



IBM **LinuxONE™**

LinuxONE and Linux on Z Security and Compliance - Update

Pradeep Parameshwaran

Technical Security Lead for LinuxONE and
Linux on Z



THE INFORMATION CONTAINED IN THIS PRESENTATION IS IBM CONFIDENTIAL AND IS BEING DISCLOSED TO YOU UNDER THE TERMS OF THE IBM ZCLIENT FEEDBACK PROGRAM AGREEMENT IN PLACE BETWEEN IBM AND YOUR COMPANY.

DISCLAIMER

- THE INFORMATION ON THE NEW PRODUCT IS INTENDED TO OUTLINE OUR GENERAL PRODUCT DIRECTION AND IT SHOULD NOT BE RELIED ON IN MAKING A PURCHASING DECISION.
- THE INFORMATION ON THE NEW PRODUCT IS FOR INFORMATIONAL PURPOSES ONLY AND MAY NOT BE INCORPORATED INTO ANY CONTRACT.
- THE INFORMATION ON THE NEW PRODUCT IS NOT A COMMITMENT, PROMISE, OR LEGAL OBLIGATION TO DELIVER ANY MATERIAL, CODE OR FUNCTIONALITY.
- THE DEVELOPMENT, RELEASE, AND TIMING OF ANY FEATURES OR FUNCTIONALITY DESCRIBED FOR OUR PRODUCTS REMAINS AT OUR SOLE DISCRETION.

Agenda



IBM LinuxONE III Security Capabilities



New Security Offerings on LinuxONE III
& Linux on IBM Z




Hardening Recommendations



Ease of use compliance aspects

IBM LinuxONE™ Security Capabilities

Integrated Hardware Crypto Accelerators

CPACF – Crypto accelerator on every core for high-speed, bulk symmetric encryption
 Crypto Express7S – PCIe Hardware Security Module (HSM) & Cryptographic Coprocessor

EAL 5+ Isolation and Virtualization

Workload isolation with design for highest EAL5+ security certification
Full sharing/partitioning of the installed resources with the highest levels of efficiency and utilization



IBM Hyper Protect Virtual Servers

Securely build, deploy and manage mission-critical applications for hybrid multicloud environments on IBM® Z® and LinuxONE systems.



Data Privacy Passports

Broadly protect Linux file systems across multiple hybrid data environments using fully encrypted trusted data objects with policy control and access revocation

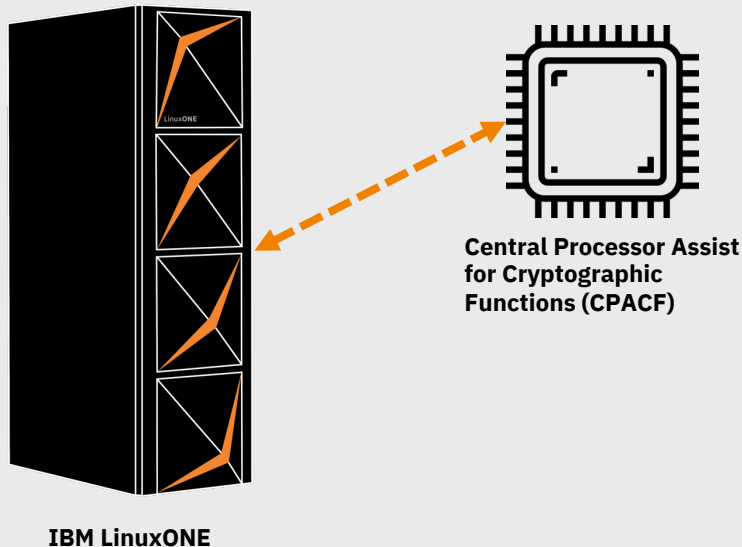


Boot Integrity for Linux

Protect your system against root level attacks and vulnerabilities during boot process
Complete chain of trust to IPL Linux from a trusted and verified boot loader

CPACF

On-Chip Crypto Acceleration



Accelerate your encryption

Hardware accelerated encryption on every microprocessor core

Protected Keys - Key values are never exposed to the OS, hypervisor, or application

Suited for high speed bulk symmetric encryption

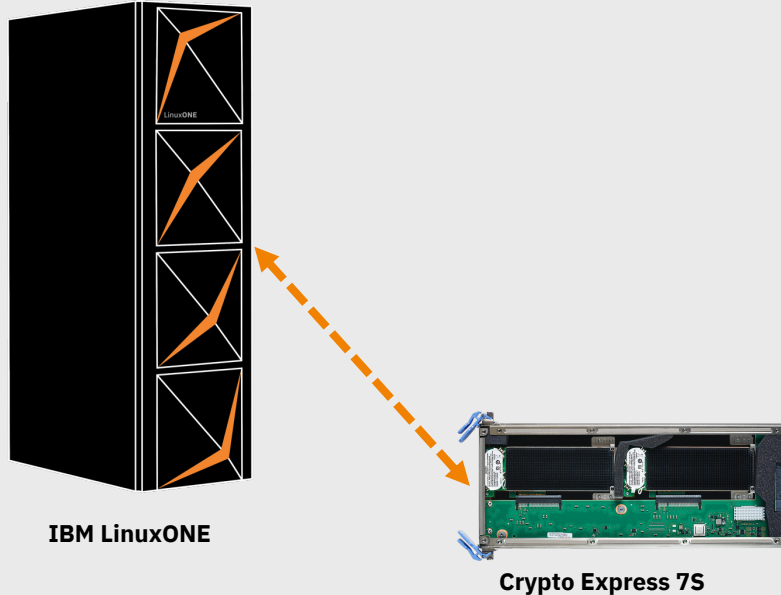
Why on-chip encryption?

More performance = lower latency and less CPU overhead for encryption operations

No-charge feature enabled on all LinuxONE systems

Crypto Express7S

Hardware Security Module (HSM)



Protect encryption keys

Secure encryption keys with tamper-responding cryptographic hardware

Suited for high value transactions, key protection, and asymmetric acceleration

FIPS 140-2 Certification

Level 1: No physical security features required

Level 2: Tamper-evident physical security features

Level 3: Tamper-responding features designed to notify of unauthorized access

Level 4: Complete tamper-responding envelope of protection that immediately deletes all plaintext keys upon detection of unauthorized access

Cryptographic acceleration with LinuxONE III hardware



Cryptographic acceleration with Crypto Express7S:

Improved SSL/TLS handshake performance on LinuxONE III with Crypto Express7S compared to Crypto Express6S

Updates to Common Cryptographic Architecture (CCA) for security modules that enhance remote ATM key loading, offer new protections for banking payments, and extended compliance support to stay up to date on industry standards

Cryptographic coprocessor on every core with CP Assist for Cryptographic Function (CPACF):

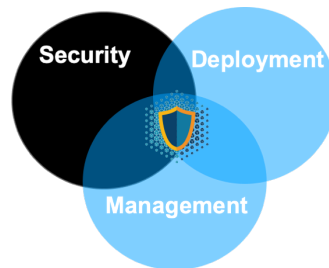
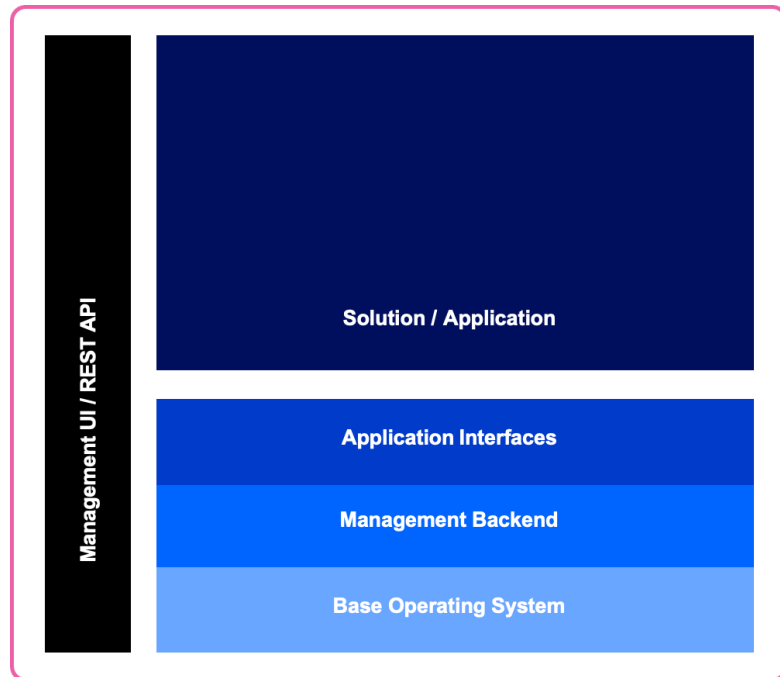
Enhanced with Elliptic-Curve Cryptographic (ECC) algorithms that can help reduce CPU consumption for applications like blockchain

Enable an EP11 secure key to be converted to a protected key that can be used by CPACF

New Security Offerings on LinuxONE III / Linux on IBM Z

IBM Secure Service Container hosting appliance

- Secure computing environment for hybrid and private cloud workloads
- **Automatic pervasive encryption** data and code in-flight and at-rest
- Straightforward deployment **without requiring code changes** to exploit security capabilities
- Restricted administrator access to help **prevent misuse of privileged user credentials**
- **Tamper protection** during installation



Secure
Service
Container

IBM Hyper Protect Virtual Servers

Protect critical Linux workloads during build, deployment, and management on-premise for IBM Z and LinuxONE servers



Build

applications with security

Leverage the secure image build process to sign images, validate code, and integrate into CICD



Deploy

workloads with trust

Provenance - Validate the origin of your applications before deployment



Manage

applications with simplicity

Manage infrastructure without visibility to sensitive code or data – RESTful API deployment

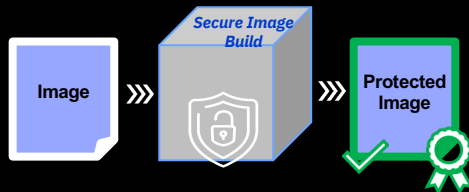


Encrypt & Sign

HSM Integration

Provide images access to industry leading FIPS 140-2 level 4 Hardware Security Module for signing and encryption

- Hosting Appliance
- Virtual Server Base Images
- Secure Image Build Server
- CLI Tool
- Grep 11 Server Container
- Host Monitoring Container
- Logstash (Future)



Where It Matters

A Secure Infrastructure Foundation

IBM Hyper Protect Virtual Servers serves as both a solution for external clients to securely build Docker based applications on IBM Z and LinuxONE and a foundational component of IBM solutions

Exploiting IBM Solutions

Digital Assets Platform

Enabling custodians, exchanges, & ecosystem participants to protect tokenized assets and ensure valid participants for Distributed Ledger Technology transactions

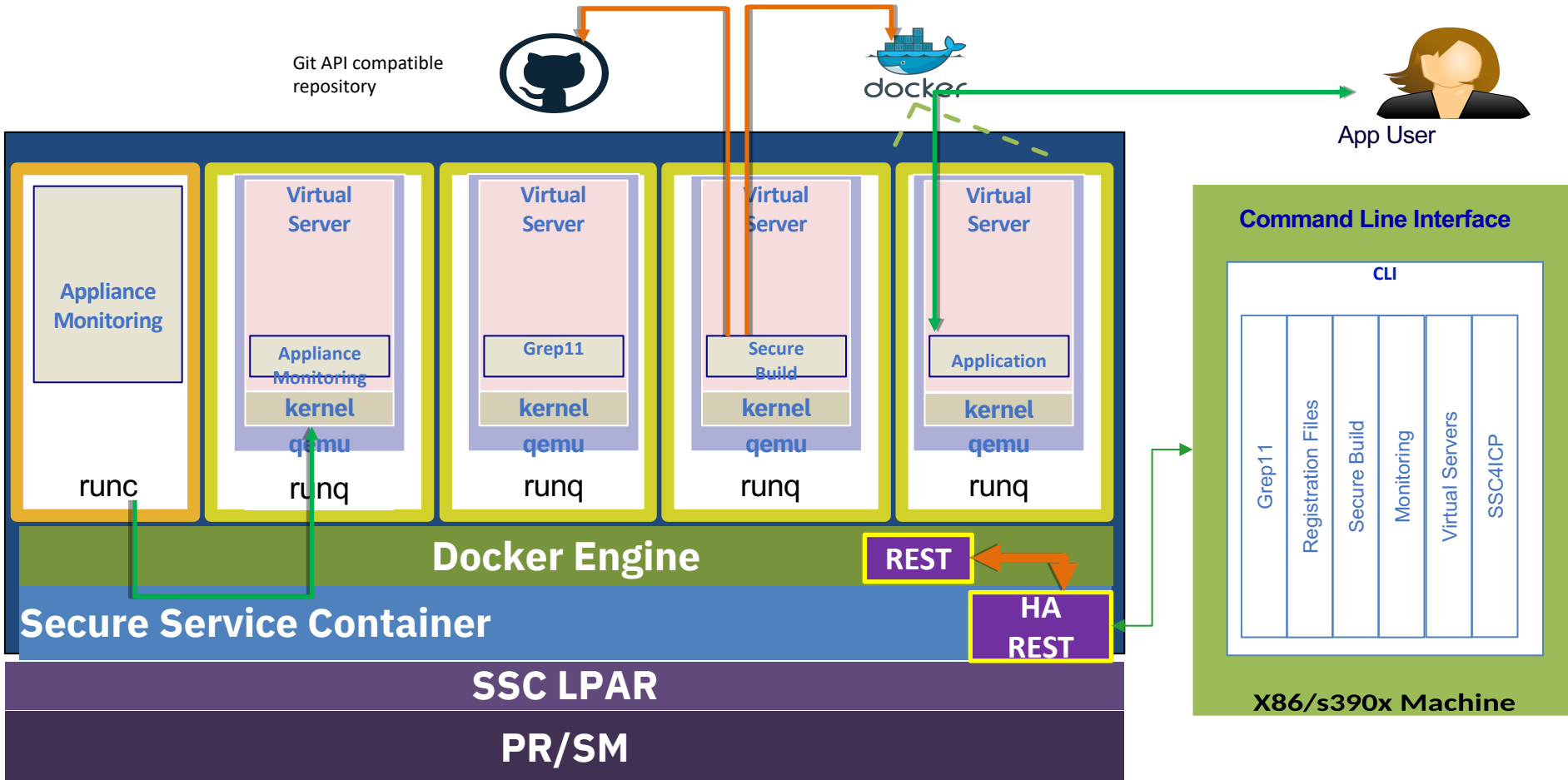
IBM Data Privacy Passports

Provide secure locked-down hosting environment to ensure only desired workload components are deployed



*FUTURE / ROADMAP:
Enable clients to securely build their Platform as a Service, protecting critical containerized workloads from even cloud / k8s administrators*

HPVS Architecture



More Information on runQ repository : <https://github.com/gotoz/runq>

Data Security

Keeping data safe

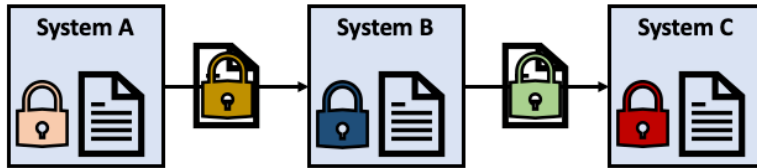


Data Privacy

Appropriate use of data

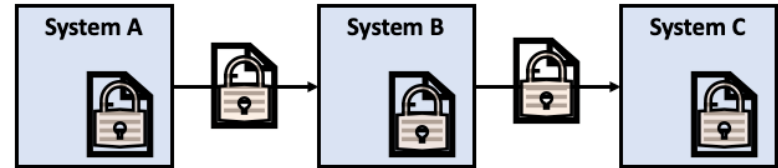


Data Centric Audit and Protection (DCAP)



point-to-point

data is protected via encrypted network sessions. encryption & decryption occurs at each point as data traverses the network. any data stored at endpoints and intermediate points must be explicitly encrypted.



end-to-end

data itself is encrypted at the starting point and remains encrypted until it reaches the end point. data stored at endpoints and intermediate points is implicitly encrypted and managed through centralized policy

e.g. TLS, AT-TLS, IPSec,
MQ AMS, Connect: Direct Secure Plus,
Encryption Facility, SFTP, etc...

Extending LinuxONE Encryption value

Smart, Secure Data Movement
Application transparent protection
for data leaving LinuxONE

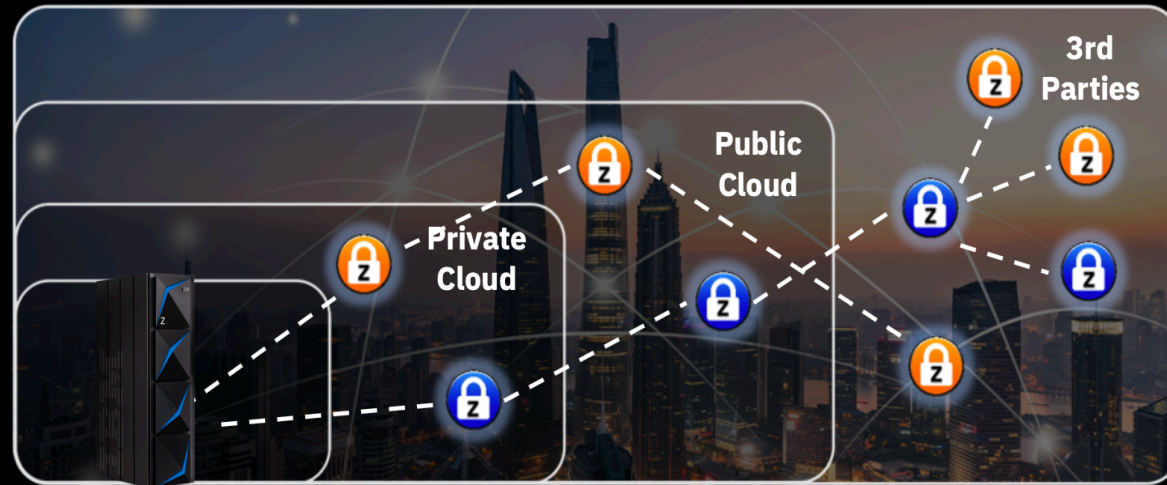
Protect individuals' identity in a digitized world with *Data Privacy Passports*

- **Protection** – Encryption and Revocation
- **Privacy** – Controls and Consent
- **Proof** – Audit and Compliance



*\$40 to start an attack vector,
\$40,000/HR for an attack recovery*

-- Source: Eduard Kovacs, *Security Week*

Desired State



Current State	Data protected within Z
Desired State	Data protected for the life of the data

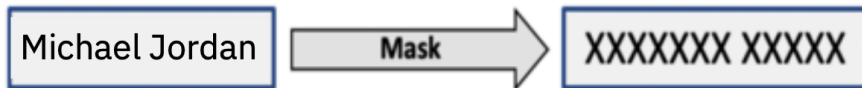
	Desired State: Trusted Data Objects	<i>End-to-end protection via "Trusted Data Objects"</i>
	Desired State: Enforced Data	<i>Controlling the usage of data and auditability of data</i>

IBM Z
with pervasive encryption

Current State: Protected data within Z *Z pervasive encryption*

Protected Data (reversible)

- Data elements are encrypted into
- Trust Data Objects before leaving the platform
- Data can be shown in different views based on the user's need to know



Enforced Data (irreversible)

- Data elements are transformed (masked, encrypted, hash, omitted) at the time of consumption
- Transformations based on a user's need to know
- Can be performed on Protected Data or "on the fly"

What are the flows for enforcement on data

Data can be enforced “on the fly”

- Source data remain in the clear and clients connect to a proxy which will enforce data for them
- No changes needed to the database system where the data originates

Data can be protected then enforced

- Source data is encrypted into Trust Data Objects (TDO) and then inserted into a new table
- Clients connect to the new protected table and based on policy are presented an enforced view of the data
- The new protected table elements are stored encrypted

Where is the protected or enforced data stored

Enforced Data

- Can be stored in a table with the same schema as the source table
- Data can be enforced in a way where it remains compatible with the original source schema
- Easy for application transparent enforcement

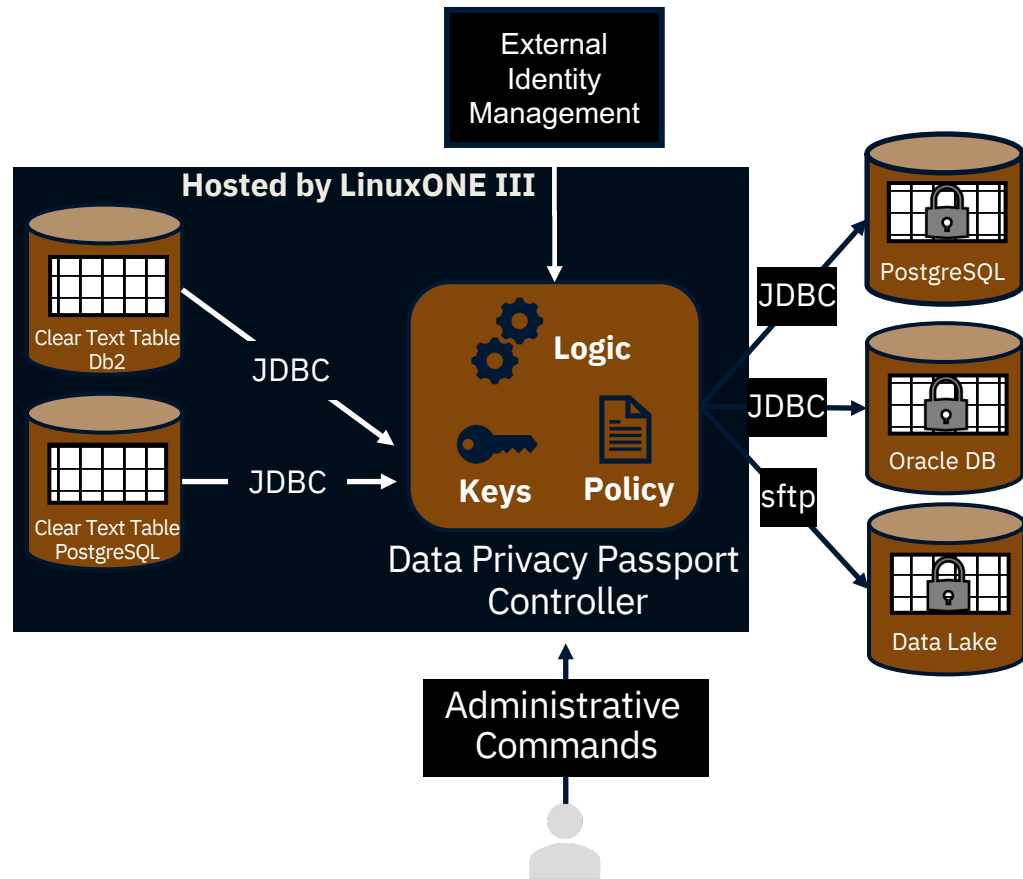
Protected Data

- Data elements can be packaged into Trust Data Objects (TDO)
- The TDOs do not share the same size as the source data, it is an encrypted package with additional metadata
- The target tables needs to be able to store data with a different schema than the source table
- This table can be on any system and does not need to be managed by the same database as the original source table

Introducing IBM Data Privacy Passports

Protected, Private, Provable

- Protected at the point of extraction
Enforced at the point of consumption
- Move data from IBM LinuxONE to distributed as Trusted Data Objects – Start with SQL data sources on IBM LinuxONE
- Passport Controller deployed in an SSC LPAR
- Policy for enforcement can be changed dynamically to revoke or entitle users to data
- **Create a single, protected table, to provide multiple views of data**



Components of Data Privacy Passports

Trust Authority

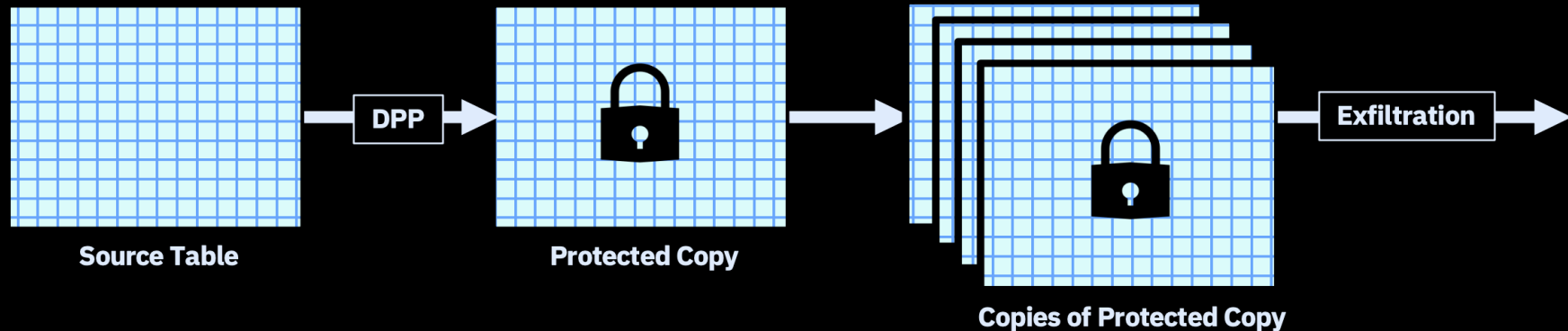
- Central point of control for managing and enforcing data security and privacy. It may be deployed independent from Passport Controller and serves as center of trust for Data Passports solution. Concept of Local, Master and Central Trust Authorities
- Accessed by Data Controllers both on and off IBM LinuxONE

Data Controller

- Data Controller provides an intercept point to transform “raw” data into “trusted data objects” or enforce data protection
- Needs to be deployed on IBM LinuxONE for protection and/or enforcement
- Data Controller only available on IBM LinuxONE for MVP
- **For simplification the MVP will include an embedded Trust Authority in the Controller**

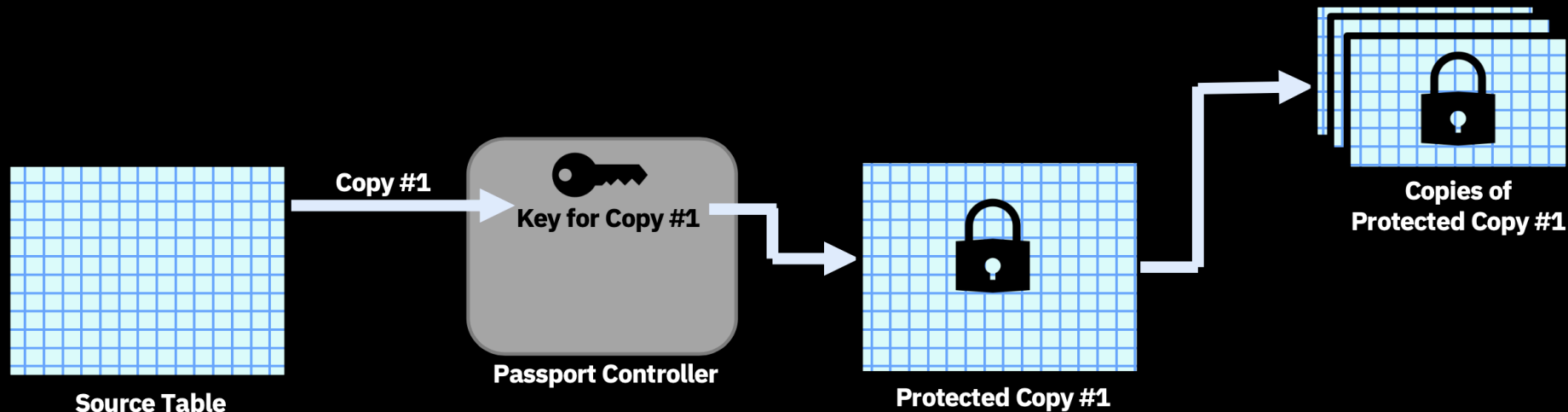
Protecting Copies of Copies of Copies ... of Copies

- Utilize the basic principle of data centric protection
- Protect Personally Identifiable Information (PII) as it leaves IBM Z by policy
- All copies retain protection
- Opening the data requires a return trip to the **Passport Controller**



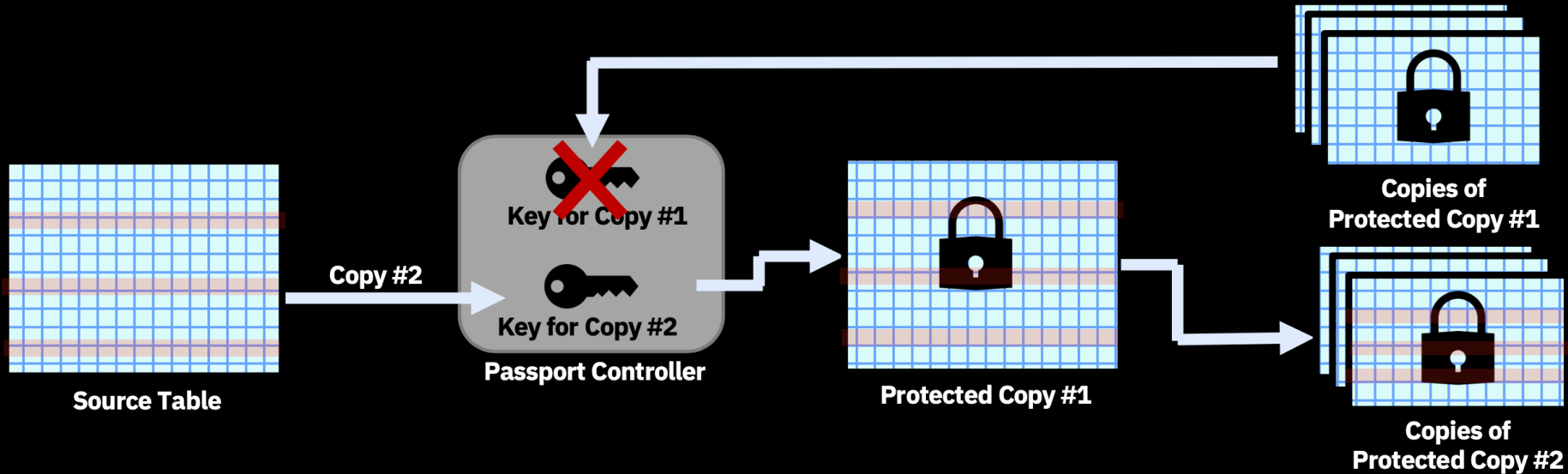
Data Revocation

- Copies of data through the enterprise contain Trusted Data Objects (TDOs)
- These copies circulate throughout the enterprise
- All TDOs are encrypted using a specific key (or set of keys)



Data Revocation (cont)

- SoR gets updated (i.e. to remove some users)
- Old data gets invalidated by deleting the key, new data gets created and copied with modified or removed records
- Old data can provably not be opened ever again



Introducing Boot Integrity for Linux

A complete chain of trust from trusted power-on to a started boot loader

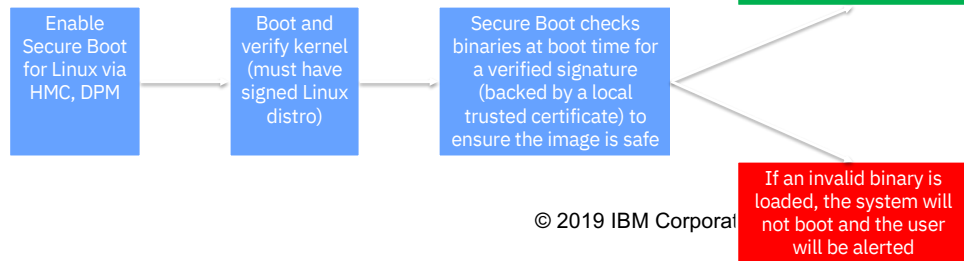
- New with IBM z15 & IBM LinuxONE III, this capability allows you to IPL Linux with Secure Boot
- Secure Boot is designed to protect a system against malicious code being loaded and executed early in the boot process – before any OS has been loaded
- Enable through an option on the HMC or DPM interface
- **Common Criteria Certification** (NIAP OSPP v4.2) for systems booted from SCSI (future boot from all media)
- Initial support for **RHEL 8.1, Ubuntu 19.10**

What security issues does this solve?

Secure Boot protects your system from root level attacks and viruses that target vulnerabilities during the boot process

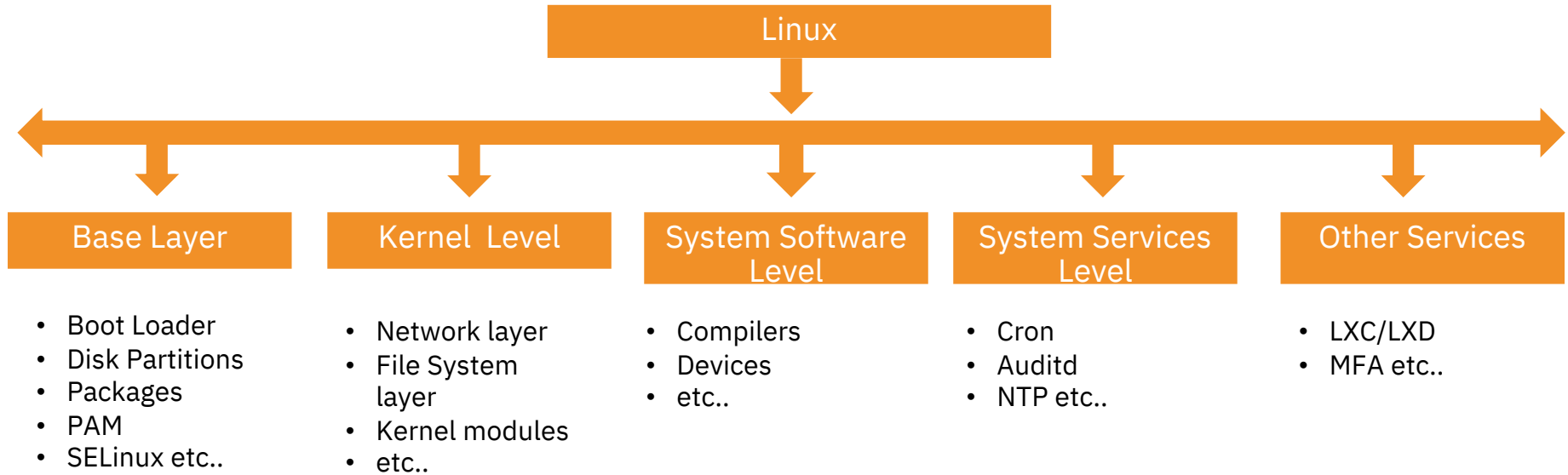
“Bootkit” attacks can mask their presence and give malicious parties elevated administrator access to your environment

Secure Boot validates that Linux images have not been tampered with or replaced by malicious 3rd parties



Linux on Z Security Hardening building blocks

Layers of Security Hardening



Note: The hardening recommendations are covering the recommendations by the distribution together with on the top recommendations.

Building Blocks

Focus Areas	Building Blocks
Access Control	SELinux, AppArmor, sudo, IBM Security Identity manager, PAM (Pluggable Authentication Modules)
MFA (Multi Factor Authentication)	IBM Z Multi Factor Authentication (MFA), Google Authenticator
Directory Services	OpenLDAP, Active Directory
Firewall	iptables, nftables, fail2ban
Intrusion Detection	AIDE, Qradar connector, Snort, Bro, OSSEC, Open DLP (Agent)

Building Blocks

Focus Areas	Building Blocks
Secure Network Communications	OpenSSH, GnuPG (OpenPGP Compliant), IPSec
Secure Socket Layer	TLS, OpenSSL, PKCS#11
Hardening (Locking down)	IBM Secure Service Container, Hyper Protect Virtual Server
Secure Data at rest	dm-crypt, IBM Security Guardium
Compliance checks	OpenSCAP, CIS Benchmarks, BigFix Compliance
Docker (Container based deployments)	Image Security, Container Security (seccomp),

Compliance tools and aspects

Data Privacy is no longer optional with strict Regulatory requirements

- Organizations facing unprecedented data privacy fines from GDPR and FTC



January 2019 – July 2019

Unlike on-site systems, which have a hierarchical structure and a peripheral network that scrubs and analyses data being transmitted, AWS makes it possible for every instance to communicate with the internet in the event of a misconfiguration or insufficient security settings. The exposed applications structure requires companies to strengthen existing security controls. This includes continuously updating security configurations with sufficient and dynamic patching, strong firewall configurations, proper network security implementations and – most importantly – monitoring of the AWS security settings.

Unfortunately, despite providers like AWS providing ample information about the best practices for cloud security, the volume of AWS-related data leaks continues to grow. The main culprit? Human error on the customer's end. In fact, Gartner predicts that, by 2020, 95% of cloud security incidents will be the customer's fault.

What is causing these data breaches?

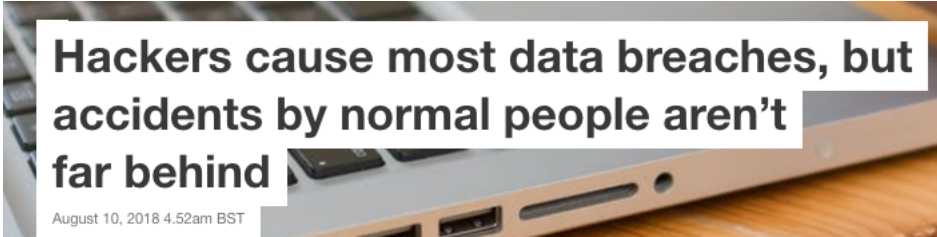
Three main reasons were cited for data breaches in the last quarter: malicious or criminal attacks (59%), human error (36%), and system fault (5%).

Breach Incidents on Record Pace for 2019



by Ericka Chickowski on May 9, 2019

Poorly configured cloud resources and plentiful credential leaks are vaulting 2019 toward the record books when it comes to the volume of publicly reported breach incidents. A [new report](#) out this week by Risk Based Security on data compromise incidents during Q1 2019 shows that these events are happening more frequently than ever before.



Hackers cause most data breaches, but accidents by normal people aren't far behind

August 10, 2018 4.52am BST

PCI-DSS Compensating Controls

PCI DSS Requirement (Subset)	Recommendation on Linux On Z
Use PCI Scan policy for Internal Vulnerability scans on the workloads (Webapps)	OWASP ZAP can be used to scan the workloads. Additional recommendation is to use Nessus Scanner.
File Integrity monitoring	AIDE (Advanced Intrusion Detection Environment), IBM Data Guardium
Firewall rule and network segmentation (Linux level)	iptables, nftables
Automatic logout of idle sessions after 15 mins	TMOU setting in the bashrc. MFA time outs.
Remove (or) disable inactive accounts automatically	Customizable via userdel settings
Security events monitoring	Qradar Connector for monitoring System logs
Secure Configuration Validation	Automated configuration check using OpenSCAP

OpenSCAP

- The OpenSCAP ecosystem provides multiple tools to assist administrators and auditors with assessment, measurement, and enforcement of security baselines for the operating environment
- Built and Maintained by RedHat. SUSE has its own integration with OpenSCAP via SUSE Manager
- NIST Certified and contains multiple regulatory and compliance policies
- Link: <https://www.open-scap.org/>

OpenSCAP Demo on Linux on Z

Summary

- In this session we covered,
- Built in Security capabilities LinuxONE / Linux on Z provides
- How regulatory requirements can be mapped to the Security and Compliance capabilities offered by Linux on Z and Open Source Ecosystem around it (*)
- Certain tooling around regulatory requirements analysis and enforcement

*We have customers & ISV's validating the capabilities mentioned above as a part of Hardening their Linux on Z environment

Additional References

- Docker IBM Z Security : https://www.ibm.com/support/knowledgecenter/en/linuxonibm/com.ibm.linux.z.ldvd/ldvd_r_security.html
- RHEL 8 Security Hardening Guide: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/pdf/security_hardening/Red_Hat_Enterprise_Linux-8-Security_hardening-en-US.pdf
- IBM Security Guardium: <https://www.ibm.com/uk-en/security/data-security/guardium>
- OpenSCAP: <https://www.open-scap.org/getting-started/>
- Securing Your Cloud: IBM Security for LinuxONE redbook <https://www.redbooks.ibm.com/abstracts/sg248447.html>



Pradeep Parameshwaran

*Technical Security Lead
Linux on Z & LinuxOne*

*Schoenaicher Strasse 220
D-71032 Boeblingen
Mail: Postfach 1380
D-71003 Boeblingen*

*Phone +497031161171
Mobile +49 15146505935
PRADEEP@de.ibm.com
www.ibm.com*