# One Click – Security and Compliance Done?

David Spurway
IBM Power AI and Sustainability
Principal, EMEA, IBM Technology
Email: david.spurway@uk.ibm.com
LinkedIn: @David Spurway

# Agenda

- IBM Power delivers reliable performance and lowers risk
- With built in security features and orders of magnitude fewer vulnerabilities, IBM Power is reliable platform
- Apply security standards quickly and easily, and get real time alerts if compliance is broken
- Surround resilient applications with trusted and secure containers to modernise
- A secure infrastructure is part of the framework for trusted AI

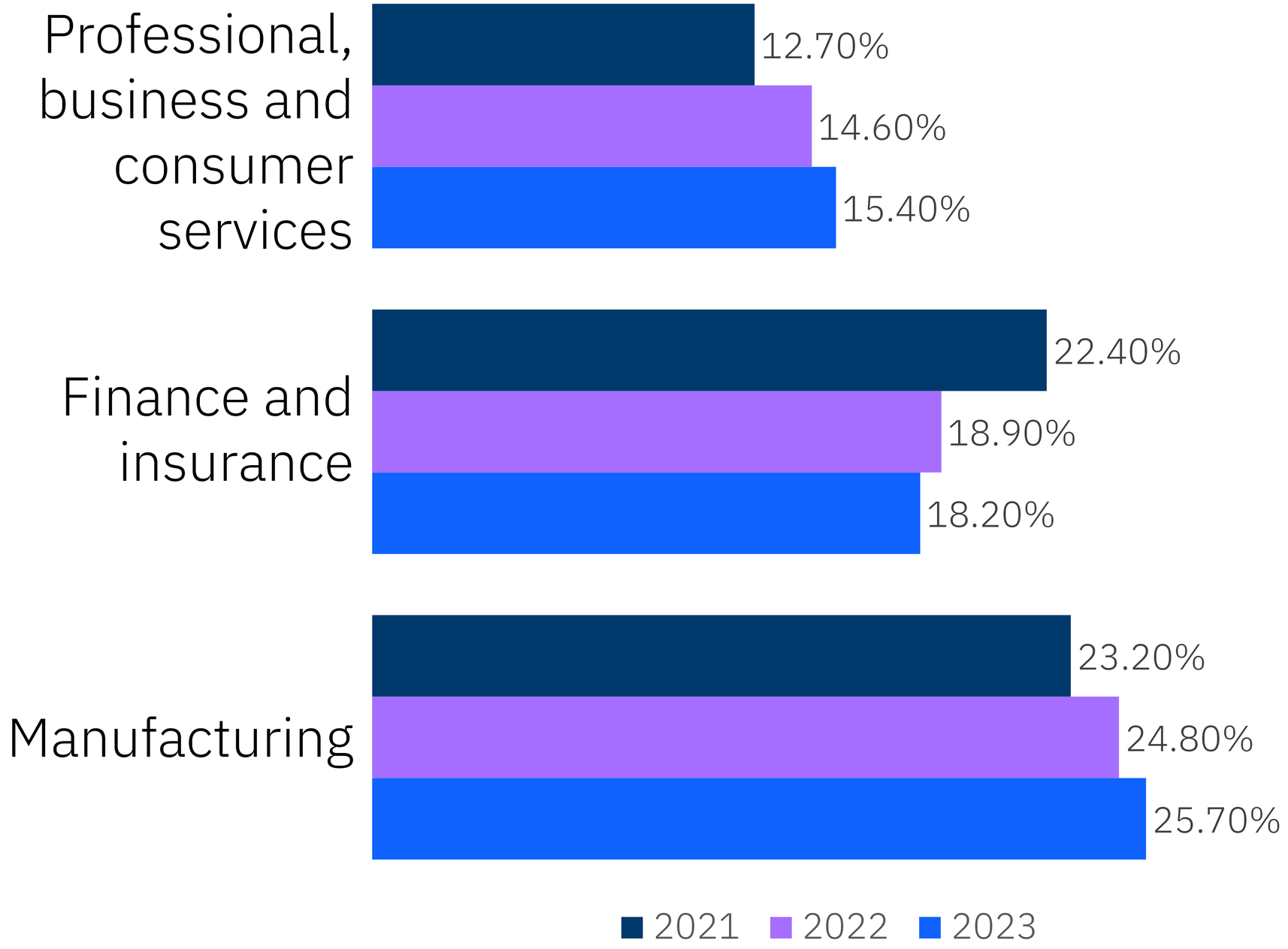
260,473

# 32%

84,245 vulnerabilities with weaponized exploits

82%

# All industries are targets



# Virtualization in IBM Power is even more secure

Virtualisation is built into IBM Power, rather than installed later. This drastically reduces the “surface area” that can be attacked.

My daughter was born in 2004, when VIO was released.

She is 19 now.

During that whole time, **only 4 vulnerabilities** have been published for VIO.

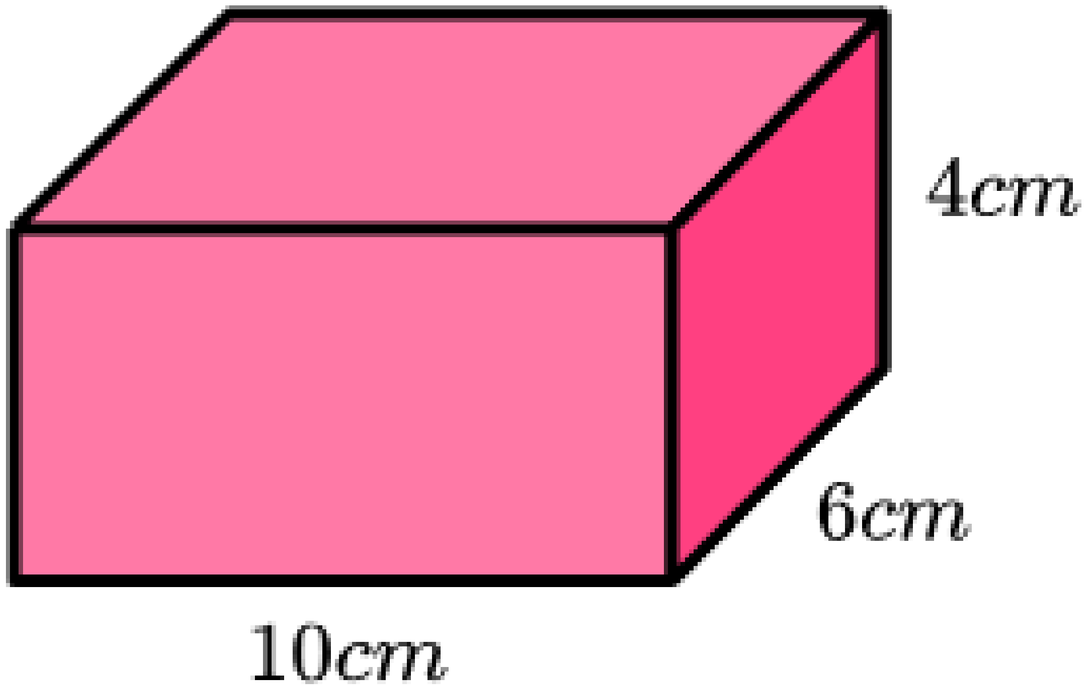
Details from CVEdetails.com

VMware has 871 since 1999, with **65 published in last 12 months** alone.

Details from CVEdetails.com

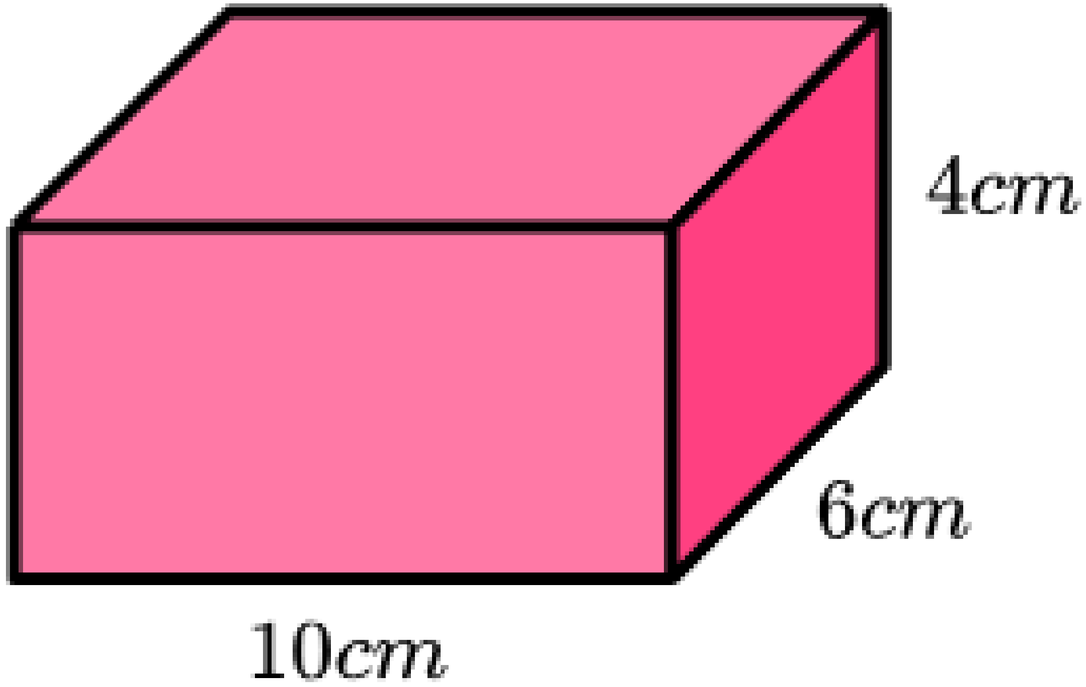
Virtualization Technology CVEs

| IBM PowerVM | VMWare ESX | Microsoft Hyper-V | “KVM”[1] |
|---|---|---|---|
| 15 | 448 | 211 | 314 |

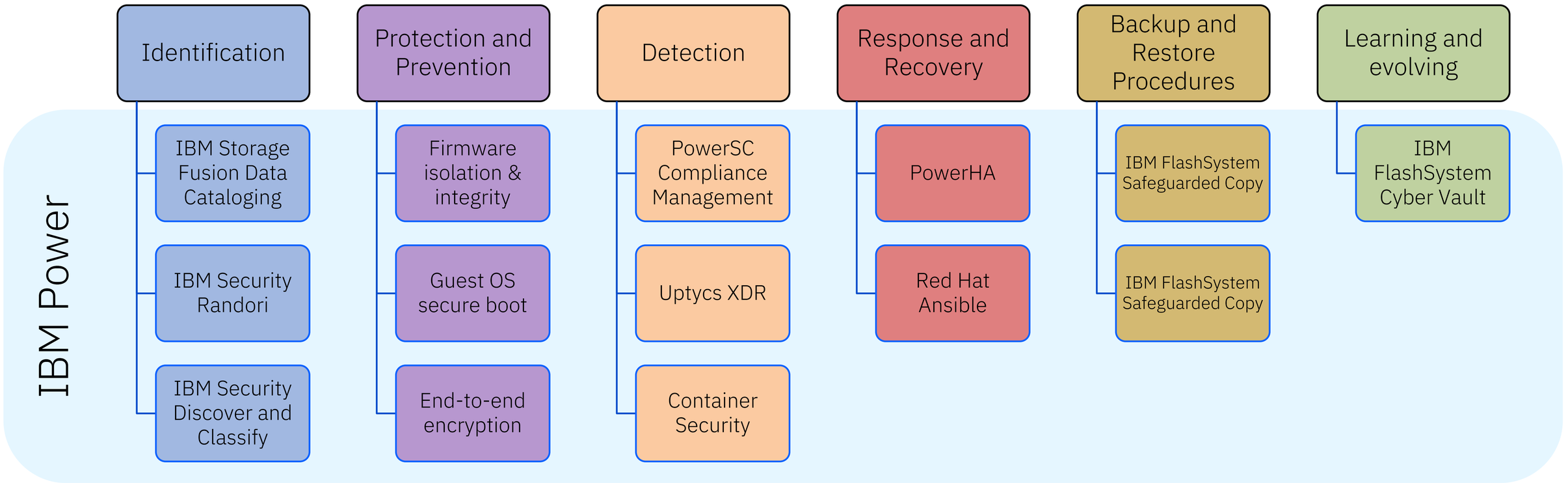


Operating Systems CVEs

| IBM AIX | IBM i | “Windows” | “Linux” |
|---|---|---|---|
| 418 | 35 + 13 = 48 | 12326 | 11447 |



# IBM Power value vs. DORA requirements



# Cybersecurity measures and reporting obligations
# Network and Information Systema Directive (NIS2)

## MEASURES

- risk analysis and information system security policies;
- **incident handling (prevention, detection, and response to incidents);**
- business continuity and crisis management;
- supply chain security;
- security in network and information systems acquisition, development and maintenance, including **vulnerability handling** and disclosure;
- policies and procedures (**testing and auditing**) to assess the effectiveness of cybersecurity risk management measures;
- the use of **cryptography and encryption**.

## REPORTING

- Initial notification within 24 hours after having become aware of the incident
- A final report in one month including at least the following:
  - a detailed description of the incident, its severity and impact;
  - the type of threat or root cause that likely triggered the incident;
  - applied and ongoing mitigation measures.

# IBM Power value vs. DORA requirements

IBM Power

- Protection and Prevention
  - Firmware isolation & integrity
  - Guest OS secure boot
  - End-to-end encryption

## Protect the Hybrid Cloud

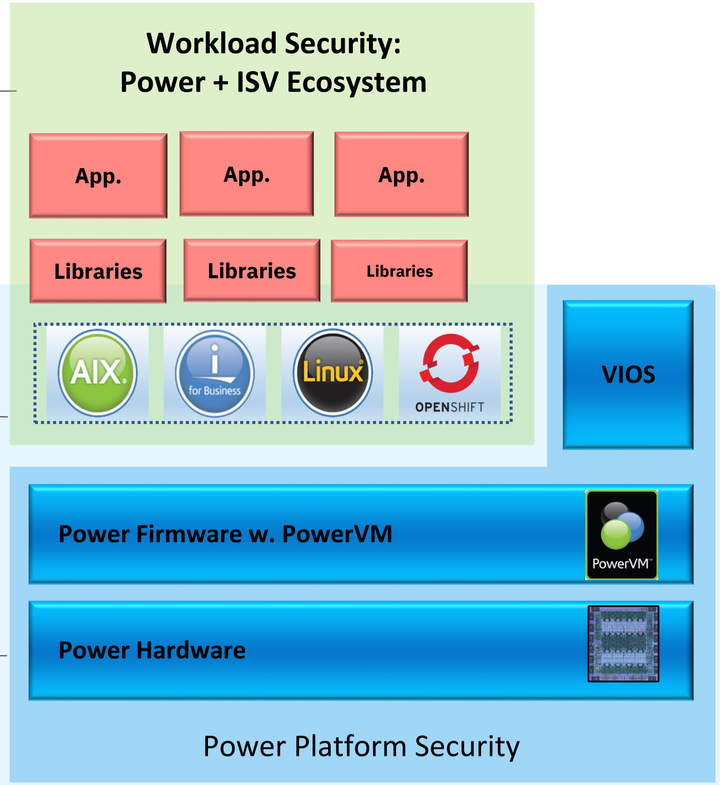
- End-to-End data encryption w. Bring/Keep Your Own Key (BYOK)

## Preserve Data & Workload Privacy

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

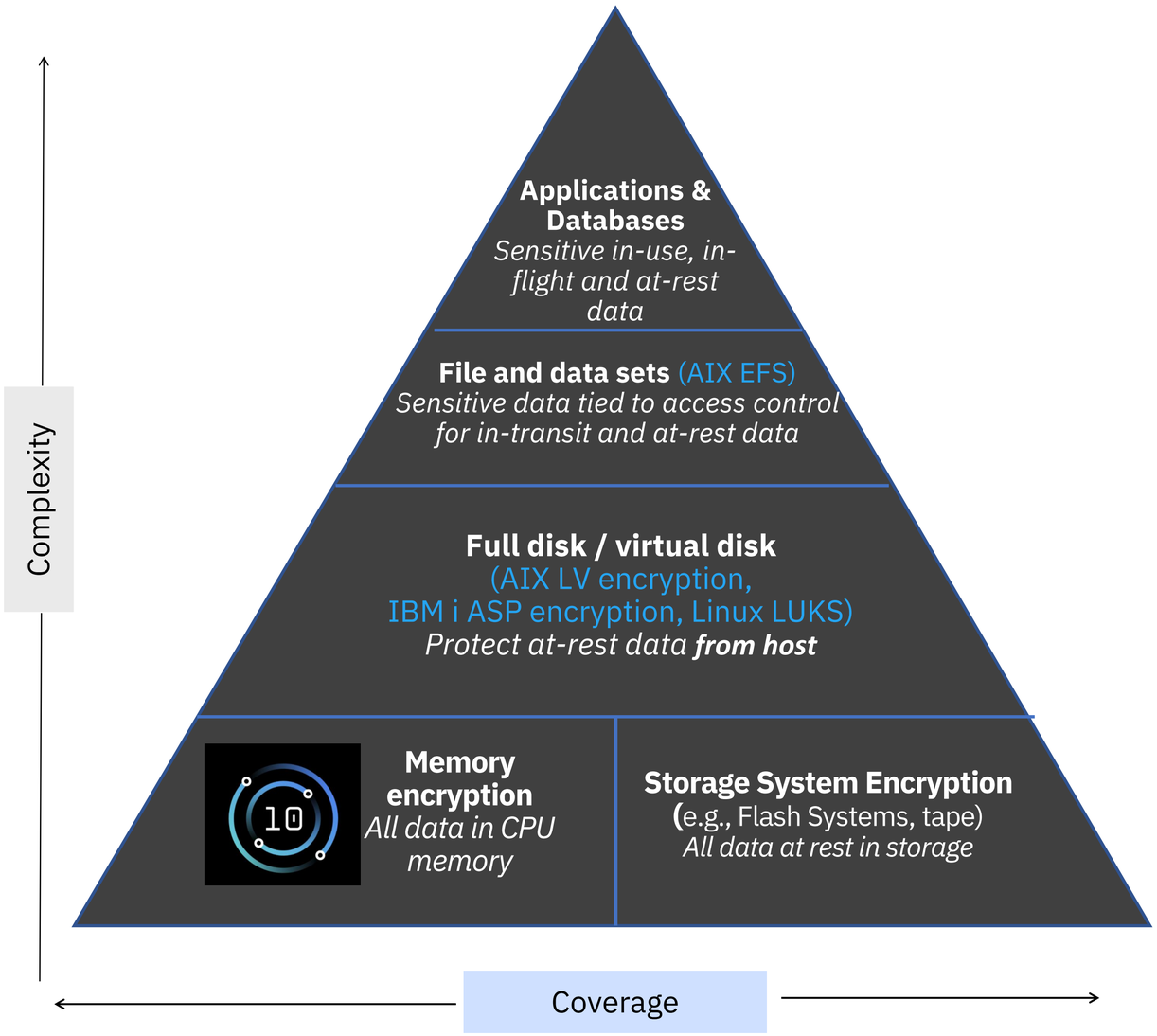
## Reduce the Risk of Ransomware

- Platform Integrity
  - Power10 enhanced CPU FSP/BMC isolation
  - Main memory encryption
  - Performance-enhanced side-channel avoidance
  - Power10 Return Oriented Programming (ROP) protection



# 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 Power10 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*

# Cryptography impacts everything

## Cryptography touches every corner of the digital world

**Internet**
Domain Name Service(DNS), Hyper-text Transfer Protocol (HTTP), Telnet, File-Transfer Protocol (FTP)

**Digital Signatures**
eIDAS – PDF Advanced Electronic Signature – (PAdES), Advanced Electronic Signatures (AES), ...

**Critical Infrastructure**
Code updates, Control systems, Car systems,...

**Financial Systems**
Payment Systems: (EMV, CHAPS, Fedwire, Target2, EURO1, ...), SWIFT, Settlement Systems, ...

**Blockchain**
Wallets, Transactions, Authentication

**Enterprise**
EMAIL – PGP, Identity Management PKI/LDAP/.., Virus scanning patterns, PKI Services, Bespoke applications, ...

## Upgrading digital infrastructure takes a long time

Passports – 10 years from issue

Road Vehicles – 15-20 Years

Critical Infrastructure – 25-30 Years

Aircrafts / Trains – 25-30 Years

(Some) Critical Mainframe Applications – 50 Years

## Data needs to stay secure for a long time

HIPAA – 6 years from its last use, Securities exchange act

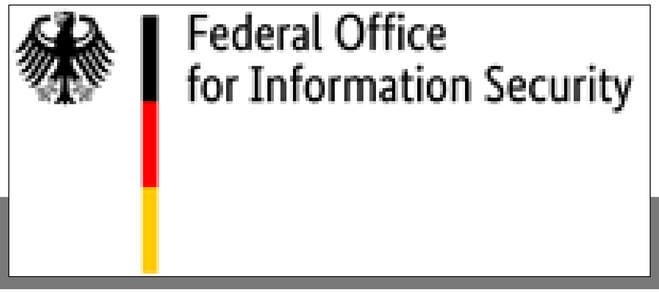
Tax Records – 7-10 Years in most countries, Sarbanes Oxley

Guide 0068 - Clinical Trials – 25 Years

Toxic Substances Control Act / Occupational Safety and Health Act

Medical Records in Japan – 100 years

# Start now!


- Critical to **begin planning** for the replacement of hardware, software, and services that use public-key algorithms **now**
- **Be ready to adopt and** implement the new algorithms at the end of the standardization process
- **5 to 15 or more years** following, standardization **to replace** most of the vulnerable public-key systems currently in use

- The protection of long-lasting secrets makes it **urgent** that actions be taken now or as soon as possible
- BSI is **not waiting** for NIST to come out with a standard to issue technical guidance
- In high security applications, hybrid schemes (use classical algorithms + quantum-safe algorithm) are **required** by BSI

https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography

# Power Roadmap Supporting Quantum Safe

## Positioning of Current Systems
(Power10)

- Existing systems will receive OS and Cryptographic Libraries Quantum Safe updates when they become available in the future.
- Early experiments and PoCs provide evidence that these systems will run Quantum Safe algorithms efficiently.

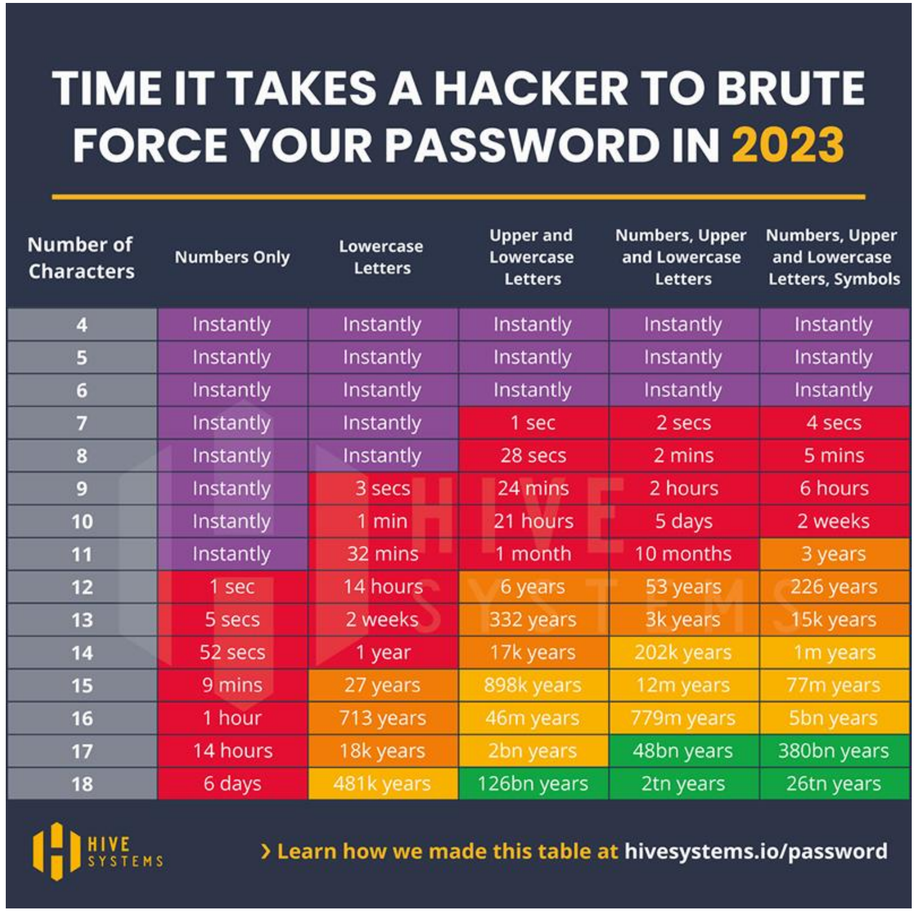
*All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only*

## Positioning of Power11

In addition to the Power10 updates, Power11 will include significant, updates to future-proof customer workloads and data, with priority on Quantum Safe firmware signing, consistent with CNSA 2.0 guidelines.

- Quantum Safe Hybrid Host Secure Boot to protect firmware integrity.
- Quantum Safe encryption of Live Partition Mobility (LPM) traffic to protect from “capture now, decrypt later” attacks.
- Offer the latest IBM Crypto Express Card, 4770, with support of Dilithium & Kyber Quantum Safe algorithms, with significantly faster performance than 4769.

# Change the default password for padmin!



**TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023**

| Number of Characters | Numbers Only | Lowercase Letters | Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters, Symbols |
|---|---|---|---|---|---|
| 4 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 6 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 7 | Instantly | Instantly | 1 sec | 2 secs | 4 secs |
| 8 | Instantly | Instantly | 28 secs | 2 mins | 5 mins |
| 9 | Instantly | 3 secs | 24 mins | 2 hours | 6 hours |
| 10 | Instantly | 1 min | 21 hours | 5 days | 2 weeks |
| 11 | Instantly | 32 mins | 1 month | 10 months | 3 years |
| 12 | 1 sec | 14 hours | 6 years | 53 years | 226 years |
| 13 | 5 secs | 2 weeks | 332 years | 3k years | 15k years |
| 14 | 52 secs | 1 year | 17k years | 202k years | 1m years |
| 15 | 9 mins | 27 years | 898k years | 12m years | 77m years |
| 16 | 1 hour | 713 years | 46m years | 779m years | 5bn years |
| 17 | 14 hours | 18k years | 2bn years | 48bn years | 380bn years |
| 18 | 6 days | 481k years | 126bn years | 2tn years | 26tn years |

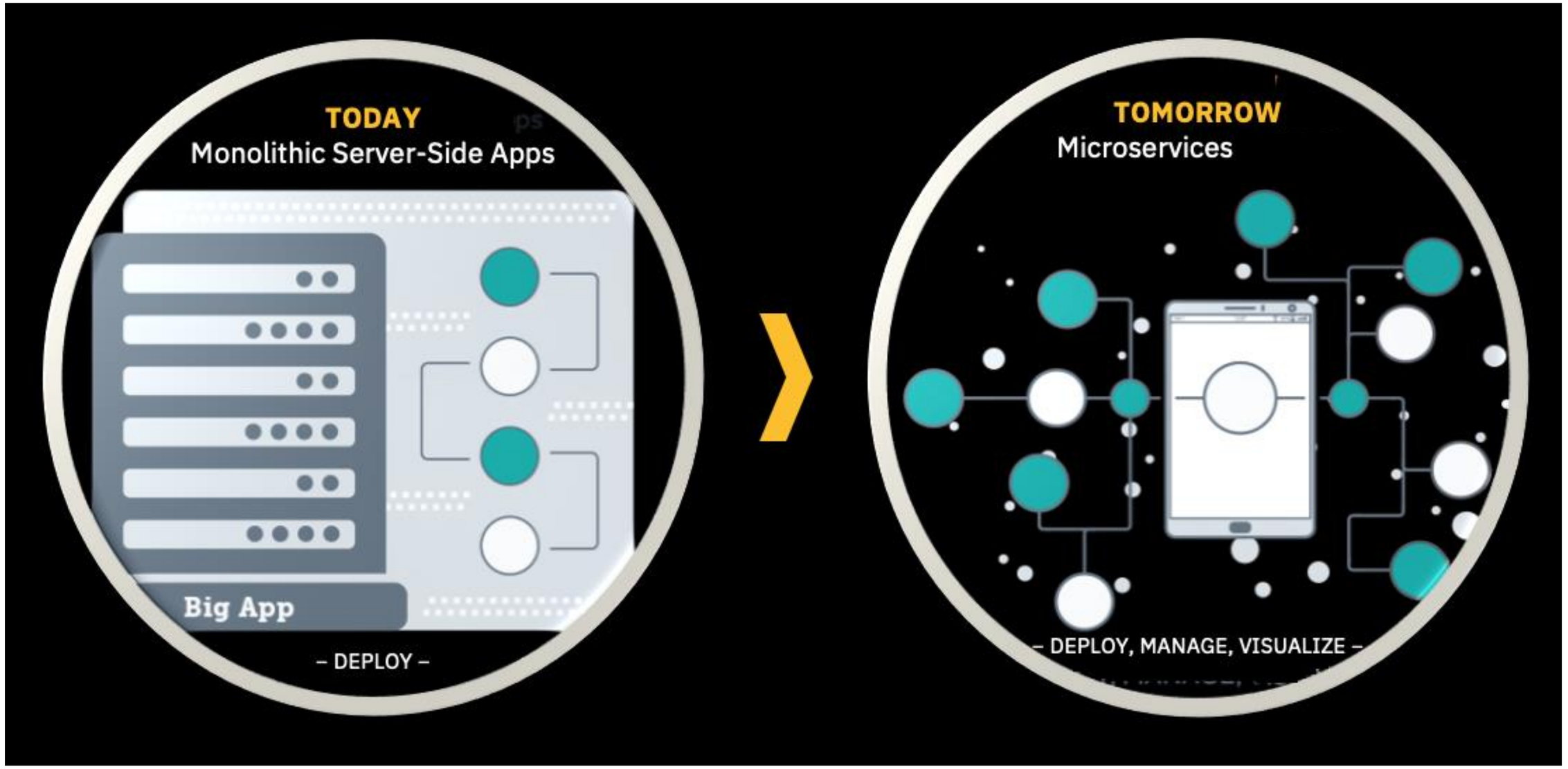
HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

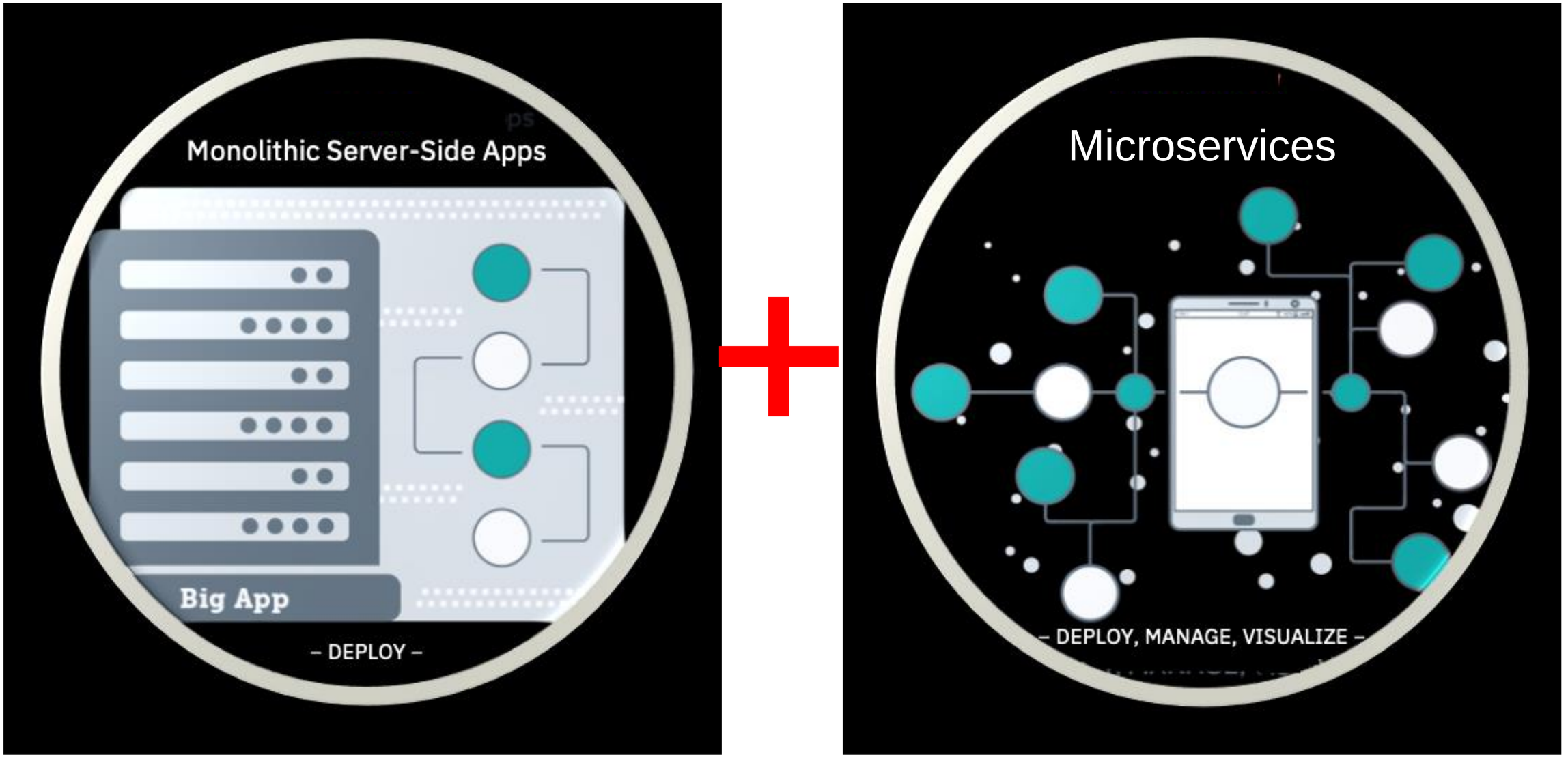
https://www.netsec.news/how-long-does-it-take-a-hacker-to-brute-force-a-password-in-2023

“The problem with passwords is they can be guessed, and **with modern GPUs**, brute-force attempts to guess passwords can crack weak passwords incredibly quickly. **Passwords of 6 characters, for instance, can be guessed instantly**, regardless of the letters, numbers, and special characters used.”

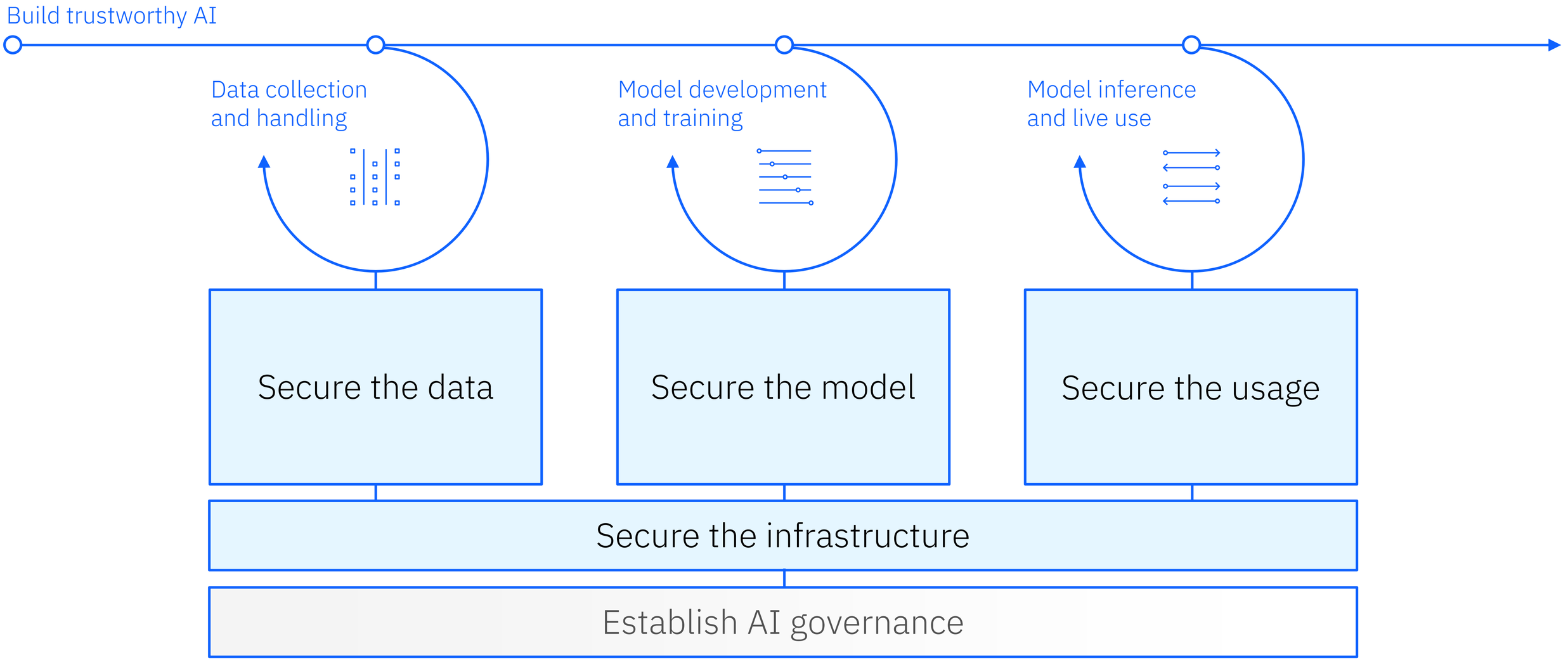
# Application Modernization Theory



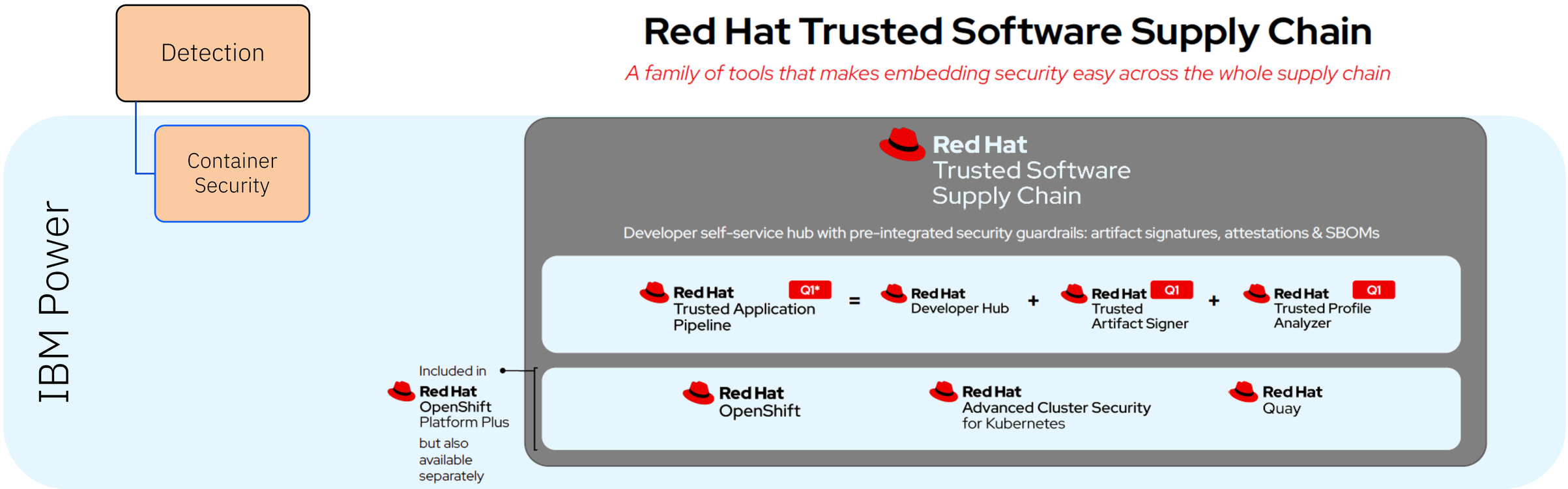
# Application Modernization Reality



# Safeguard AI Workflows - a holistic framework



# IBM Power and Container Security



Red Hat Customer Concerns

90%

Have experienced a security incident in their Kubernetes and container environments during the last 12 months.

92%

Found to have at least one CVE with known exploits in their environment at the time of scanning

1 in 5

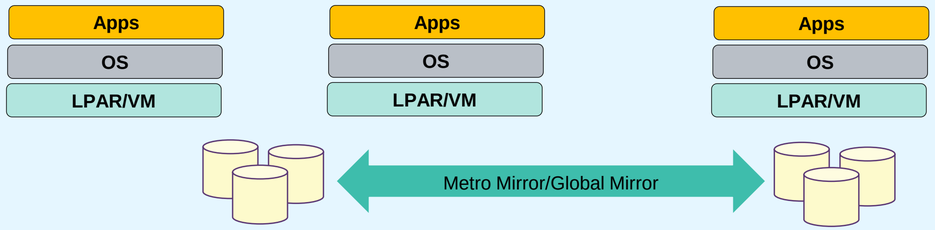
Security incident led to employee termination, and more than 1 in 3 experienced revenue or customer loss

# IBM Power value vs. DORA requirements

IBM Power

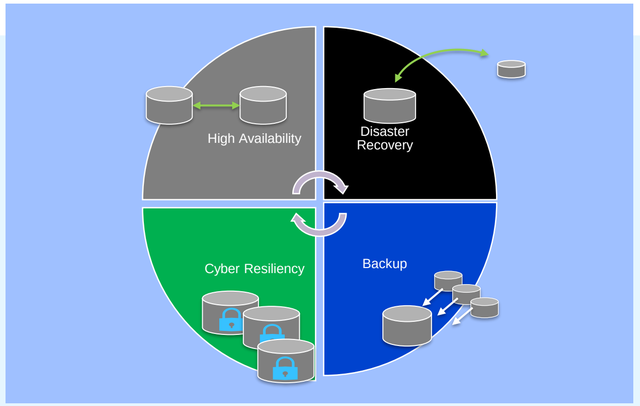
Response and Recovery

PowerHA



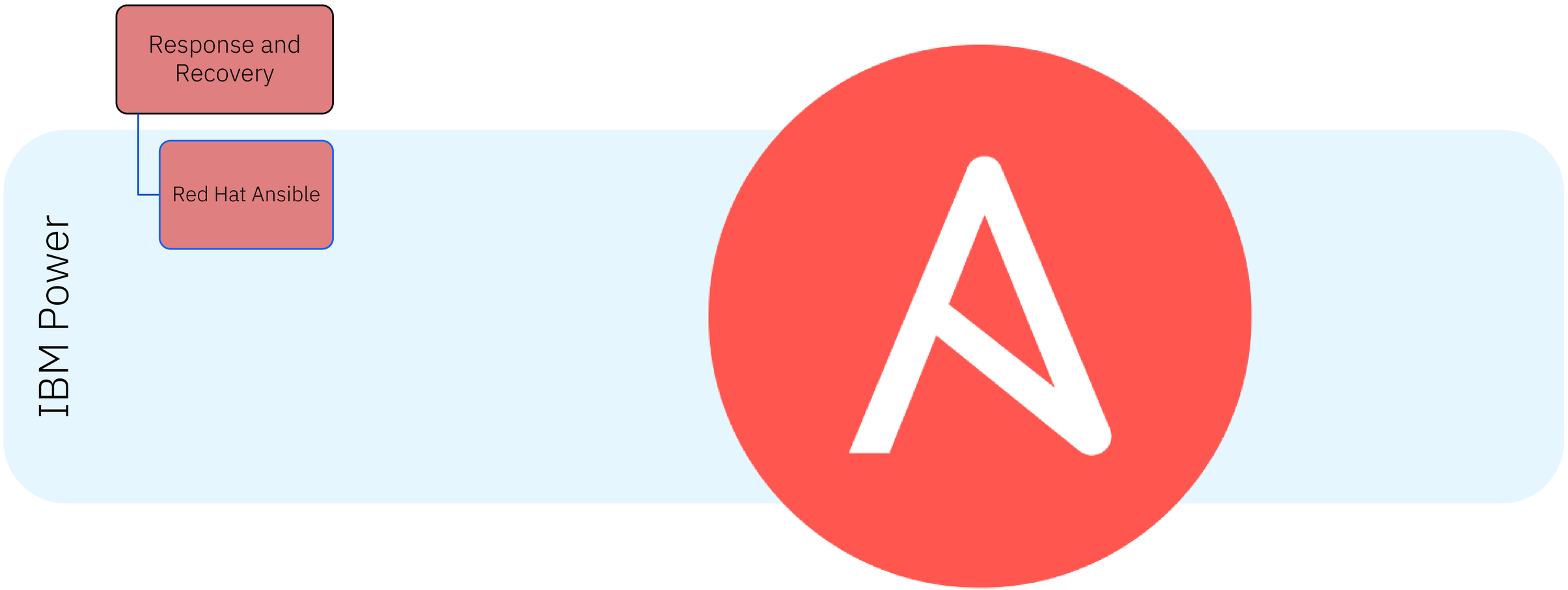

**PowerHA for AIX, PowerHA for IBM i**
- Provides highly automated business continuity
- Covers all outage types: planned, unplanned, HW, SW
- SAN storage replication for private cloud deployments

**VM Recovery Manager - Private Cloud**
- Automates LPM and VM restart in the datacenter
- Covers hardware outages, planned and unplanned
- SAN storage replication for DR operations
- Compliments PowerHA, supports AIX, i and Linux




**IBM Storage**
- Integrated resilient storage infrastructure
- Global Mirror, Metro Mirror, FlashCopy
- Multi-target for three site (DS8K), HyperSwap
- PowerHA 7.2.8 AIX Safeguarded Copy automation

# Automation



# BUILDING A CYBERSECURITY KINGDOM

# the old way

**Cavalry = Endpoint Protection**. Protects your local endpoints, such as computers and servers, with definition-based and behavior-based anti-virus, drive encryption, and device management. The cavalry protects the kingdom and its people from bad actors.

**Drawbridge = VPN Connection**. Allows off-network visitors to safely and securely access your business. Think of it as having a secret password for lowering the drawbridge to enter the castle.

**Castle Wall = Firewall**. Prevents incoming security threats with automatic remediation, sandboxing, anti-virus, intrusion prevention, and content filtering. The castle wall deters and catches threats.

**Gatehouse = Multifactor Authentication**. MFA provides an additional layer of security by verifying your identity using more than one method. For example, MFA prevents unwanted access to critical information by verifying usernames and passwords with an additional secret code, usually delivered through a mobile device or notification. The Gatehouse provides an extra layer of security when accessing assets (like files or software programs) that are on your network or in the cloud.

**Guardian = EDR**. Endpoint Detection and Response (EDR) monitors your entire business for suspicious behavior in real-time to detect cyberattacks, isolate infected machines, alert administrators, and remove cyberthreats. Like an omniscient guardian, EDR recognizes advanced, sneaky attacks and shuts them down before they attack your business, anywhere an asset is located.

**Library = User Education**. Teaches users about safe IT practices, such as internet, email, and peripheral device usage; password management; and data control. User educations also includes testing to ensure students retain what they have learned.

**Clerks = Security Information and Event Management (SIEM)**. Records and stores your system's log files for use if a cyberattack occurs. Think of SIM like clerks recording a history of the castle's happenings for future scholars to reference.

**Royal Archives = Data Backup**. Whether you're on-premise or working from home, company files are stored, up-to-date, and protected.

**Guards = Anti-Virus**. Anti-virus keeps your business safe from known cybersecurity threats and bad actors. The guards need to be informed or see something illegal happening before responding.

**Masons = Patching**. Maintains your hardware, software, operating system, and security with regular code updates as new threats and vulnerabilities are detected. Patching works like masons who identify and repair cracks, holes, and other weak points in the castle's walls.

**Moat = Email Security**. Automatically scans email for spam, unlawful interception, phishing, malicious attachments. Encrypts outbound emails containing sensitive data and employs advanced threat protection (ATP) to identify bad actors based on their behavior. The moat ensures only safe traffic enters and exits the castle.

# BUILDING A CYBERSECURITY KINGDOM

# the old way

**Cavalry = Endpoint Protection**. Protects your local endpoints, such as computers and servers, with definition-based and behavior-based anti-virus, drive encryption, and device management. The cavalry protects the kingdom and its people from bad actors.

**Drawbridge = VPN Connection**. Allows off-network visitors to safely and securely access your business. Think of it as having a secret password for lowering the drawbridge to enter the castle.

**Castle Wall = Firewall**. Prevents incoming security threats with automatic remediation, sandboxing, anti-virus, intrusion prevention, and content filtering. The castle wall deters and catches threats.

**Gatehouse = Multifactor Authentication**. MFA provides an additional layer of security by verifying your identity using more than one method. For example, MFA prevents unwanted access to critical information by verifying usernames and passwords with an additional secret code, usually delivered through a mobile device or notification. The Gatehouse provides an extra layer of security when accessing assets (like files or software programs) that are on your network or in the cloud.

**Guardian = EDR**. Endpoint Detection and Response (EDR) monitors your entire business for suspicious behavior in real-time to detect cyberattacks, isolate infected machines, alert administrators, and remove cyberthreats. Like an omniscient guardian, EDR recognizes advanced, sneaky attacks and shuts them down before they attack your business, anywhere an asset is located.

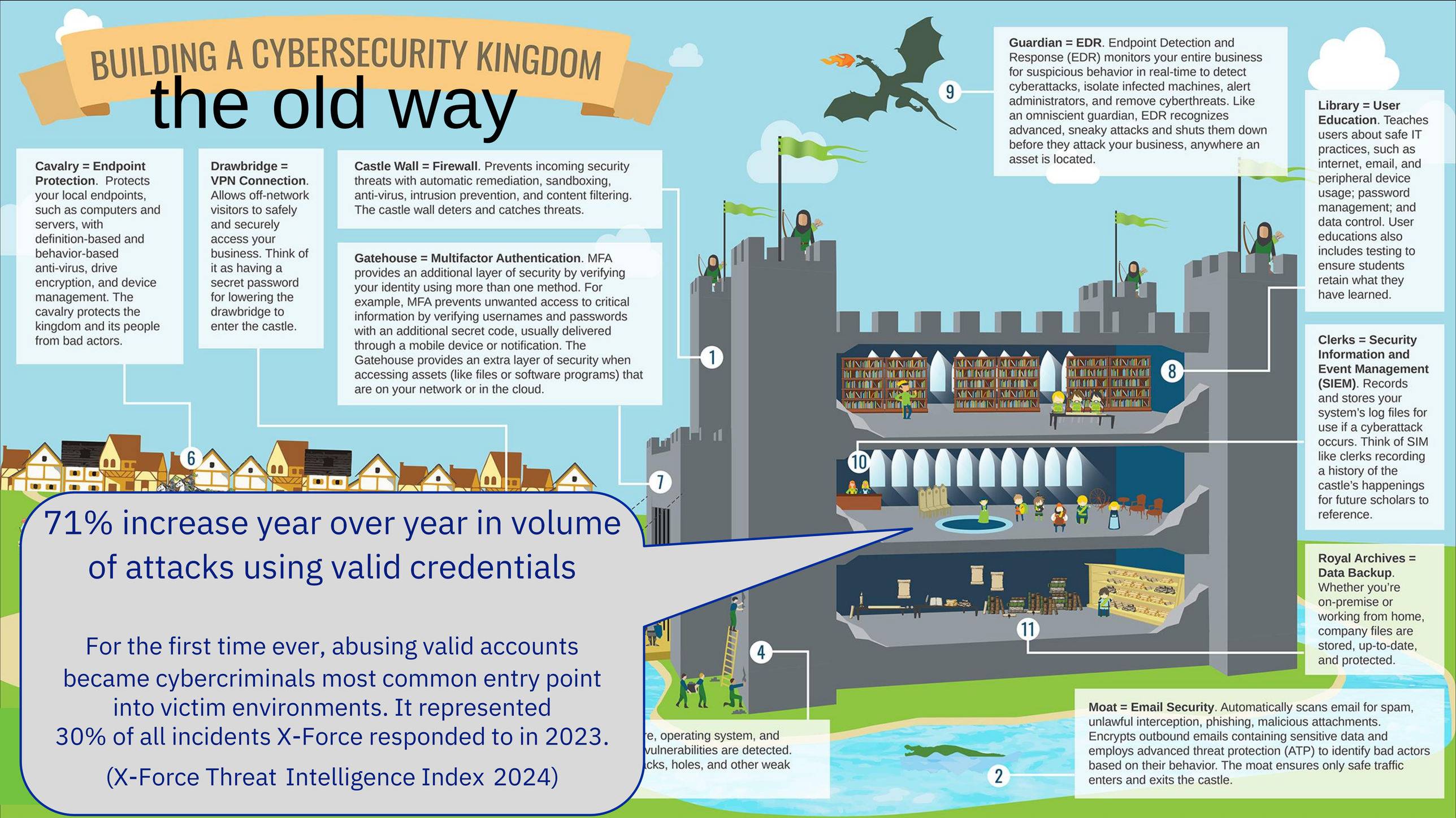
**Library = User Education**. Teaches users about safe IT practices, such as internet, email, and peripheral device usage; password management; and data control. User educations also includes testing to ensure students retain what they have learned.

**Clerks = Security Information and Event Management (SIEM)**. Records and stores your system's log files for use if a cyberattack occurs. Think of SIM like clerks recording a history of the castle's happenings for future scholars to reference.

**Royal Archives = Data Backup**. Whether you're on-premise or working from home, company files are stored, up-to-date, and protected.

**Moat = Email Security**. Automatically scans email for spam, unlawful interception, phishing, malicious attachments. Encrypts outbound emails containing sensitive data and employs advanced threat protection (ATP) to identify bad actors based on their behavior. The moat ensures only safe traffic enters and exits the castle.

re, operating system, and
vulnerabilities are detected.
cks, holes, and other weak



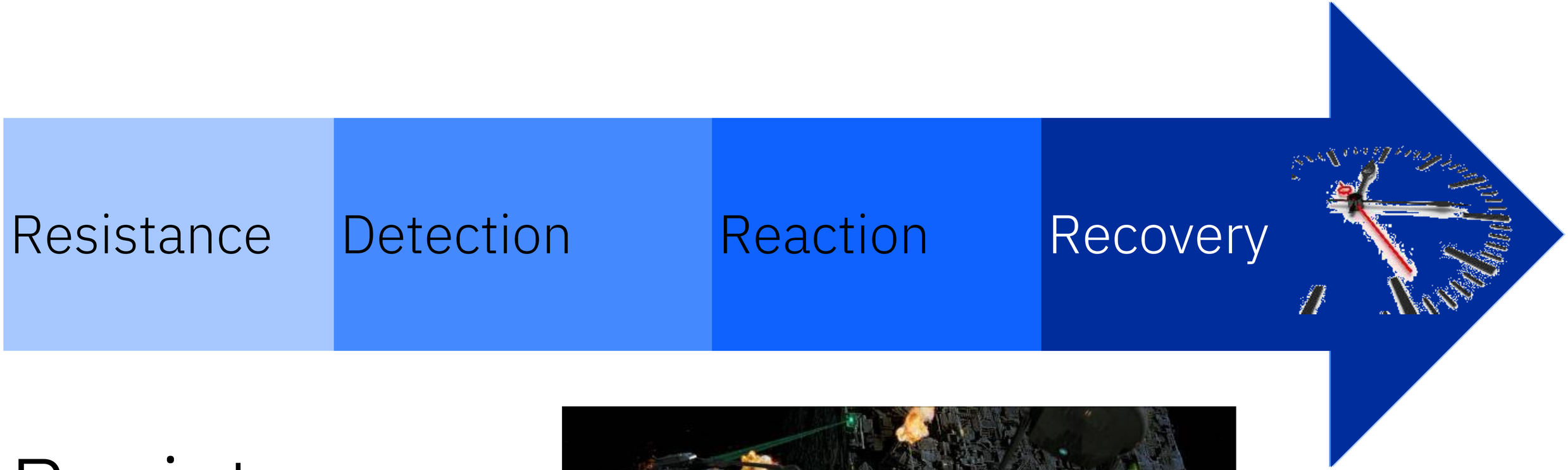

71% increase year over year in volume of attacks using valid credentials

For the first time ever, abusing valid accounts became cybercriminals most common entry point into victim environments. It represented 30% of all incidents X-Force responded to in 2023.

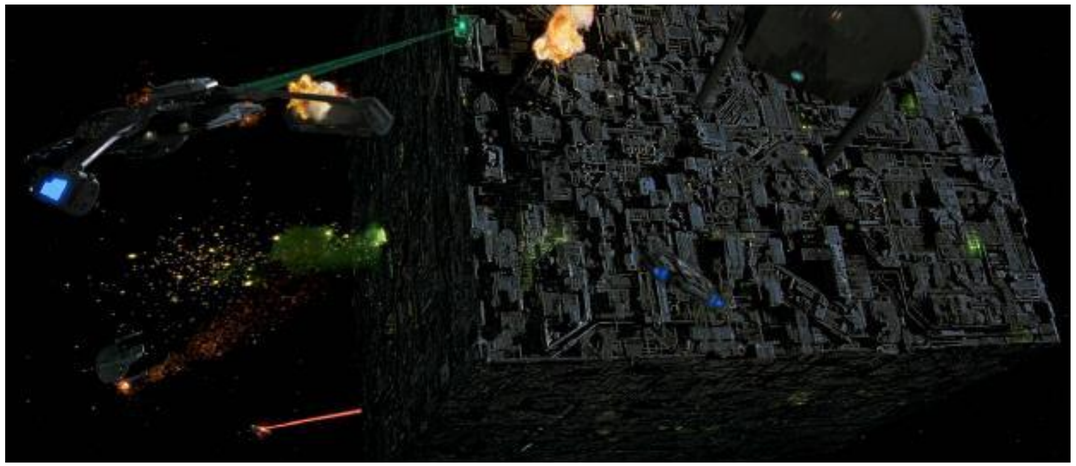
(X-Force Threat Intelligence Index 2024)

# The timeline of a cyber “event”

Resistance | Detection | Reaction | Recovery



## Resistance is not futile!



# Where are you on the Zero Trust journey?

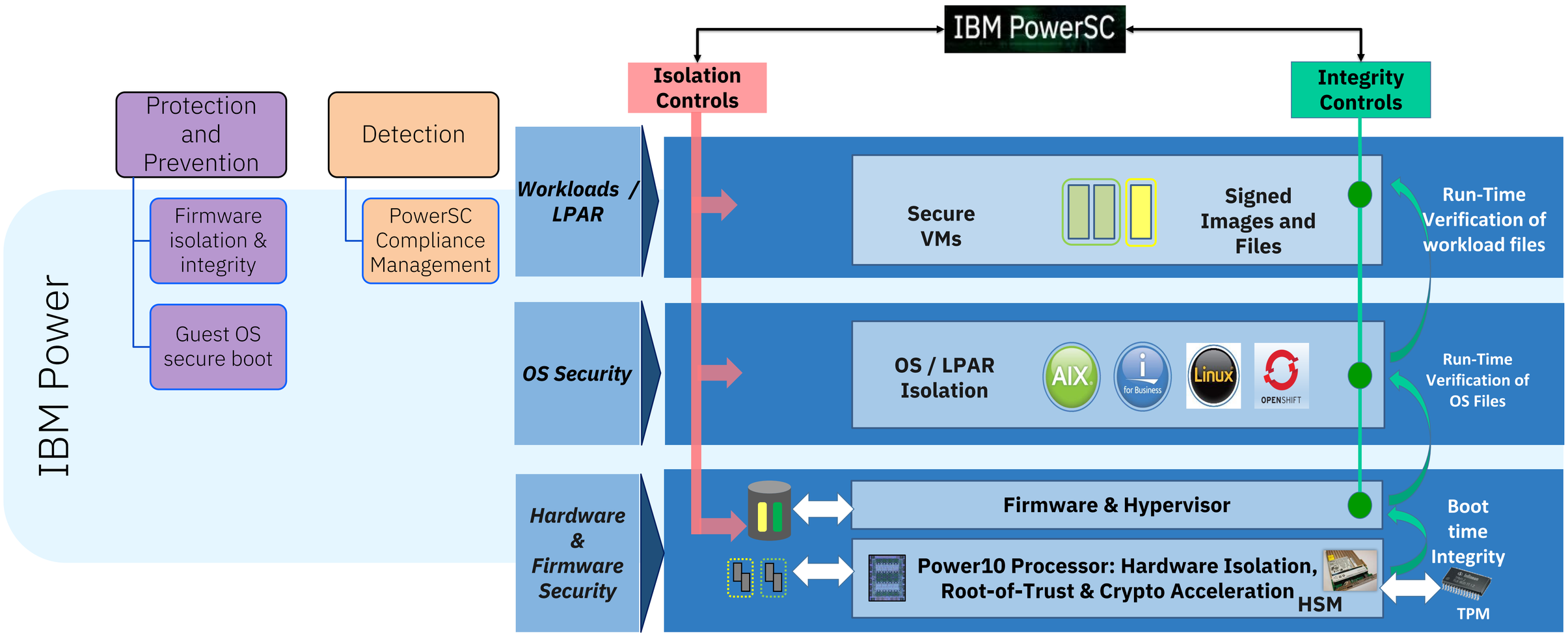
| Preparing for ZT | Basic ZT | Intermediate ZT | Advanced ZT |
|---|---|---|---|
| Adhoc processes | Defined processes and best practices | Repeatable processes and best practices | Automated |

PowerVC
PowerVM

PowerSC

Radar

# IBM Power value vs. NIST requirements



View Security and Compliance status of an entire Power datacentre through a single pane of glass.

## Automate Protection

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

## Broad Compliance

Deploy industry standard security with preconfigured security profiles that are customizable.

## Detect

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

## Respond

View and Orchestrate anomaly responses with Endpoint Detection and Response & anti-malware

## Recover

Reduce recovery time in the (unlikely) case of breaches via integration with IBM Storage Safeguarded Copies.

**Data Sheet**

# PowerSC Security Features

| Feature | PowerSC 2.2 |
|---|---|
| Automated compliance | ✔ Check and Apply |
| Compliance reporting capabilities (incl timelines) | ✔ AIX, Linux, IBM i |
| File Integrity Monitoring | ✔ AIX, Linux, IBM i |
| Allow Listing / Application Control | ✔ AIX & Linux |
| Block Listing / Threat Hunting (hash search) | ✔ AIX, Linux, IBM i |
| Anti-Malware (virus DB) | ✔ AIX, Linux, IBM i |
| Integration with IBM Safeguarded Copy | ✔ AIX, Linux, IBM i |
| Patch Management | ✔ AIX, Linux, IBM i |
| Endpoint Detection and Response (EDR) | ✔ AIX, Linux, IBM i |
| Intrusion Detection Sys & Prevention / Firewall (EDR) | ✔ AIX & Linux |
| Log inspection & analysis (EDR) | ✔ AIX, Linux, IBM i |
| Anomaly detection, correlation & incident response (EDR) | ✔ AIX, Linux, IBM i |
| Response / action triggers (EDR) | ✔ AIX, Linux, IBM i |
| Event context and filtering (EDR) | ✔ AIX, Linux, IBM i |
| Multifactor Authentication (MFA) | ✔ AIX, Linux, IBM i |

# Management software

PowerSC 2.2.0.3

- New service pack release available on FixCentral
- Policy based profile management
- New profiles
- CIS for IBM i 7.5
- PCIv4 for AIX and Linux
- Restart PowerSC Agents from GUI server
- Skipping NFS mounts for anti-malware scans
- Ability to parse FLRT JSON files for ifix lists
- Ability to update malware database within GUI

PowerSC 2.2.0.4 (December 2024)

- PowerSC GUI Server can be run on IBM i as well as AIX / Linux
- Quantum inventory capability
- Selective apply / undo for profiles
- Generic event acceptance for other PowerSC events and other application logs
- LKU support within PowerSC GUI
- OpenSSL update for AIX Trusted Boot
- Health report

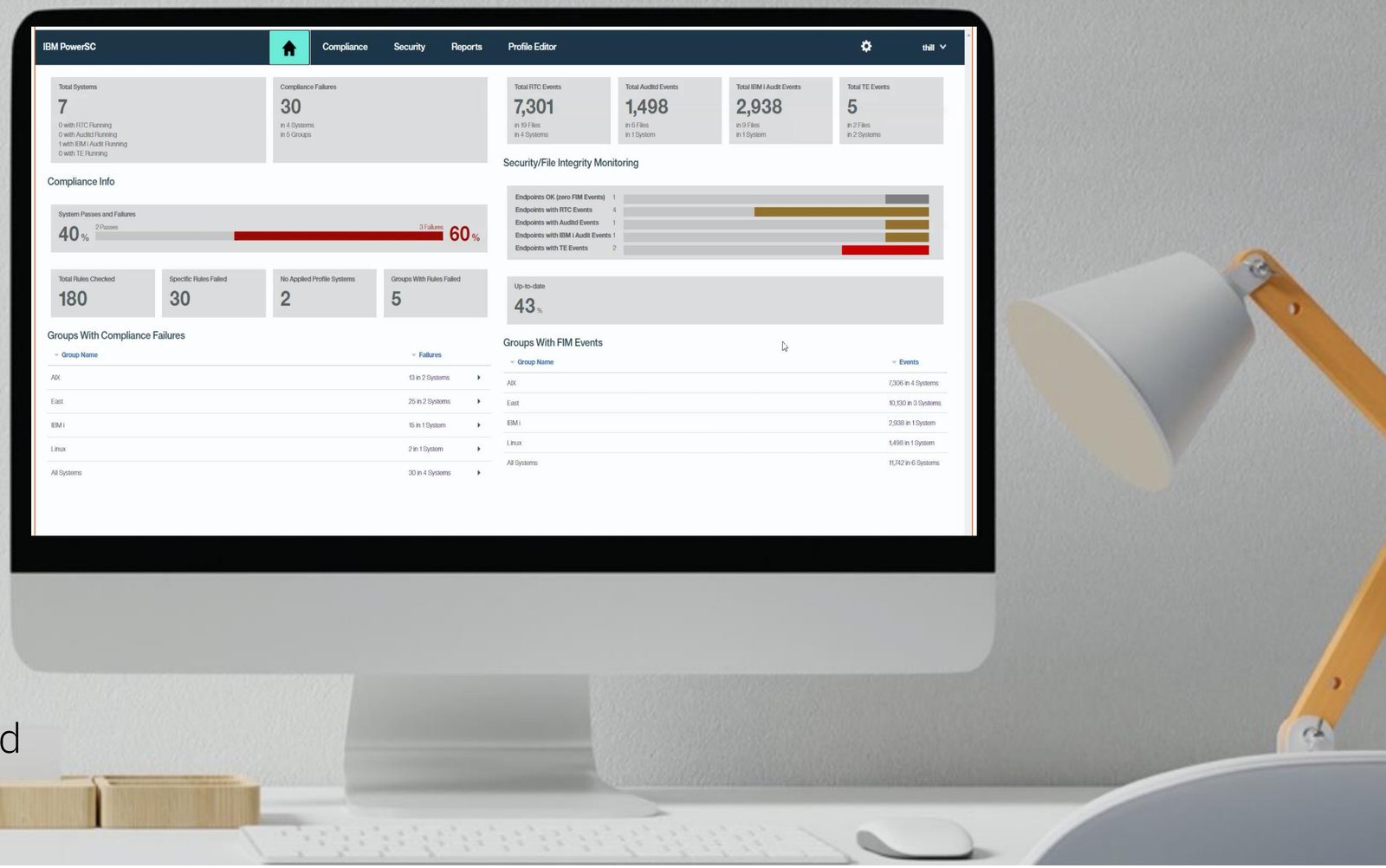
# PowerSC provides a user-friendly, web-based UI to manage Security & Compliance

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

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

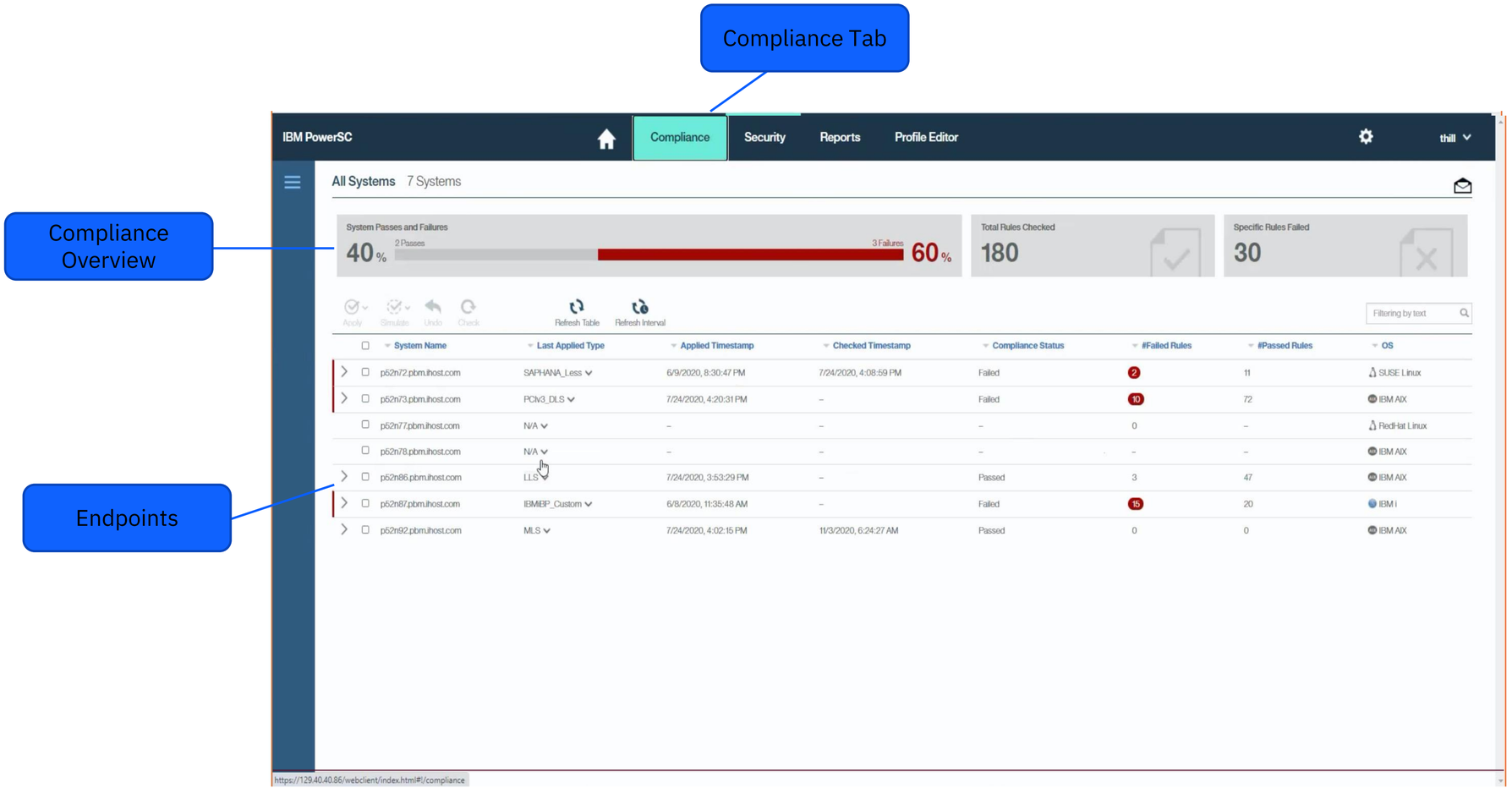
## Patch Management
- Trusted Network Connect (TNC)
- Detect & alert policy issues
- Policy enforcement

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



# PowerSC Compliance Dashboard


- Compliance dashboard
- Compliance overview status
- Automated enforcement
- Profile check and simulation
- Failure analysis
- Profile customization




Alerts sent for non-compliance

# Endpoint Protection – Correlation

- Recognize trends and patterns over time
- Near real-time analysis
- Root cause and symptomatic messages

EDR Capabilities

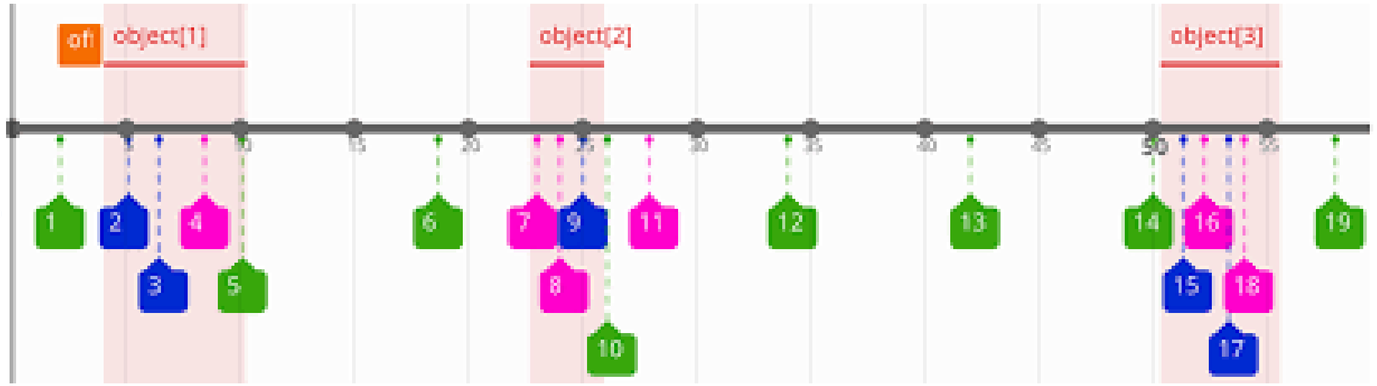
Intrusion Detection & Prevention (IDP)

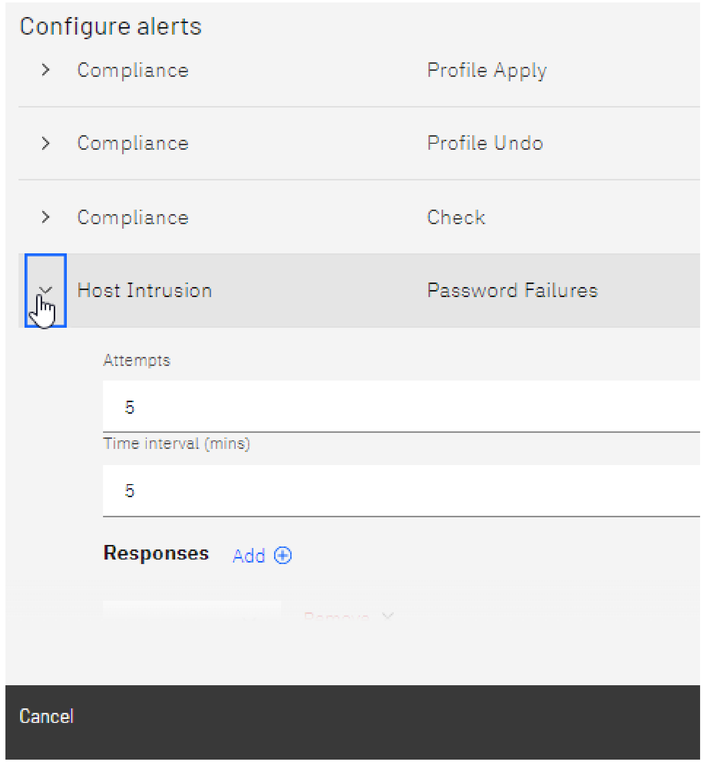
Log Inspection & Analysis

Anomaly detection, correlation & incident response

Response Triggers

Event context & filtering



# Malware

https://ibm.biz/powersc-clamav

“This service provides deployment of up to three measures for malware defense: Threat Hunting, Allowlisting, and ClamAV. The PowerSC Graphical User Interface (GUI) server provides browser-based centralized management of these security measures deployed on endpoints configured with the PowerSC GUI agent.”

# Cyber Resilience Assessment

The Cyber Resiliency Assessment  provides a way to evaluate the current data resilience of the organization, identifies strengths and weaknesses and provides recommendations to **build an effective cyber resilience plan.**

[IBM Cyber Resiliency Assessment]


Storage Cyber Resiliency & Disaster Recovery Assessment Report

IBM Security & Resilience

January 5, 2021

Overview

IBM is pleased to present [a report based on our findings from the IBM® Storage Cyber Resilience & Disaster Recovery Assessment workshop that took place with the [Customer] team on December 5th, 2019. It is understood that an effective cybersecurity resiliency program must be grounded in effective systems and processes that provide valuable insight into information and events that occur within an environment and provide the confidence for an orchestrated storage resiliency process in order to not disrupt [Customer]'s business continuity objectives. By evaluating the current cybersecurity and resiliency environment, the organization now has specific recommendations designed to help increase the value of the solution and services in its environment and meet RTO and RPO requirements.

Additionally, [Customer] will be able to help deliver faster return on investment and higher operational productivity by leveraging time-tested practices and updates to product features and resiliency functions. It will be able to help decrease errors and inconsistency through the implementation of the incremental recommendations we have provided in this document.

Executive summary

Based on the information gathered during our initial reviews within IBM during 4Q 2019 as well as the assessment workshop in Benton Harbor on December 5th, [Customer] has realized great value from its investment in cyber resilience and is generally on-par with other customers that IBM has worked with. However, there are several areas where [Customer] has exposure to risk resulting in unrecoverable data loss or corruption and where more value can be realized.

[Customer] has many IT service providers of which IBM is a significant partner. Of the many environments considered and reviewed for this assessment, we have taken an enterprise-view.

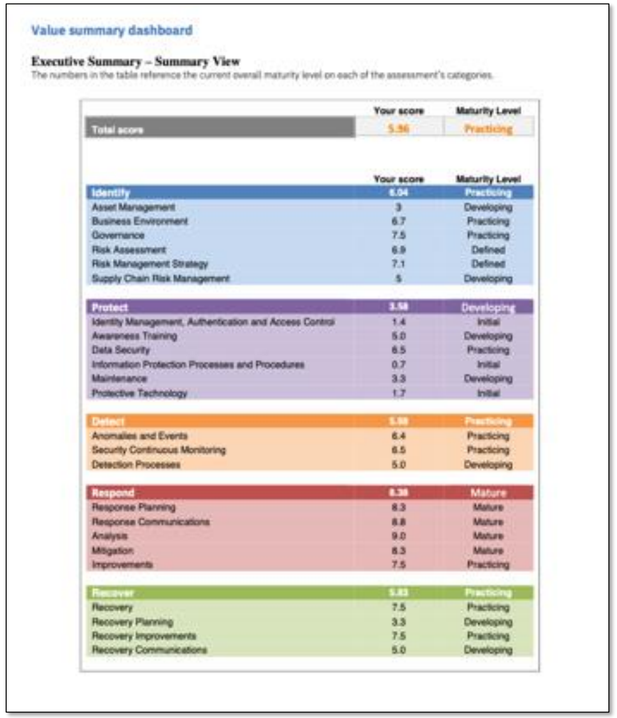
Performance in the environment is satisfactory, though [Customer] recognizes that the organization is one cyber breach away from severely impacting business continuity. [Customer] senior management must understand that risk is the new normal. Being a digital enterprise in 2020 incurs significant risk and Cyber Resiliency (protection, data vaulting and recovery) is now an absolute part of the cost of doing business.

Additionally, IBM feels that [Customer] would benefit from the use of Spectrum Insights to measure different performance and capacity areas in order to drive them toward strong outcomes.

Cyber resiliency should be viewed as a dynamic and ever-evolving practice that requires continuous improvement and focus. With the continued expansion of the threat landscape and pace of technology change, it is imperative that organizations constantly take inventory of how they are doing and where they need to be evolving.

Please review the Recommendation Section for our roadmap, which, if followed, will improve functionality and increase the value realized from implementing resiliency and disaster recovery best practices and solutions. Establishing a mature cyber security and resiliency plan will enable a more proactive approach in detecting, identifying, and protecting their environments, as well as their ability to respond and recover quickly.

IBM

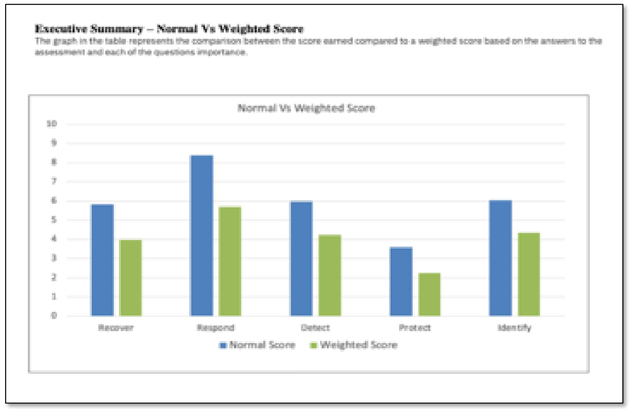

Value summary dashboard

Executive Summary – Summary View

The numbers in the table reference the current overall maturity level on each of the assessment's categories.

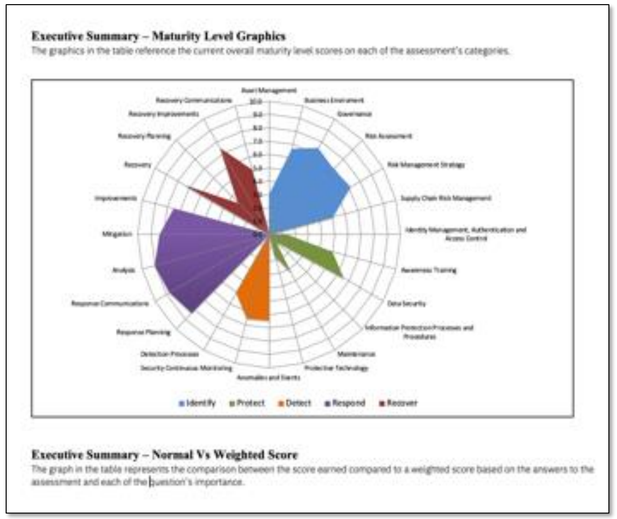
| | Your score | Maturity Level |
|---|---|---|
| Total score | 5.86 | Practicing |

| | Your score | Maturity Level |
|---|---|---|
| Identify | 6.04 | Practicing |
| Asset Management | 3 | Developing |
| Business Environment | 6.7 | Practicing |
| Governance | 7.5 | Practicing |
| Risk Assessment | 6.9 | Defined |
| Risk Management Strategy | 7.1 | Defined |
| Supply Chain Risk Management | 5 | Developing |
| Protect | 3.58 | Developing |
| Identity Management, Authentication and Access Control | 1.4 | Initial |
| Awareness Training | 5.0 | Developing |
| Data Security | 6.5 | Practicing |
| Information Protection Processes and Procedures | 0.7 | Initial |
| Maintenance | 3.3 | Developing |
| Protective Technology | 1.7 | Initial |
| Detect | 5.93 | Practicing |
| Anomalies and Events | 6.4 | Practicing |
| Security Continuous Monitoring | 6.5 | Practicing |
| Detection Processes | 5.0 | Developing |
| Respond | 6.38 | Mature |
| Response Planning | 6.3 | Mature |
| Response Communications | 6.8 | Mature |
| Analysis | 9.0 | Mature |
| Mitigation | 6.3 | Mature |
| Improvements | 7.5 | Practicing |
| Recover | 5.83 | Practicing |
| Recovery | 7.5 | Practicing |
| Recovery Planning | 3.3 | Developing |
| Recovery Improvements | 7.5 | Practicing |
| Recovery Communications | 5.0 | Developing |


Executive Summary – Normal Vs Weighted Score

The graph in the table represents the comparison between the score earned compared to a weighted score based on the answers to the assessment and each of the questions importance.





Executive Summary – Maturity Level Graphics

The graphics in the table reference the current overall maturity level scores on each of the assessment's categories.




Executive Summary – Normal Vs Weighted Score

The graph in the table represents the comparison between the score earned compared to a weighted score based on the answers to the assessment and each of the question's importance.

# Summary

- IBM Power delivers reliable performance and lowers risk
- With built in security features and orders of magnitude fewer vulnerabilities, IBM Power is reliable platform
- Apply security standards quickly and easily, and get real time alerts if compliance is broken
- Surround resilient applications with trusted and secure containers to modernise
- A secure infrastructure is part of the framework for trusted AI

# Thank you!

David Spurway
IBM Power AI and Sustainability
Principal, EMEA, IBM Technology
Email: david.spurway@uk.ibm.com
LinkedIn: @David Spurway