious or catastrophic**

65% had **SAP system breached** in the *past 24 months*

47% "not confident" or had **"no confidence" they could detect an SAP breach** within a year

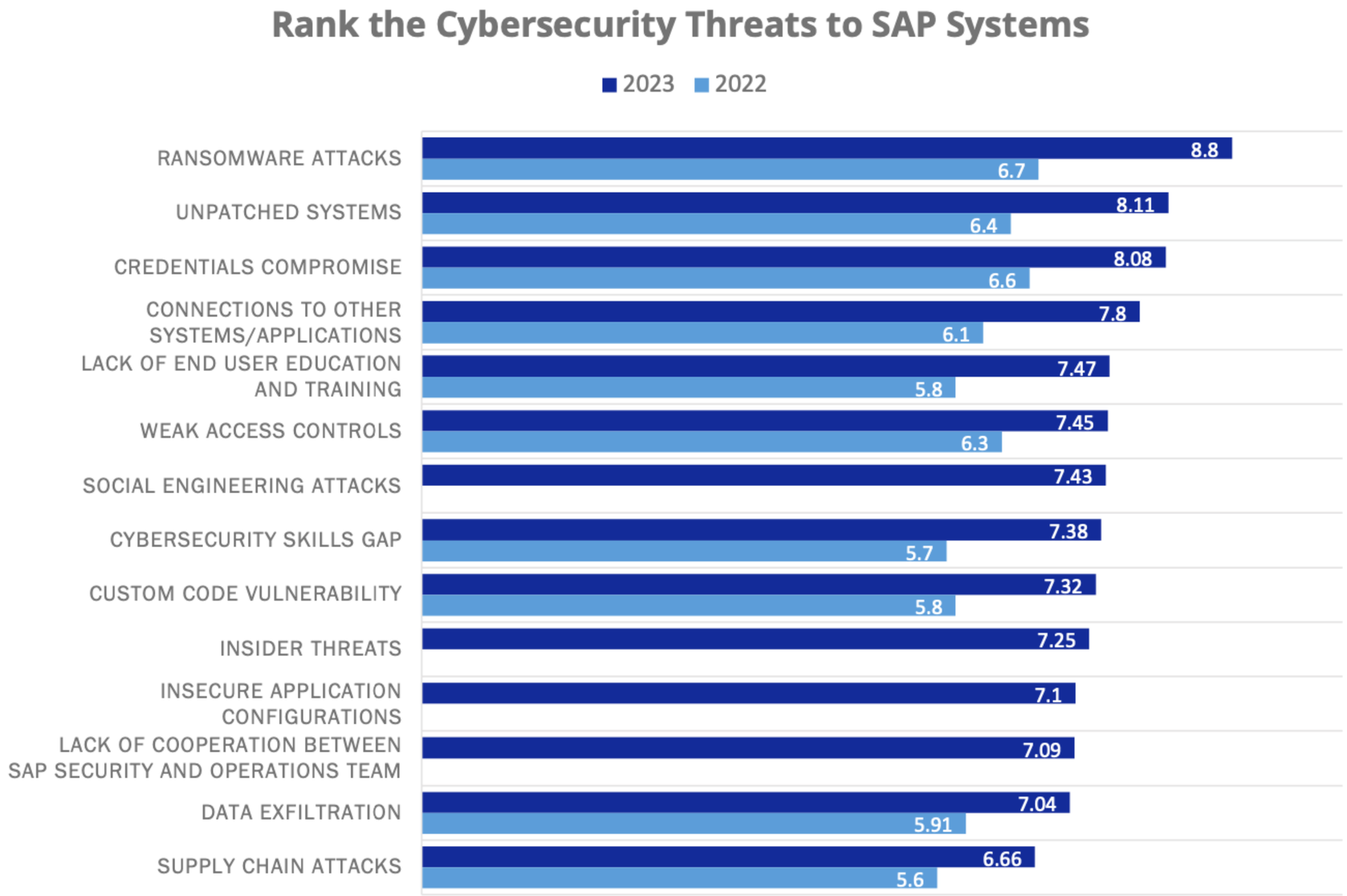
4.5M **Average cost to take SAP offline** because of a Security incident

59% believe Cloud, HANA, Fiori, IOT all **increase likelihood of an attack**

SAPinsider Cybersecurity Threats to SAP Systems: Detailed Findings

Ransomware attacks remain the biggest potential threat, but this is closely followed by unpatched systems and a potential credentials compromise — both of which potentially open SAP systems to attacks that can compromise or expose data.

Put a patching strategy in place that ensures that critical vulnerabilities are patched in a timely manner. Consider leveraging application lifecycle management tools to help automate patching processes.

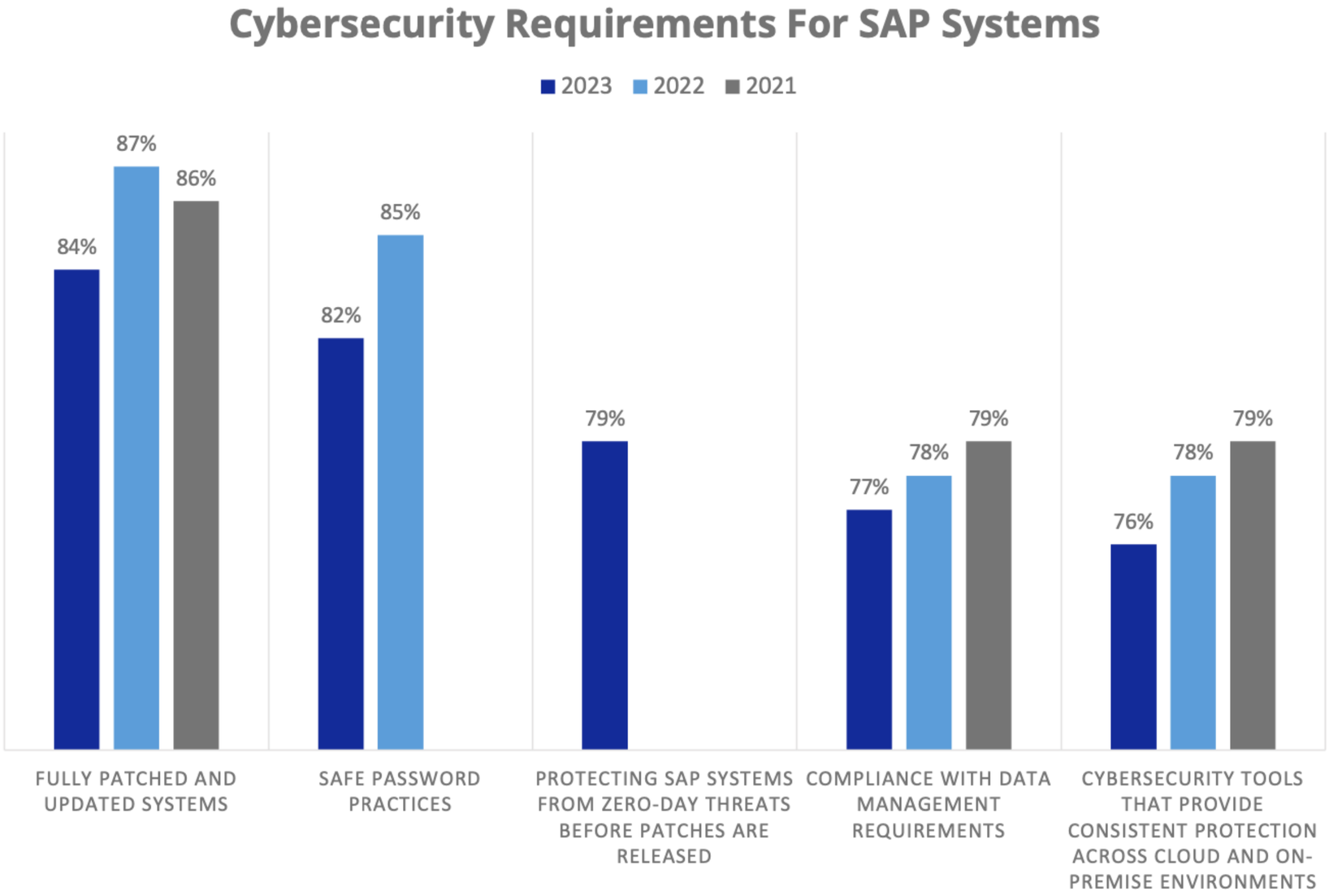


Source: https://sapinsider.org/research-report/cybersecurity-threats-to-sap-systems-benchmark-report/

SAPinsider Cybersecurity Threats to SAP Systems: Detailed Findings

Having fully patched and updated systems continues to be the most important cybersecurity requirement for SAP systems for the third consecutive year, with safe password practices being almost as important.

Protecting SAP systems from zero-day threats before patches are released, a new option for 2023, immediately became the third most important requirement showing just how concerned respondents are about newly discovered vulnerabilities being exploited.

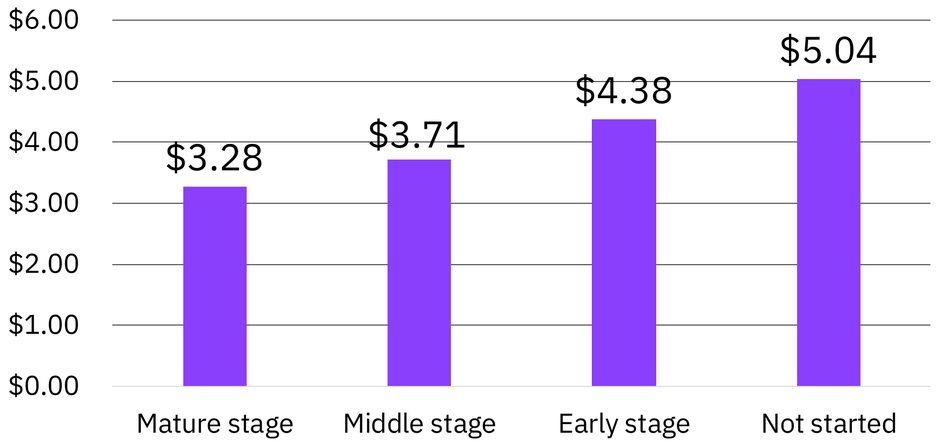


Source: https://sapinsider.org/research-report/cybersecurity-threats-to-sap-systems-benchmark-report/

Key Findings from IBM's Cost of a Data Breach Reports:
Reducing the Cost Impact of Breaches

Key principles of zero trust:

- Implement least privilege
- Augment perimeter-based controls
- Never trust, always verify
- Assume breach
- Continuous improvement



The average cost of a breach through Zero Trust Maturity in US$ millions

Source: "Cost of a Data Breach Report 2021", IBM & Ponemon Institute

Using a DevSecOps approach, deploying IR teams, security AI and automation produced large savings

USD 1.68 million

Savings for organizations using a DevSecOps approach at a high level compared to other organizations at a low level or no use of DevSecOps

USD 1.49 million

Savings for organizations with an IR team and regularly tested IR plan versus no IR team or IR testing

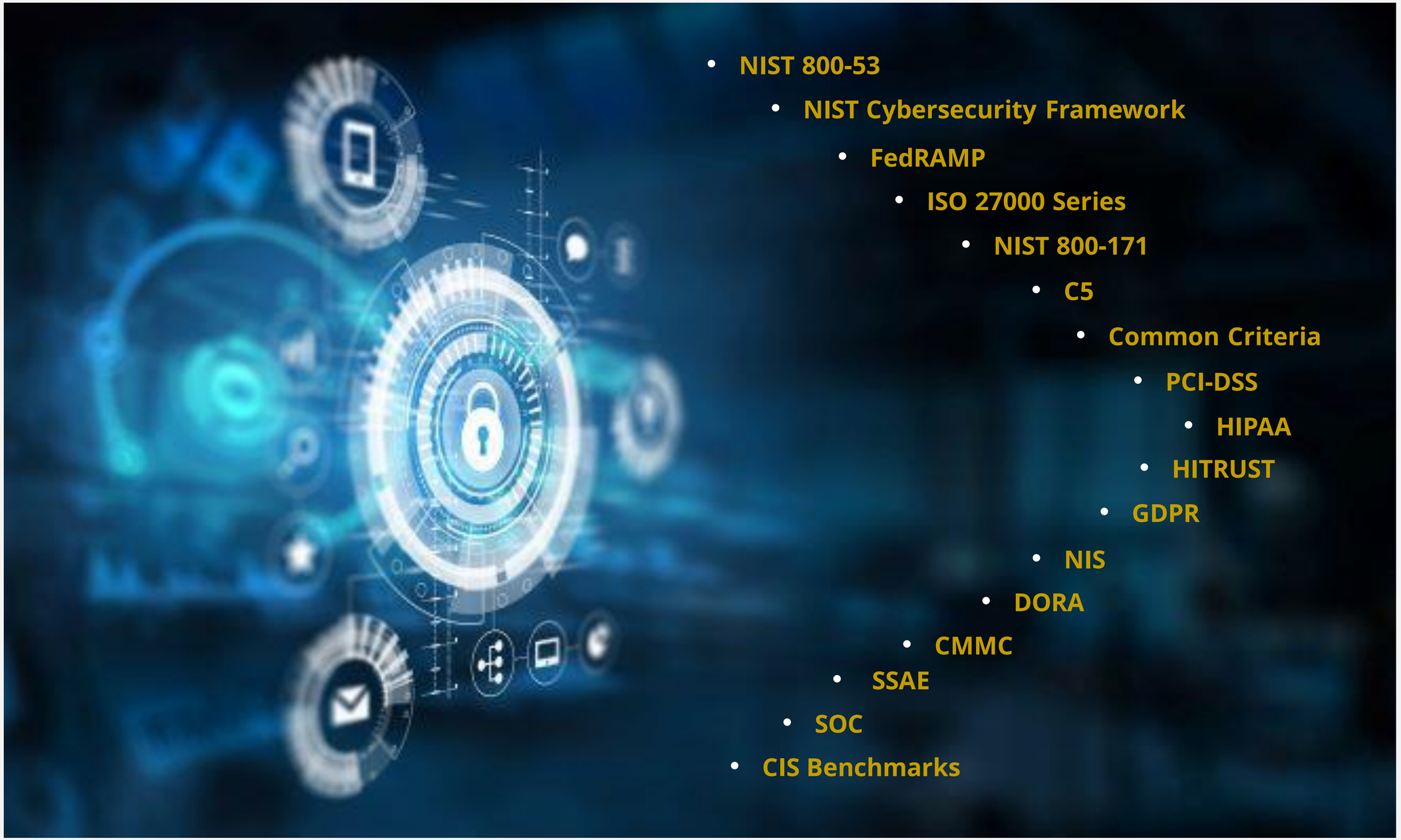
108 days

Breach response time saved for organizations with extensive use of security AI and automation

USD 1.76 million

Savings for organizations with extensive use of security AI and automation compared to organizations with no security AI or automation deployed

Multitude of Cybersecurity Standards, Frameworks, and Compliance Regulations



How to ensure we bring the proper level of Security for SAP workloads?

13 layers of SAP Security

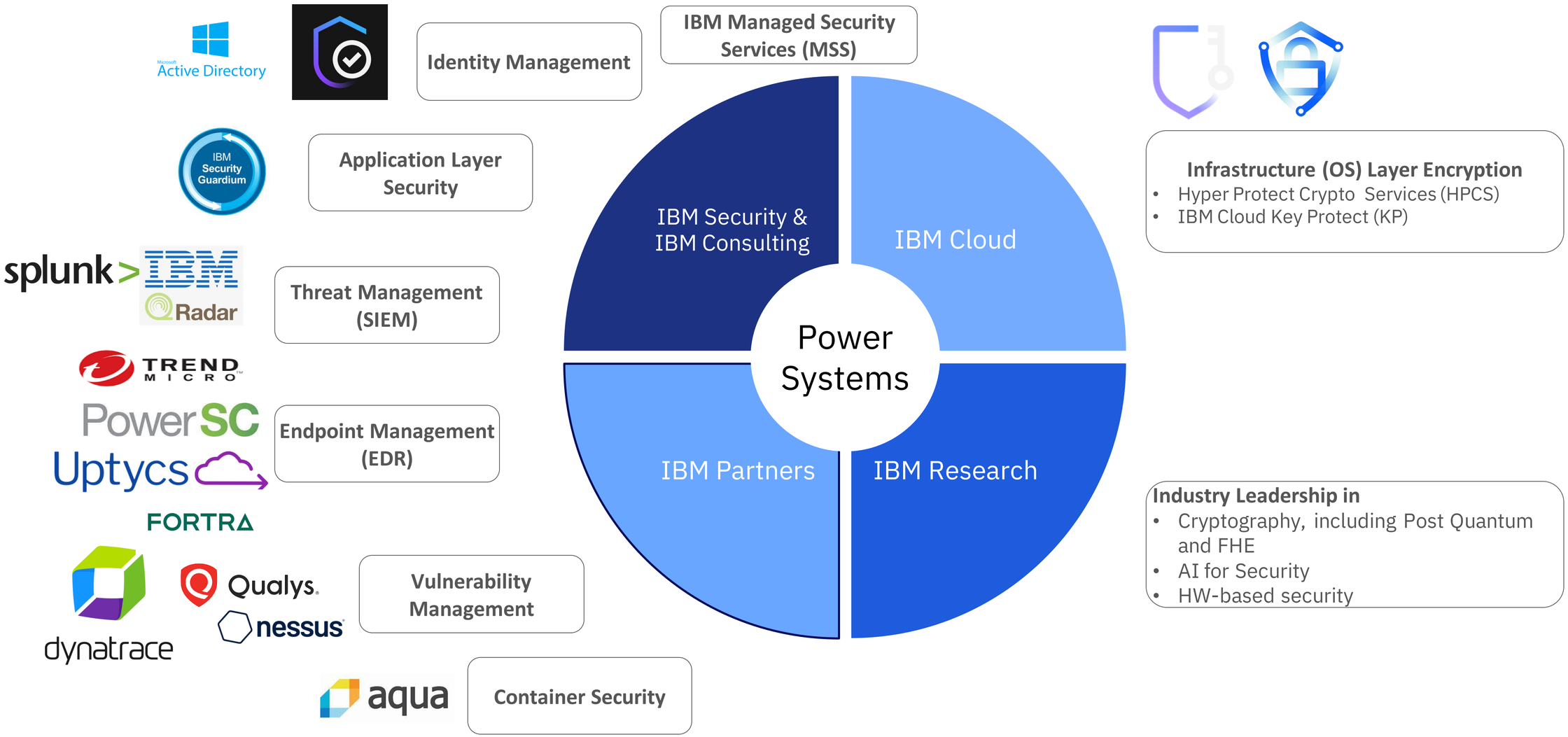
applied to IBM Power deployments

Consider the IBM SAP security framework…

The 13 layers of SAP security is a stratified approach that decompose security aspects in different layers, following a top-down approach that moves from Regulatory and Compliance to the most technical aspects of security hardening for SAP ensuring full coverage of our client's needs

Compliance	1. Governance & Regulatory	Risk Assessment and Quantification
	2. Access Management	Cybersecurity Assessments
	3. Data Privacy	SAP Application Layer **Data Privacy / Protection Discovery**
	4. Continuous Control Monitoring	Security **monitoring automation**
Technical Security	5. Authentication	Infrastructure and SAP **continuous authentication and MFA**
	6. Secure Source Code / DevSecOps	Infrastructure and SAP **DevSecOps**
	7. Secure Configuration / Baseline	Security hardening and **health checks**
	8. SAP HANA Security	Application endpoint security, SAP **security controls**
	9. Data Protection / Encryption	End-to-End Data Privacy, Encryption & Key Management
	10. Interface Security	Network and Interface Security
	11. Vulnerability &Threat Management	Infrastructure and SAP **Threat and Vulnerability Management**
	12. SAP Cloud / SAP BTP	
	13. Infrastructure Security	On Prem, IaaS Cloud, RISE with **SAP infrastructure deployment options**

… and Leverage the IBM Power & Partner Security Ecosystem for SAP



NIST Power Security Framework Mapping: Power + Partners

Identify

IAM & PAM
- Discover Risk Users & Apps, SOD Violations, etc. IBM Security Verify
- Discover Privileged users and accounts
- PowerSC MFA PowerSC

Data & Crypto
- Unstructured and Structured data discovery & classification.
- Key discovery and agility
- IBM Security Guardium IBM Security Guardium

Supply Chain Risk Management
- IBM systems O-TTPS Certification

Protect

IAM & PAM (Verify)
- PowerSC MFA PowerSC

Crypto, Data & Privacy
- AIX LV Encryption and Linux LUKS Encryption with Hyperprotect Crypto Services for AIX and Linux
- PQC algorithm acceleration
- IBM Crypto Express Card (4769)
- IBM Security Guardium IBM Security Guardium

Threat Management
- IBM Power FLTR IBM Power Fix Level Recomendation Tool
- IBM Systems PSIRT
- Automated patching: OS, PowerSC

Protective Technology
- Power FW Security and Trusted boot
- Power10 BMC secure boot
- Power10 Transparent Memory Encryption
- Power10 Return Oriented Programming protection

Container Infrastructure
- Partnership w. Aqua – secure the build and infrastructure Aqua Security and IBM Power

Detect

Anomalies and Events
- PowerSC EDR for Linux & AIX
- Uptycs XDR for IBM Power

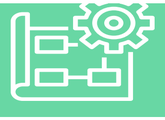
Security Continuous Monitoring
- IBM Qradar – privileged user monitoring, network anomaly detection IBM QRadar
- IBM Security Guardium

Continuous Compliance
- PowerSC Compliance Monitoring – PowerSC

Detection Processes

Network
- IBM QRadar
- 3rd party anomaly detection tools: e.g. IBM Cloud CIS - Cloud Internet Services (CloudFlare).

Container Infrastructure
- Partnership w. Aqua - ”drift detection”



Respond

Response Planning
- PowerSC EDR PowerSC
- Uptycs XDR IBM Power XDR with Uptycs

Communications

Analysis
- PowerSC EDR for LinuxPowerSC

Mitigation

Improvements

Recover

Recovery Planning
- Safeguarded copies for IBM i
- Safeguarded Copy

Security for SAP on Power: (On-prem) Reference Architecture

Identity and Access Management

Identity and Access Management (IAM)

Privileged User Management (PAM)

- *IBM Security Verify*
- *Microsoft Active Directory*

IBM Security Verify Privilege

Threat Detection and Response

Vulnerability Management: Scanning & Patching

Threat Management (SIEM)

- *Qualys (XForce RED VMS)*
- *Tenable Nessus*

- *IBM Security Qradar*
- *Splunk SIEM*

Endpoint Security

End-Point Detection and Response & Anti-Malware

Configuration Management

- *PowerSC EDR*
- *Uptycs (future?)*
- *Trend Micro (?)*

- *Tenable Nessus*
- *SLES hardening rules,*
- *CIS Benchmarks, OpenSCAP*

Data Protection

OS-Layer Logical Volume Encryption

Application Layer Encryption and Firewall

Linux LUKS, AIX LVE w. HPCS, KP, PKS (see details)

IBM Security Guardium - details

Evolved from IBM SAP RISE offering security architecture

Follows SAP (Cloud)Security Framework Guidelines

Why does Power platform provide the best security for running SAP?
Zero Trust Use Cases with Power10

Protect the Hybrid Cloud

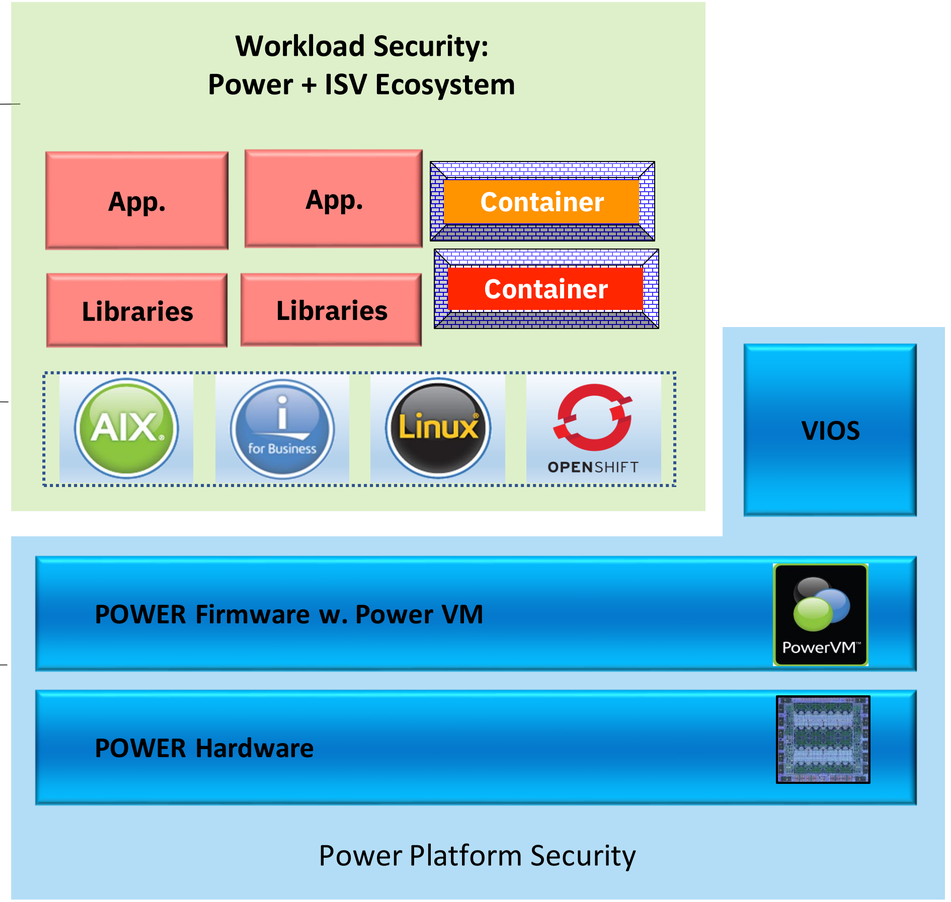
- End-to-End data encryption w. Bring/Keep Your Own Key (BYOK)
- Container Security* (DevSecOps): Secure the build, infrastructure and workloads at runtime

Preserve Data & Workload Privacy

- Cryptographic algorithm acceleration
- Support for PQC and FHE crypto algorithms

Reduce the Risk of Ransomware

- Platform Integrity
  - Power10 enhanced CPU FSP/BMC isolation
  - Main memory encryption
  - Performance-enhanced side-channel avoidance
  - Power10 Return Oriented Programming (ROP) protection
- Security Management for VM Workloads (PowerSC*)
  - Endpoint Detection & Response (EDR)
  - Continuous Multi-Factor Authentication



*Partnerships

Power vs x86 Security Differentiation Examples

Processor

- Built-in side channel avoidance
- Compared to patches that impact performance
- Encryption acceleration makes it possible to turn encryption always on by default

Firmware

- Industry leading security for service processors (BMC/FSP)
- Service processor vulnerabilities enable attacker to bypass host security protections

Lower Vulnerabilities

- Orders of magnitude lower vulnerabilities (CVEs) for firmware, OS components
- Results in less patching, reboots, critical workload interruptions

Why does Power platform provide the best security for running SAP?
Power10 Performance Enhanced Side-channel Avoidance

Competition provides patches: “band-aids” eating away performance

Retbleed slugs VM performance by up to 70 percent in kernel 5.19

Intel CPUs Suffer Performance Hit From New Spectre-v2 Mitigations

By Zhiye Liu published March 11, 2022

Guess who's back?

Intel Hardware Level Speculative Execution To Blame For Kernel Bug – KPTI Workaround Introduces Performance Hits Up To 23% On Average

2763

INFRASTRUCTURE SECURITY

Solution to hardware flaw in Intel CPUs may cause large performance hit

HOWARD SOLOMON AUGUST 10, 2023

A hardware flaw in Intel Core and Xeon CPUs lets attackers steal data from other users on the same system, including on servers that use Intel’s SGX memory protections, according to a Google researcher.

According to SC Magazine, Daniel Moghimi told the Black Hat 2023 security conference this week that the vulnerability, dubbed “Downfall”, endangers data running on virtual machines or in containers in shared environments, such as in most cloud-computing deployments, as well as on personal computers with multiple users. The flaw is also known as CVE-2022-40982.

Intel is releasing a microcode update that blocks transient results of the exploit Moghimi created. However, the information site says, according to Intel some workloads may experience up to a 50 per cent performance hit.

Power10 Processor provides built-in protection from entire classes of side-channel attacks at no performance penalty

- Power10 micro-architecture protects from several classes of speculative execution side channel attacks - always ON

Enhancing security by separating CPU and Service Processor Trust Domains

Importance of Service Processor Security

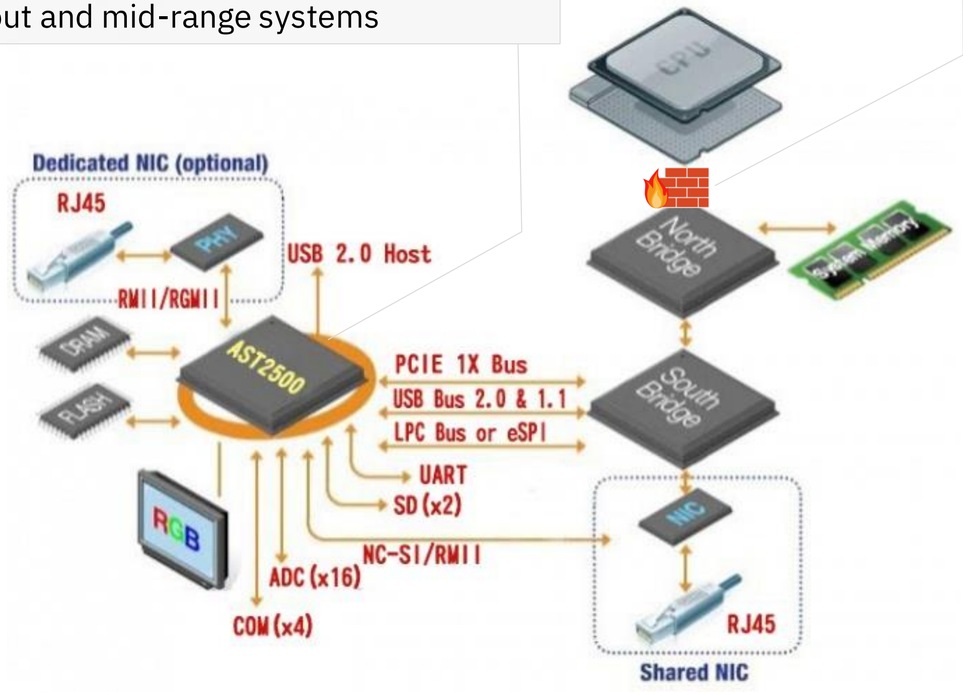
Embedded processor circuitry for increased isolation of CPU from service processors

Limits access of BMC/FSP to only necessary resources

Further reduces threat vector even if BMC/FSP is compromised

Additional Power10 features to strengthen integrity of BMC complex

BMC/OpenBMC secure boot for scale-out and mid-range systems



Simplified diagram of connectivity between the service processor and CPU (from ASPEED)

Power Platform has Orders of Magnitude Lower Vulnerabilities

Helps alleviate concerns about keeping up with patches

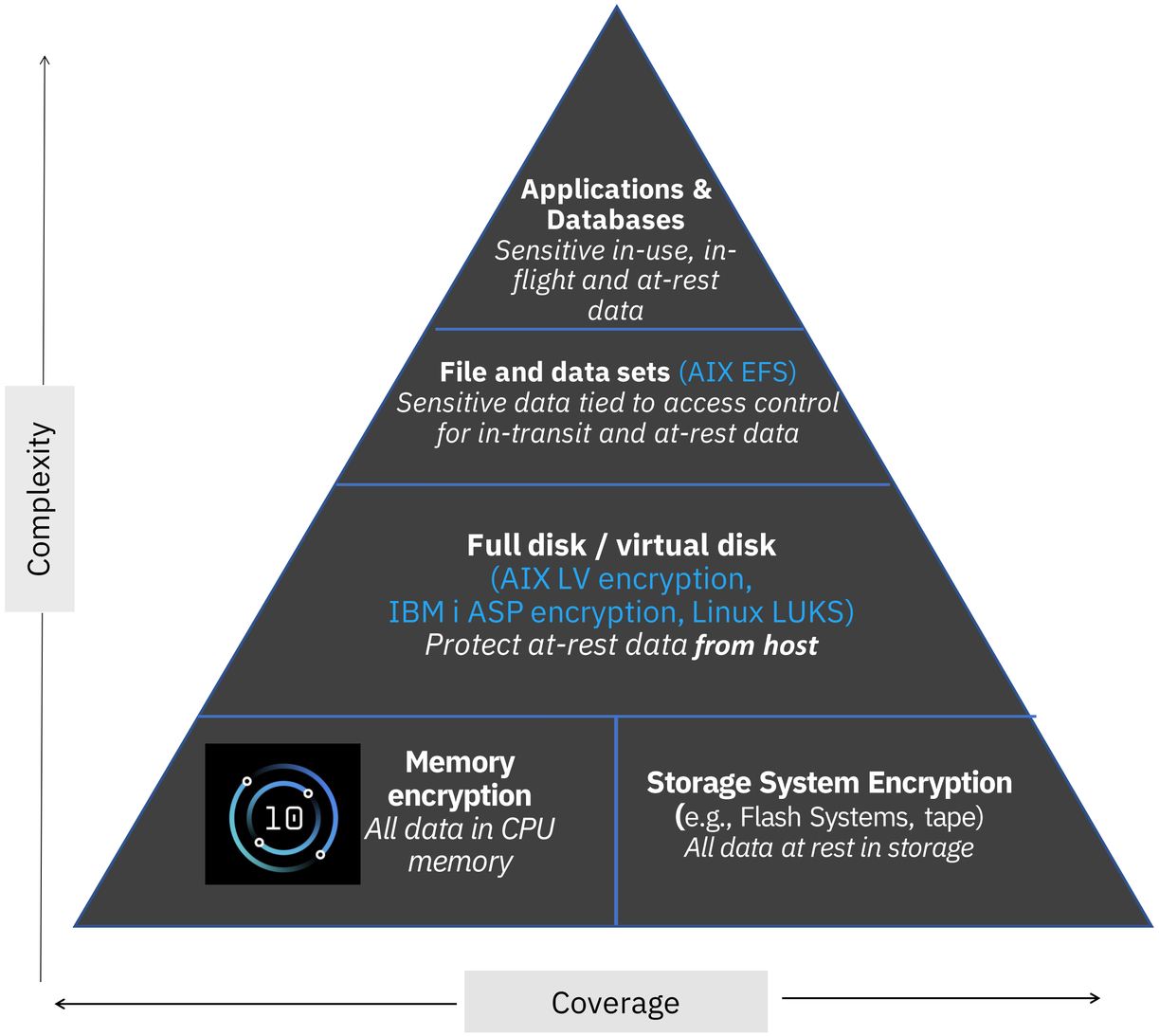
	IBM PowerVM	VMWare ESX	Microsoft Hyper-V	“KVM”[1]
Virtualization Technology CVEs	12	448	184	206

	IBM AIX	IBM i	“Windows”	“Linux”
Operating Systems CVEs	404	47 (+ OS/400): 13	11213	7158

Notes

- CVE: Common Vulnerability Exposure
- CVE counts as of 2023-10-11
- The number of CVEs is an indication of stronger security but should not be used as direct metric of resiliency against cyber attacks
- [1]Includes CVEs referring to KVM across all Linux distributions and all hardware platforms (x86, Z, Power). The number of CVE applicable to a Linux virtualization platform is likely higher than just those for KVM.

Why does Power platform provide the best security for running SAP?
Protect Data: End to end security with full stack encryption, in transit, at rest, in memory



Transparent memory encryption with:

- No additional management setup
- No performance impact

Blazing fast hardware-accelerated encryption compared to Power9

- 4X crypto engines in every core
- 2.5X faster AES crypto performance per core*
- Encrypted Live Partition Mobility (LPM)

Stay ahead of current and future threats with support for:

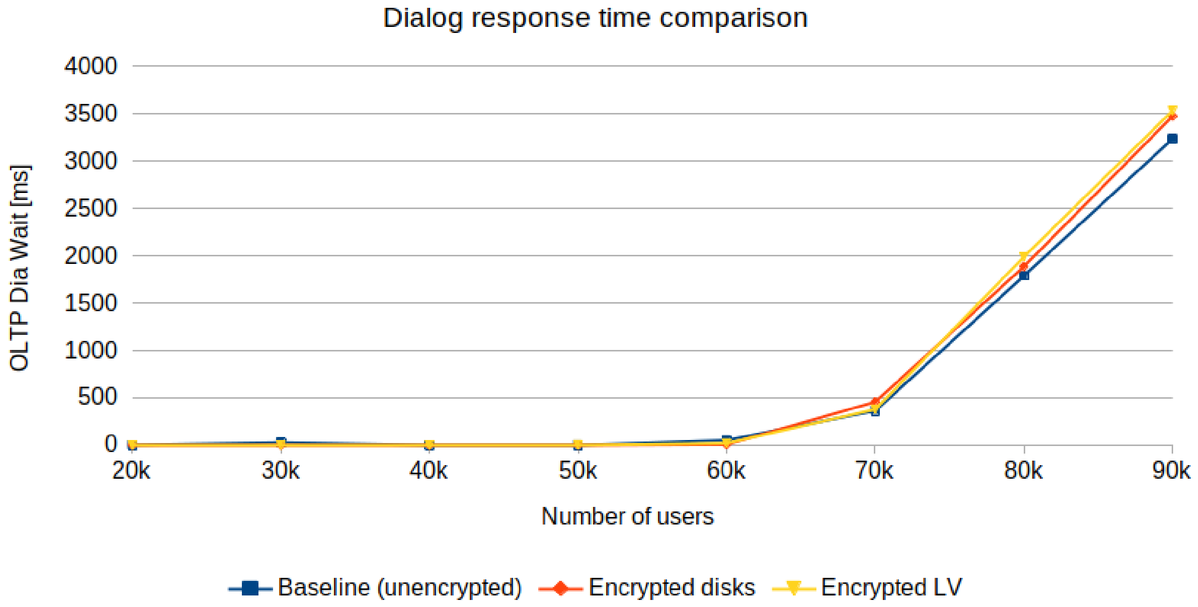
- Quantum-safe cryptography
- Fully homomorphic encryption
- Support for next generation Crypto Express Card

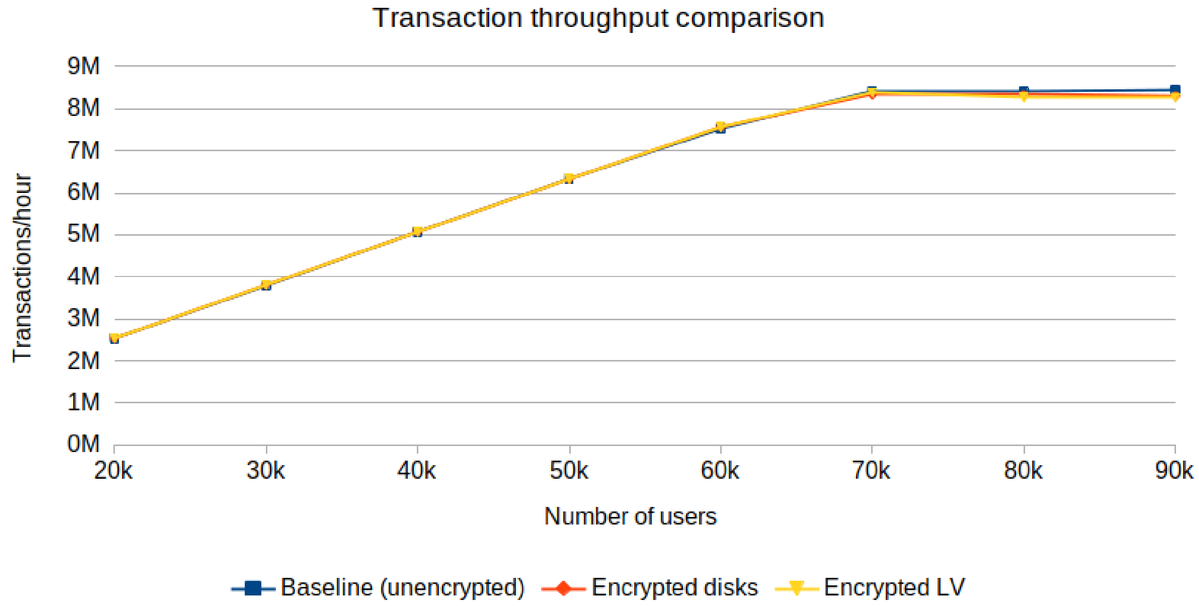
**AES-256 in both GCM and XTS modes runs about 2.5 times faster per core than comparable Power9 systems according to preliminary measurements obtained on RHEL Linux 8.4 and the OpenSSL1.1.1g library*

Power10 Cryptography Algorithm Acceleration – SAP Workload Example

Power10 Processor provides 4x AES and SHA2 encryption engines compared to P9

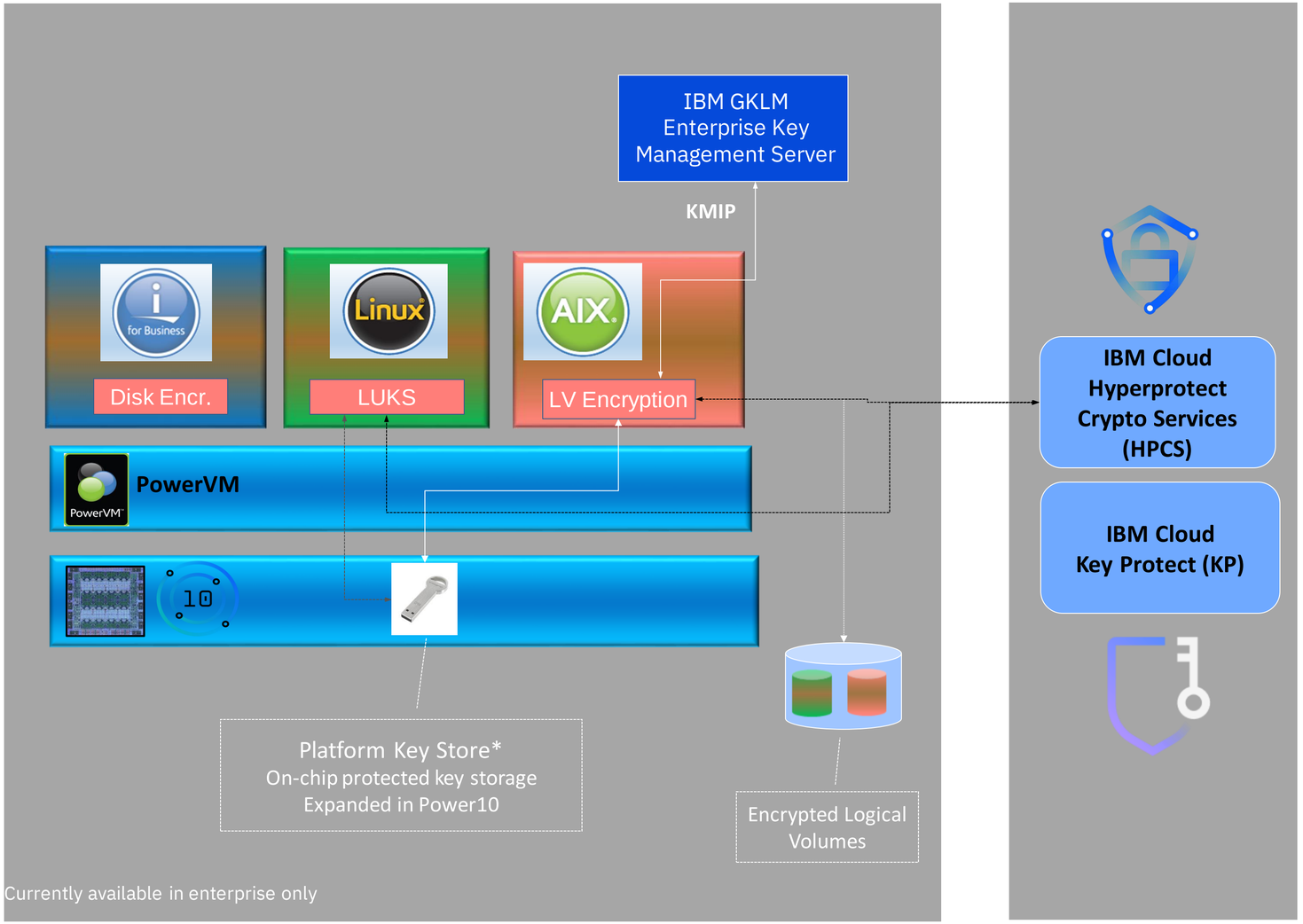
- Directly improves performance of crypto libraries used by various server applications (e.g. TLS, IPsec)
- Improved encryption performance allows for full disk encryption solutions at a negligible performance overhead (protect data at rest)
  - Linux LUKS – see SAP blog AIX LV encryption, IBM i ASP encryption





Multiple Key Management Options to Protect Hybrid Cloud Deployments
Integration with IBM Cloud Key Protect Service & HyperProtect Key Service for BYOK/KYOK Support

- **OS-level data encryption with customer-controlled keys**
- **Support Bring Your Own Key (BYOK) and Keep Your Own Key (KYOK)**
  - Integration w. IBM Cloud Hyper-Protect Crypto Services (HPCS) - KYOK
    - Based on IBM Z and Crypto Express Card, FIPS 140-2 Level 4 certified – *only such Cloud service*
    - Support in AIX and Linux on POWER
  - **New**: integration with IBM Cloud Key Protect service – BYOK
    - Based on 3rd party HSM offering
    - Support for AIX and Linux on Power
- **Zero Trust model w.r.t. to Cloud storage administrators**



Simplify and improve security and compliance with IBM PowerSC

Compliance automation

Prebuilt profiles support industry standards such as the Payment Card Industry Data Security Standard (PCI), HIPAA, GDPR, DoD, NERC and many other industries.

Real-time security

Monitor and gain automatic and immediate visibility to a summary of statuses from security event sources and and includes FIM, EDR, Allow Listing, Block Listing, and Anti-Virus capabilities.

21

Patch Management

Monitor and manage the status of security patches. Updates can be triggered directly from the PowerSC GUI for AIX and Linux on Power logical partitions (LPARs).

Multifactor Authentication

Increase the assurance level of Power servers with multiple authentication factors. Authentication factors can be added as they become available.

Automate

Reduce administrative cost and increase efficiencies with Security and Compliance automation.

Monitor

Detect security exposures in virtualized environments with real-time compliance monitoring.

Report

Reduce time and skills required for preparation of security audits with compliance reports.

Profile

Deploy industry standard security with preconfigured security profiles.

Data Sheet

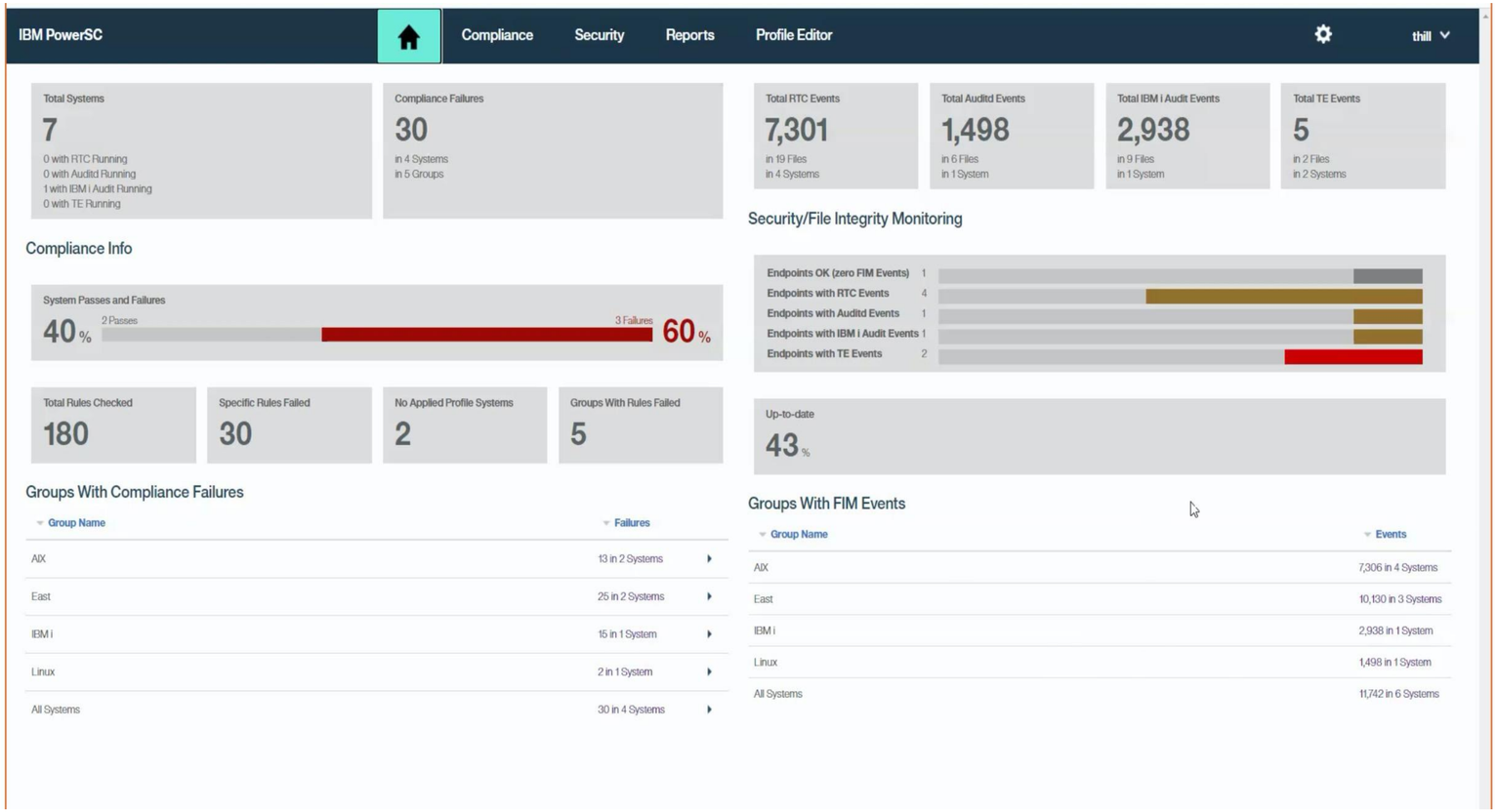
Unified Platform Security Management with IBM Power**SC**
User-friendly, web-based UI to manage Security & Compliance

Compliance and Drift Analysis
- HIPAA, PCI, CIS, and more

Security
- File Integrity Monitoring (FIM)
- Allow/Block listing
- Endpoint Detection & Response

Patch Management
- Trusted Network Connect (TNC)
- Detect & alert policy issues
- Policy enforcement

Multifactor Authentication
- Policy-based and Centrally administered
- Simplified logins (Tokens and SSO)



Power**SC** Compliance Profiles

AIX Profiles

GDPR

PCI

CIS

HIPAA

NERC

DoD STIG

SAP Hardening

Oracle Systems Hardening

Compliance

Linux Profiles

GDPR

PCI

SAP Hardening

CIS

HMC Hardening (2022)

IBM i Profiles

IBM i hardening

Compliance profiles can be customized

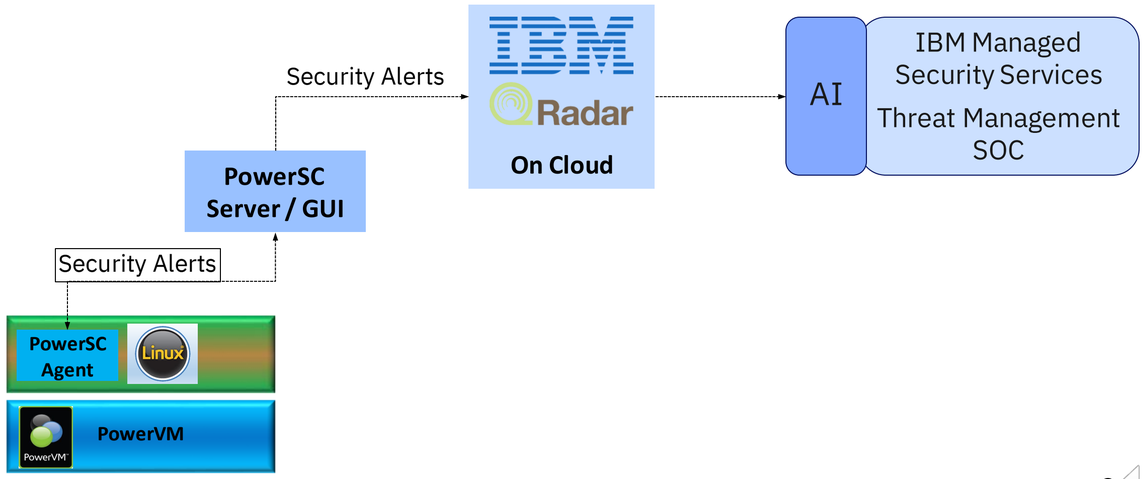
Reduce Security Operations Complexity with Power**SC** Endpoint Security
Endpoint Security Tailored for Power Endpoints

New in PowerSC 2.0

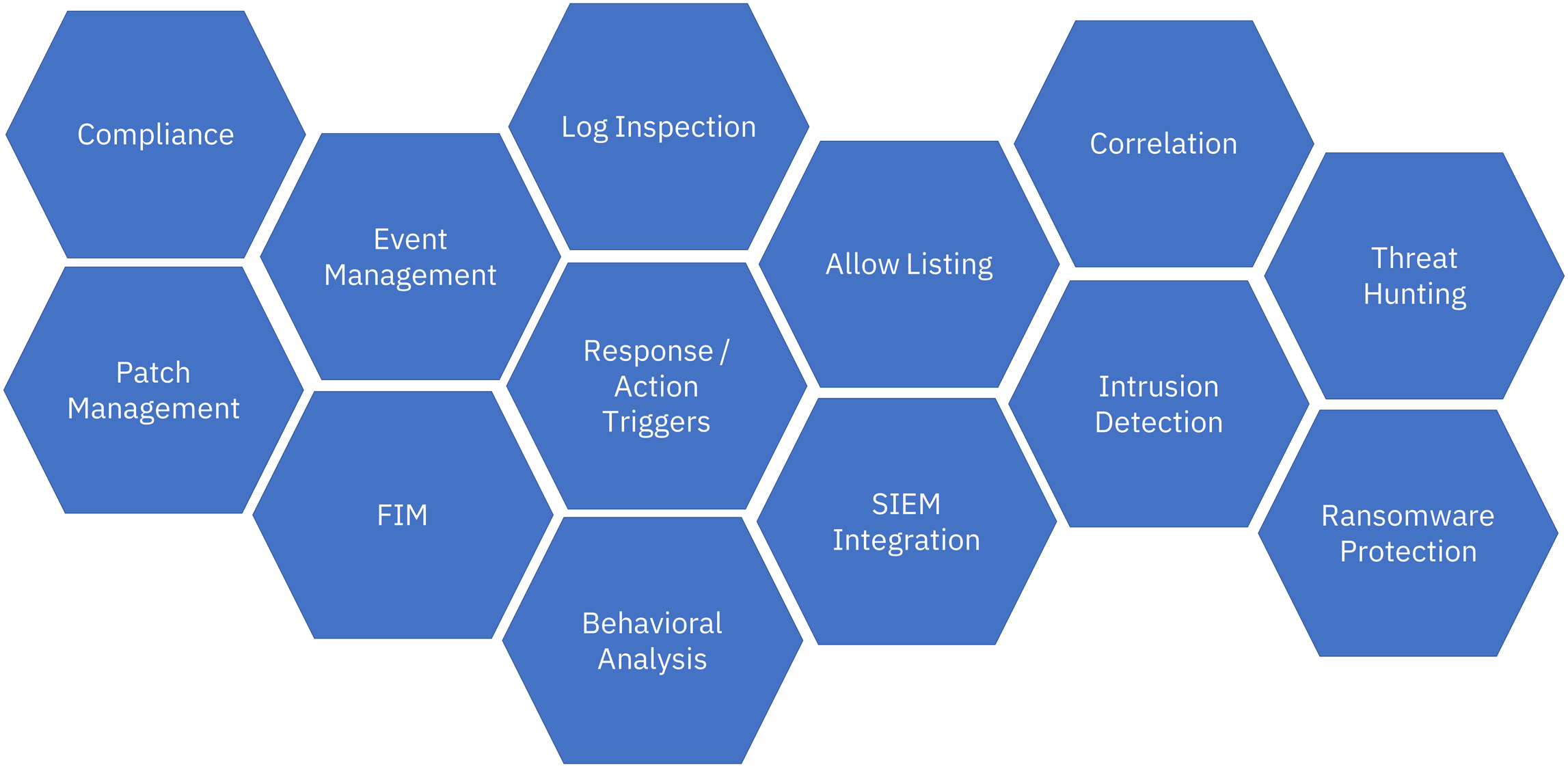
- Endpoint Detection and Response (EDR)
  - Intrusion Detection and Prevention (IDP)
  - Anomaly detection, correlation, & incident response
- MFA addition – included in PowerSC 2.0
  - Single product instead of separate offerings
- Hybrid cloud support – ability to manage systems both on prem and on Cloud

Updates in PowerSC 2.1

- "Blocklisting" (anti-malware)
- Anti-malware – anti-virus
  - Integration with ClamAV open-source project (backed by Cisco)
- Integration w. IBM QRadar on Cloud (QRoC)
  - Facilitates "single pane of glass" for security
  - Benefits from QRoC AI processing of alerts
- Deployment on IBM Power VS for SAP RISE



PowerSC Endpoint Protection – Techniques Used



Power Systems: The Strongest Defense against Ransomware Attacks

1. Prevention is the best defense

Power10 Systems provide industry-leading isolation and integrity, following the principles of Zero Trust, that help prevent ransomware

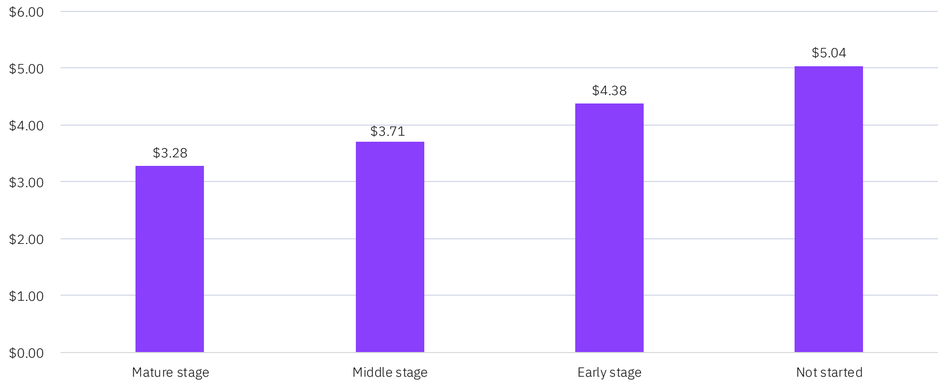
- Host/firmware isolation and integrity
- Guest OS secure boot
- Built-in OS runtime integrity
- Most secure multi-tenant environment with orders of magnitude lower CVEs vs. x86 stack
- End to end data encryption & key mgmt
- Simplified security management: PowerSC, Aqua
- Multi-Factor Authentication with PowerSC MFA

2. Early Detection is Critical

- Integrated security and compliance management for VMs and Containers makes it harder to misconfigure and easier to detect anomalies
- Advanced analytics for early indication of compromise with IBM Security QRadar

3. Fast and Efficient Recovery

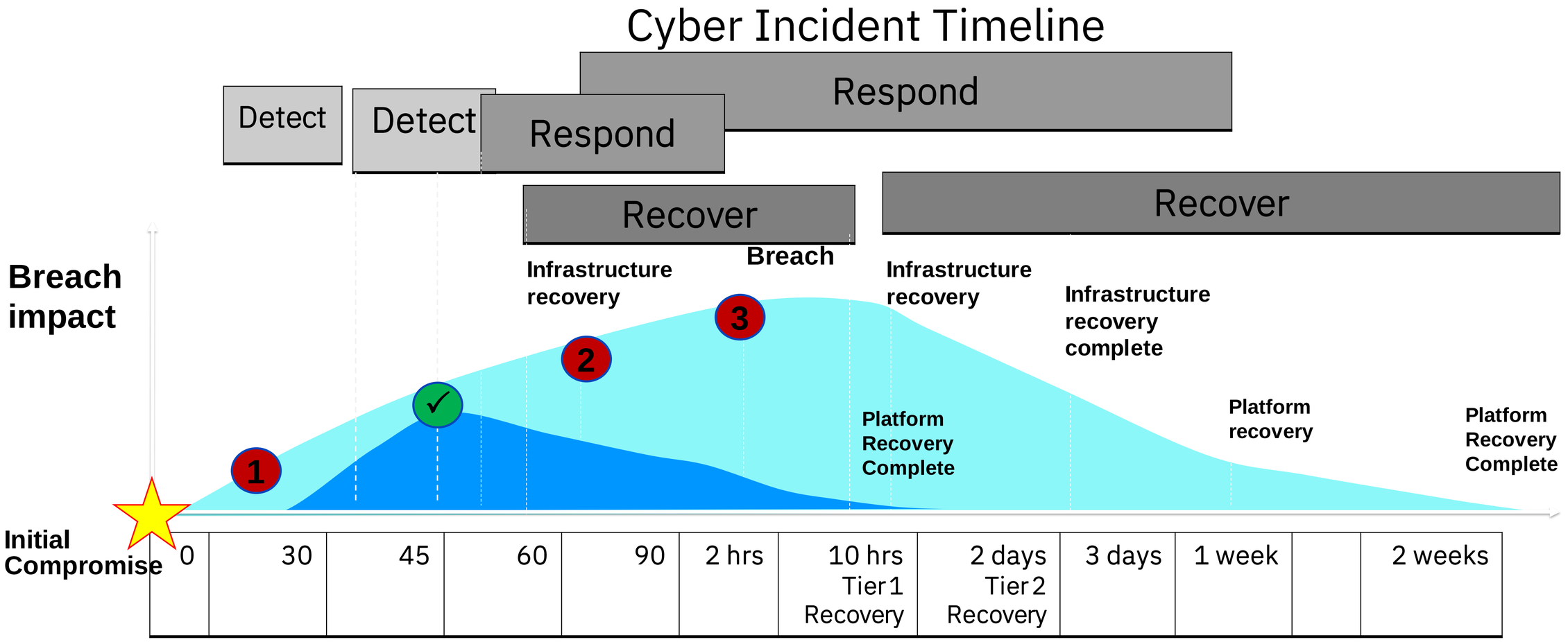
- Easy to deploy resiliency strategies with PowerHA, IBM Storage Cyber Vault, safeguarded copies and IBM Security Services



The average cost of a breach through Zero Trust maturity*
Measured in US$ millions

Source: “Cost of a Data Breach Report 2021”, IBM & Ponemon Institute

IBM Cyber Resilience w. IBM Storage Cyber Vault

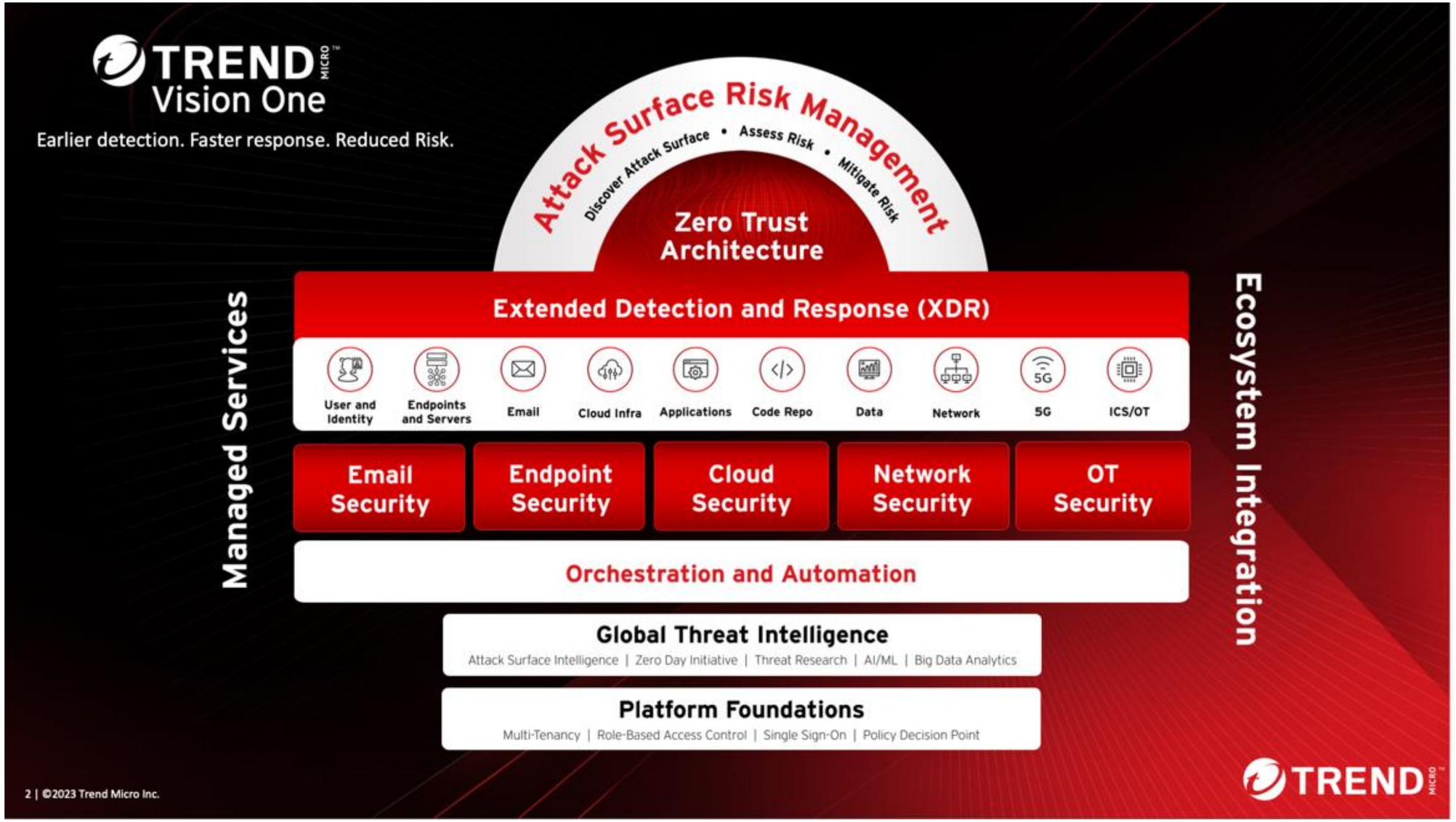


1. Corruption of data occurs - but not yet detected
2. Without the IBM Cyber Vault environment corruption is detected much later and has a greater chance to spread
3. It takes even longer to identify all impacted data once the corruption has spread within the enterprise

IBM Cyber Vault Value

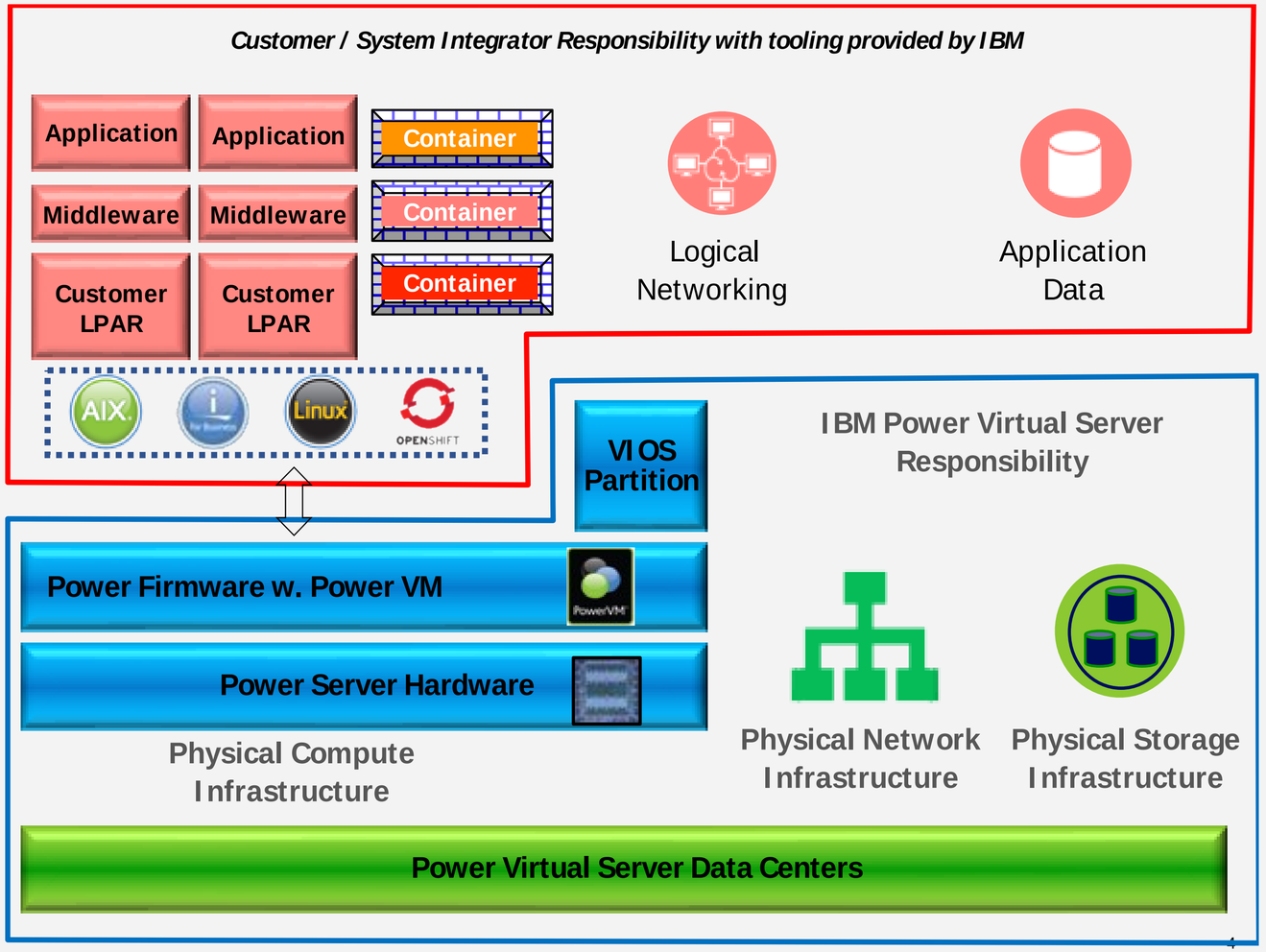
Due to the Cyber Vault environment and the use of Safeguarded Copy technology, data is continuously checked and corruption is found and corrected EARLIER and FASTER

Endpoint Protection w. Trend Micro on IBM Power (*Work in Progress*)



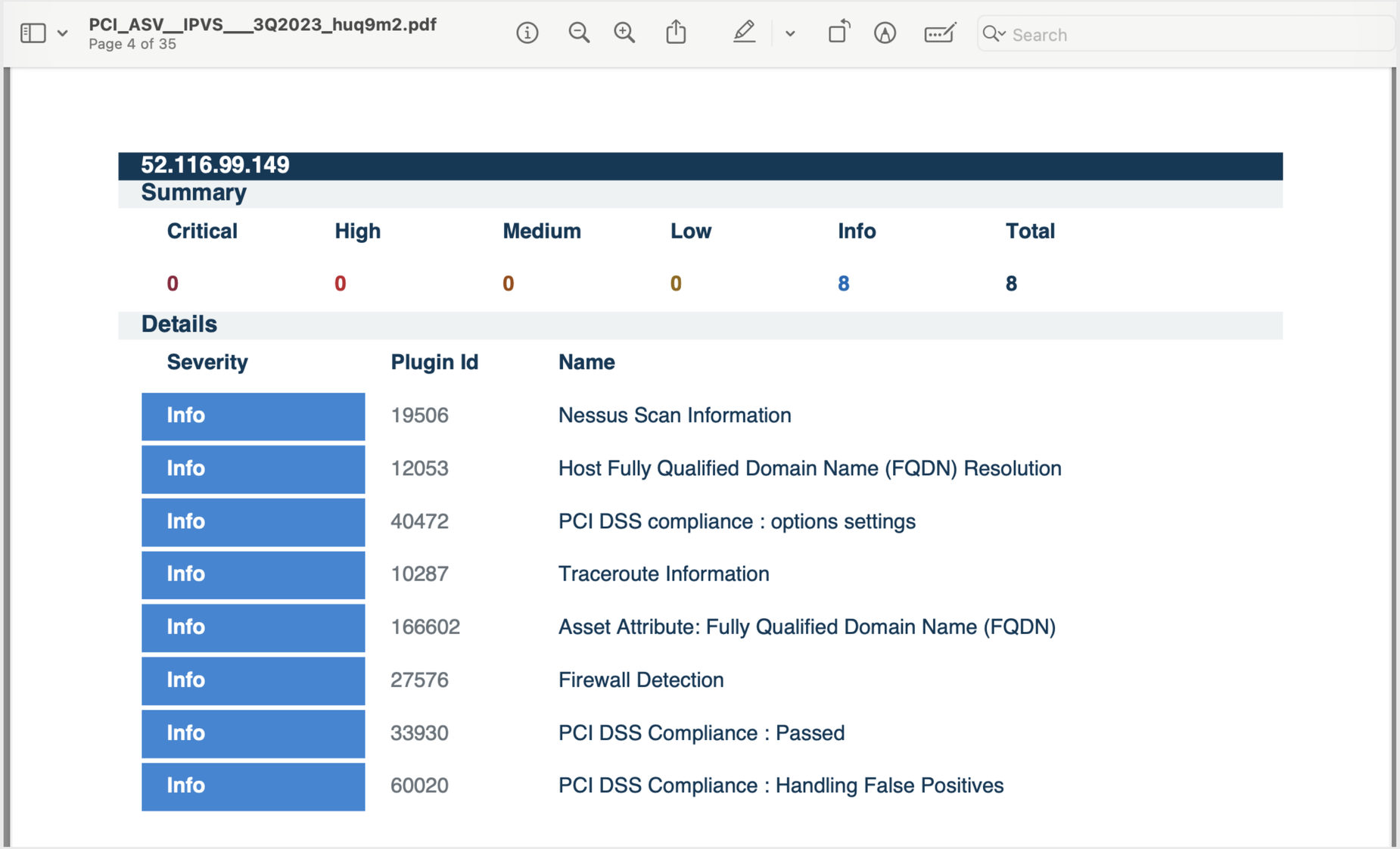
Power VS Infrastructure Security and Controls: Joint Responsibility

- IBM Cloud offering with IBM Cloud and inherent Power security capabilities – follows typical Power enterprise deployment models
- IBM manages **infrastructure security** (“hypervisor and below”), including all control plane components used to operate the IaaS layer (servers, VIOS, PowerVM, HMC, PowerVC, physical networks and SAN storage)
- IBM provides tooling and best practices for customers and system integrators to manage LPAR/workload security (AIX, IBM i, Linux, OpenShift)
- **Infrastructure security integrated with common IBM Cloud components and micro-services for security**
  - Inventory Management
  - Identity and Access Management (IBM Cloud IAM)
  - MFA: IBM Security Verify
  - Health Checking (Based on Tenable Nessus)
  - Patching / Vulnerability Management
  - Vulnerability Scanning (Tenable Nessus)
  - Auditing / SIEM (Based on IBM Security QRadar)
  - IBM Cloud SOC
  - IBM Cloud IKS Security Tooling (Kubernetes assets)
  - IBM PSIRT processes for tracking vulnerabilities
- **Applies security best practices from IBM Cloud, IBM Corporate and IBM Power**



Joint Responsibility Model for Security

Example: Vulnerability Scanning via Tenable Nessus



52.116.99.149

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	8	8

Details

Severity	Plugin Id	Name
Info	19506	Nessus Scan Information
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	40472	PCI DSS compliance : options settings
Info	10287	Traceroute Information
Info	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
Info	27576	Firewall Detection
Info	33930	PCI DSS Compliance : Passed
Info	60020	PCI DSS Compliance : Handling False Positives

Nessus Custom Plug-ins developed

- IBM Storage FlashSystem Health Checks
- Power HMC Health Checks

Security Services available for Customer Workloads

Feature	Applicable Offering (Dedicated or Shared)
Firewall	IBM Cloud Juniper vSRX or Vyatta
Health Checking, Compliance Checking	• IBM PowerSC available on Power VS • Tennable Nessus (AIX, Linux), Qualys (Linux on Power) • Fortra (formerly HelpSystems)
EDR (Endpoint Detection & Response)	• PowerSC 2.0 EDR capability for Linux on Power and AIX
Antivirus	Typically not deployed on Power but potential add-on from 3rd party – Fortra (formerly HelpSystems)
Anti-malware	New since PowerSC 2.1.0.1: • “Blocklisting” and anti-malware (integration w. ClamAV open-source project) • Integration with IBM QRadar on Cloud (QRoC) for security alerts
Load Balancer	IBM Cloud Load Balancer
Key Protect/Key Vault	• IBM Cloud Hyper Protect Crypto Services – Integration w. AIX LV Encryption and Linux LUKS • IBM Cloud Key Protect (KP) Service - Integration w. AIX LV Encryption and Linux LUKS
Certificate Manager/PKI	IBM Cloud Secrets Manager
Web Application Firewall	IBM Cloud Internet Services (CIS) w. CloudFlare
DDOS	IBM Cloud Internet Services (CIS) w. CloudFlare

AI for Security on Power: Domains of Applicability and Pain Points

“AI for Security”

- Exponential increase in volume of security events and alerts – trillions of log events to analyze and correlate
  - Humans unable to cope with volume
- Response to and remediation of security breaches takes too long
- Skills gap amplifies above pain points
- Example application domain: threat management

Power participates in AI for Security ecosystem

“Security for AI”

- Protect confidentiality and integrity of data used in AI (model, inferencing) and resulting models
  - Loss of data privacy has regulatory and reputation impact
  - Tampering of data would lead to wrong models and AI decisions
- Support new models with collaborative learning – contribute and combine data with 3rd parties with appropriate security guarantees
- Security mechanisms increase overhead and configuration complexity

Power becomes the most trusted platform to run AI workloads