# The Value of LinuxONE Virtualization Security

Brian W. Hugenbruch, CISSP
LinuxONE Cyber Resiliency Lead
bwhugen@us.ibm.com

Pradeep Parameshwaran
LinuxONE Security Lead
Pradeep@de.ibm.com

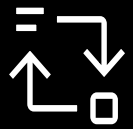
# Delivering end to end security

EXISTING PROTECTIONS

INCREASING FOCUS

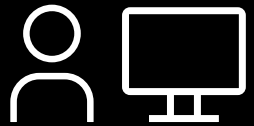
## Data at rest

Inactive data that is not currently being accessed or transferred



## Data in transit

Travelling between public or private networks



## Data in use

Actively being accessed by an application or a user and stored in memory

CONFIDENTIAL COMPUTING

IBM


the **always on** culture means customers expect 24x365 service (or as close as possible)

**9 Billion**

records

only **4%**

**45%** more security incidents due to **unauthorized access**

average cost of **downtime** is an estimated **$1-5M/hour**

# Cyber threat and regulatory landscape point to the importance of data centric security and zero trust architectures

Data privacy and security is key to regulated cloud

| Public | Internal | Confidential | Sensitive |
|---|---|---|---|
| • Press releases,<br>• Published annual reports<br>• Social media feeds,<br>• Information on public record<br>• Product/Pricing catalog | • Internal emails<br>• Project documents<br>• Training materials<br>• Organizational charts policy guides | • Employee pay stubs<br>• Customer information<br>• Personal contact information<br>• Customer preferences<br>• Credit card<br>• Non-public contracts<br>• NDA agreements offering roadmaps | • Government identification numbers<br>• SSN<br>• Driver's license<br>• Financial transactions<br>• Digital Assets<br>• Information that could pose an identity threat |

Operational Assurance

Technical Assurance

Confidential and sensitive data requires technical assurance that only customer has access to the data, and cloud provider can not.

Basic tenets of zero trust architecture*:

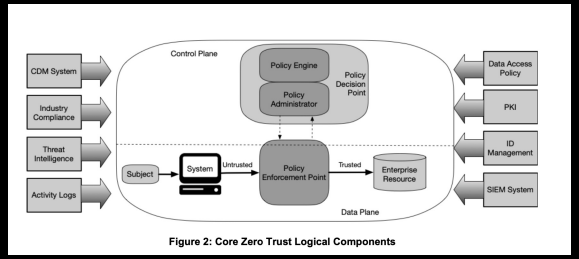



Figure 2: Core Zero Trust Logical Components

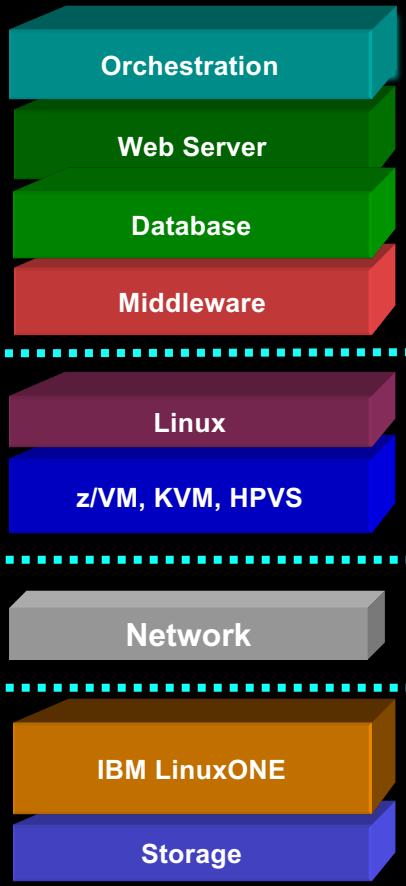
1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

* NIST publication on Zero Trust Architecture – https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

# IBM LinuxONE™ Security Capabilities

| | |
|---|---|
| Integrated Hardware Crypto Accelerators | CPACF – Crypto accelerator on every core for high-speed, bulk symmetric encryption<br>NEW Crypto Express7S – PCIe Hardware Security Module (HSM) & Cryptographic Coprocessor |
| EAL 5+ Isolation and Virtualization | Workload isolation with design for highest EAL5+ security certification<br>Full sharing/partitioning of the installed resources with the highest levels of efficiency and utilization |
| Secure Service Container hosting appliance | Secure deployment of software appliances including tamper protection during installation and runtime, restricted administrator access, and encryption of data and code in-flight and at-rest |
| NEW Hyper Protect Data Controller | Broadly protect Linux file systems across multiple hybrid data environments using fully encrypted trusted data objects with policy control and access revocation |
| NEW Secure Execution for Linux | Protect your system against root level attacks and vulnerabilities from a malicious admin at the hypervisor level |

# Security Features: LinuxONE




**Software, Workload, Automation and Orchestration**

**Operating Systems**

**Virtualization Layer**

**Networking**

**Physical Compute and Storage**

HyperProtect Crypto Services

Qradar, IBM zSecure, MFA, HyperProtect Data Controller

SELinux, chmod, qemu, AV, application scanning

z/VM: Privclasses, RACF, device isolation, EAL 4+

sVirt, Secure Execution, SSC Boot Integrity

TLS, Virtual LAN enforcement

Integrity Checking, Crypto Express, Fibre Channel Endpoint Security

Storage Encryption, Fibre Channel Endpoint Security

# Let's start with the hardware.


EAL5 – better than an air gap when it comes to data confidentiality and compute management

- Isolation of a logical partition at the architectural level (more on this in a moment)
- Controls on direct access to devices
- **Elimination** of covert channels
- Role-based access controls to a partition (or partitions), or hardware

With a few added bonuses:

- Controlled in-memory communication paths (**HiperSockets**)

# Let's start with the hardware.

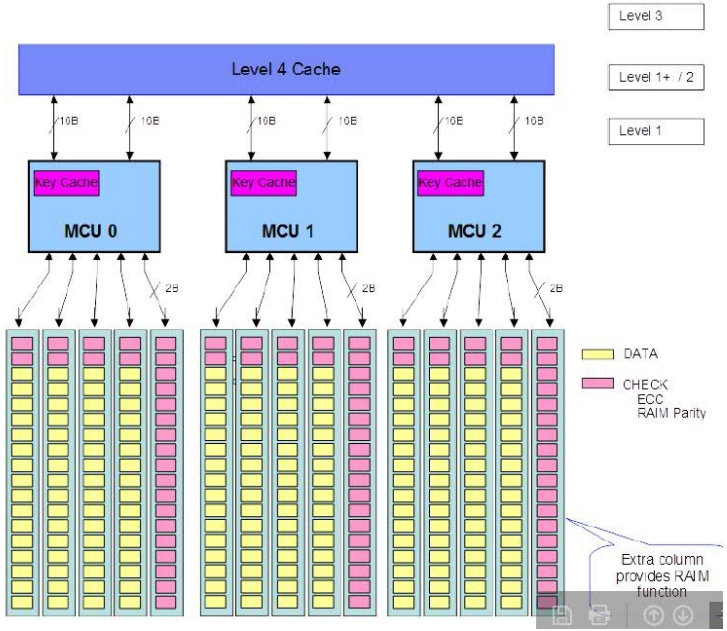
IBM LinuxONE

Data Protection

Built-in redundancy protects data against attacks on hardware

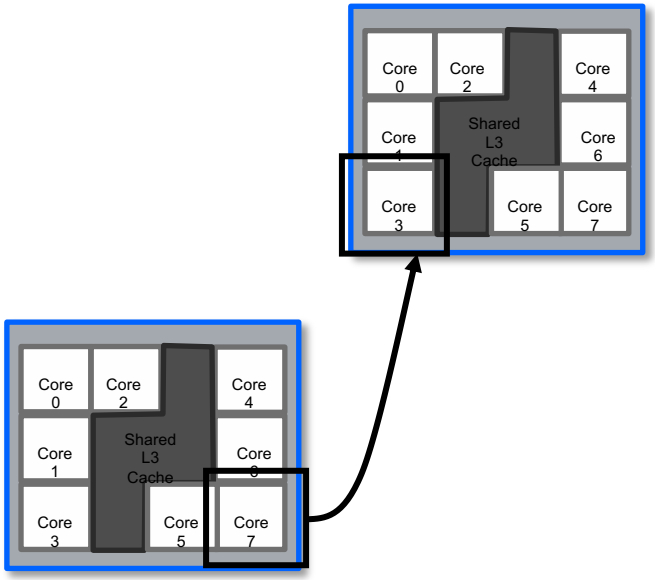
- ECC
- RAIM
- Defense against rowhammer etc.

Cache separation and virtualization tech prevents side-channel attacks



# If a core fails, a spare is “turned on” without system or program interruption


- Each LinuxONE server has two cores designated as spare
- Core failover (called sparing) is transparent to applications
- Spares need not be local to the same node or drawer
- Any core (general processing core or I/O core) can failover to spare



# Cryptographic acceleration with LinuxONE III hardware

## Cryptographic acceleration with Crypto Express7S:

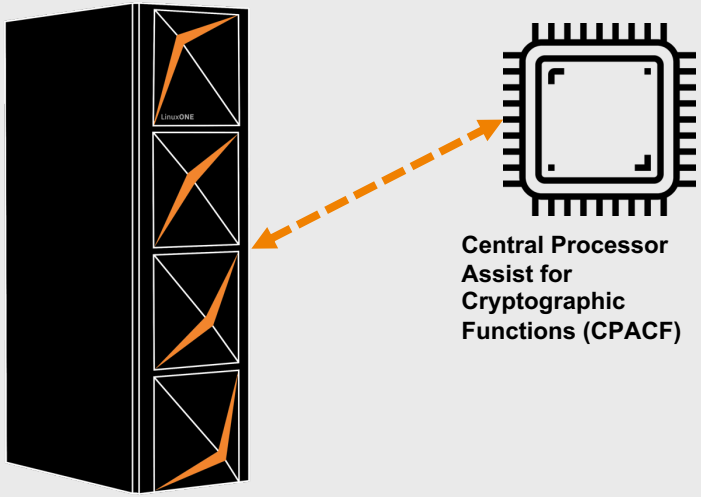
- Improved SSL/TLS handshake performance on LinuxONE III with Crypto Express7S compared to Crypto Express6S
- Updates to Common Cryptographic Architecture (CCA) for security modules that enhance remote ATM key loading, offer new protections for banking payments, and extended compliance support to stay 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

## Designed for EAL5+

# 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

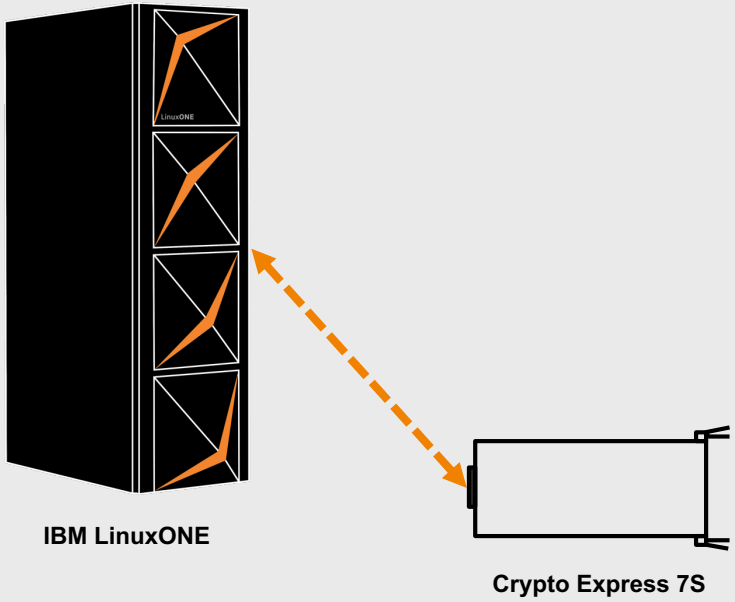
Suited for high speed bulk symmetric encryption

## 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

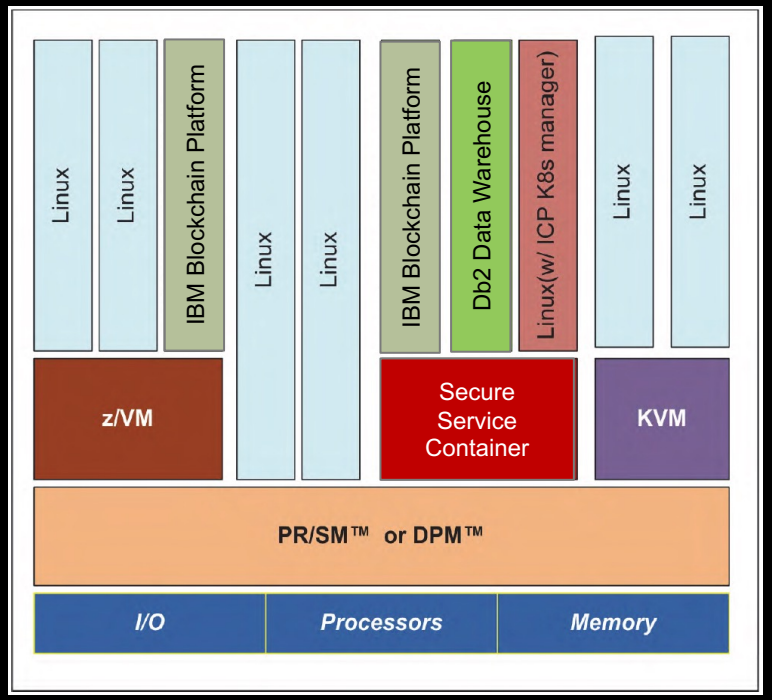
Level 3: Tamper-responding features designed to notify of unauthorized access

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

# Why Use LinuxONE Hardware Cryptography?


- Maximize Trust & reliability – proven hardware implementations
- Minimize Cost (security does not come for free)
  - Save money:  offload expensive CPU workload
  - Save time: Faster crypto algorithms
- Industry-leading security
  - special built-in functions for banking and financial applications (secure key)
- Regulatory compliance starts at hardware (FIPS 140-2)

# Hypervisors and Virtualization for IBM LinuxONE




Virtualization is **built into the DNA of IBM LinuxONE**

**PR/SM LPAR**

**IBM DPM**

- **Workload isolation** with design for highest EAL5+ security certification
- PR/SM™ **manages and virtualizes all** the installed and enabled system resources as a single large SMP system
- IBM Dynamic Partition Manager **simplifies provisioning and management experience**
- **Full sharing/partitioning of the installed resources** with the highest levels of efficiency and utilization
- **Scale up or scale out on demand** with support for up to 85 partitions

---

**z/VM v7.2**

- **Enables extreme scalability, security and efficiency –** Support for 2TB of memory, Dynamic Memory Downgrade, 80 logical processors, and improved z/VM paging enabling workload consolidation, growth in memory-intensive applications, and superior levels of elasticity
- **LinuxONE III Support** – Crypto Express7S, crypto enhancements, On-chip compression enabled for guest exploitation; Also supported by z/VM 7.1.

---

**Linux KVM**

- Support for **RHEL, SLES, and Ubuntu** KVM
- Pass-through of Crypto Express adapter domains in KVM guests
- Secure and protected business data with exploitation of elliptic-curve crypto (ECC)
- **Familiar standard Linux user interfaces** for open source developers, offering a low barrier to adoption and easy integration with hybrid environments

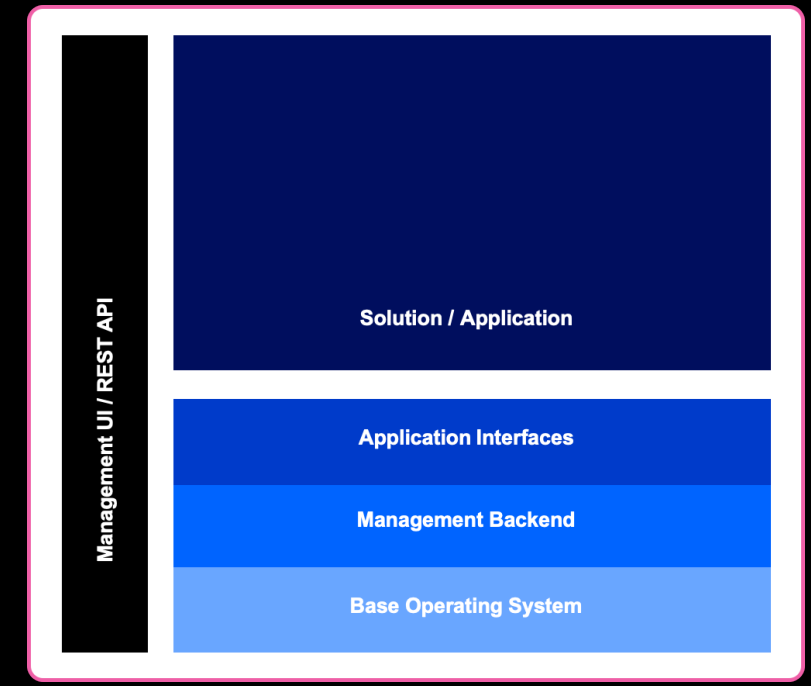
# Virtualization security requires some basics:

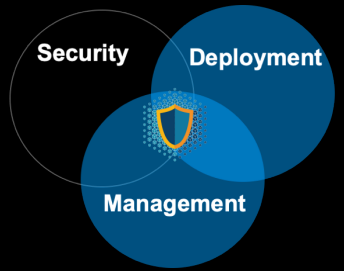
Virtualization

- Isolation of hosted guests
  - Confidentiality of data on the system
  - Protection of privileged hypervisor commands and operations
  - **Controlled** sharing of data between virtual machines
- Management of virtual devices and integrity of data
- Securing connectivity to and within the hypervisor layer
  - TCP/IP connectivity
  - Virtual networking
- Hardening of the hypervisor layer
- Multi-tenancy and “security zones”
- Auditing of security-relevant operations

# 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



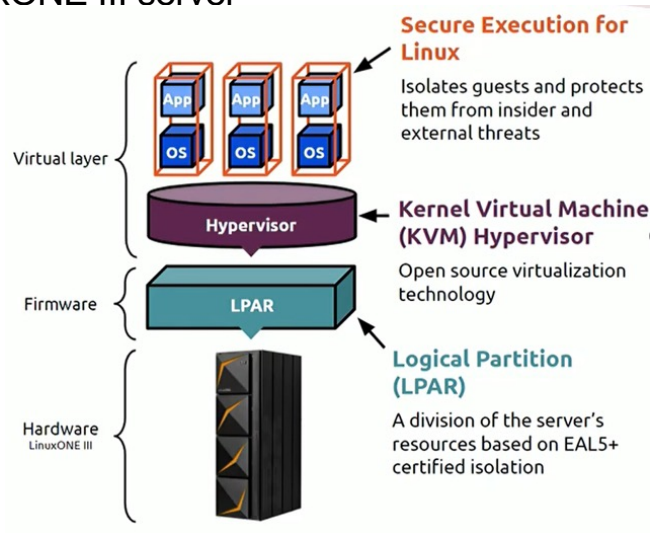




# Secure Execution for Linux

*New for LinuxONE III*

## What is it:

Trusted Execution Environment built into the LinuxONE III server




**Protects data-in-motion in the memory of the KVM Hypervisor**



## What does it do

Provides scalable isolation for individual workloads to help protect them from not only external attacks, but also insider threats

## How is it better

- Current approaches only address data at rest and data in transit, Secure Execution Linux secures data in use.
- Trusted Execution Environment (TEE) allows for Hardware enabled protections to realize a Zero Trust environment with workload isolation and hardened access restrictions of data.

# Hardened access restrictions

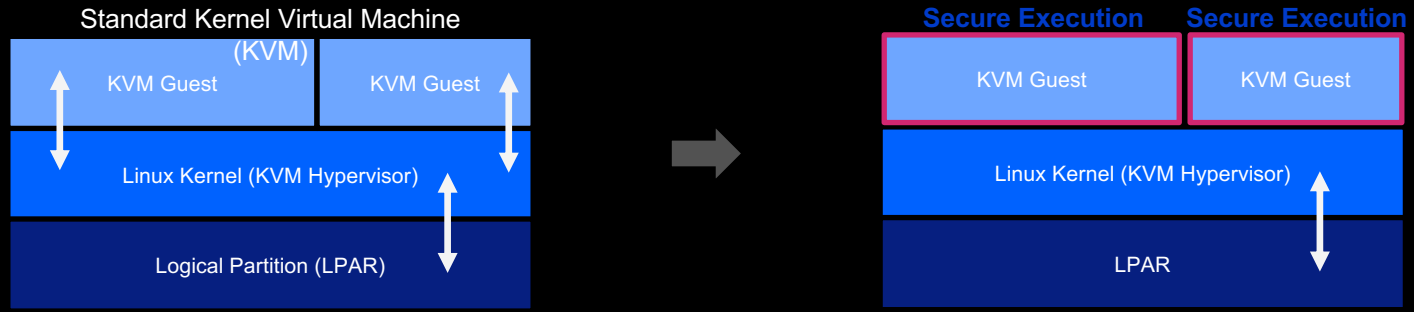
## Ex. Simplest implementation through KVM

**Today's Challenges**

- No isolation between host and guests in multi-tenant deployments
- Hypervisor administrator have visibility of data and state of running guests
- Vulnerable to misuse by malicious insiders or hacked/stolen admin credentials

**With Secure Execution**

- KVM guests are fully isolated and protected from hypervisor
- Hypervisor admins can still manage and deploy workloads, but are unable to access hosted data
- Fully isolated environments for multi-tenant workloads running on shared LPAR



# IBM Hyper Protect Virtual Servers –
*Built on Secure Service Containers*

*Securely hosts Docker and Kubernetes based solutions*

*Enable organizations to manage Hybrid Cloud IT infrastructure without visibility to end user applications and customer data*

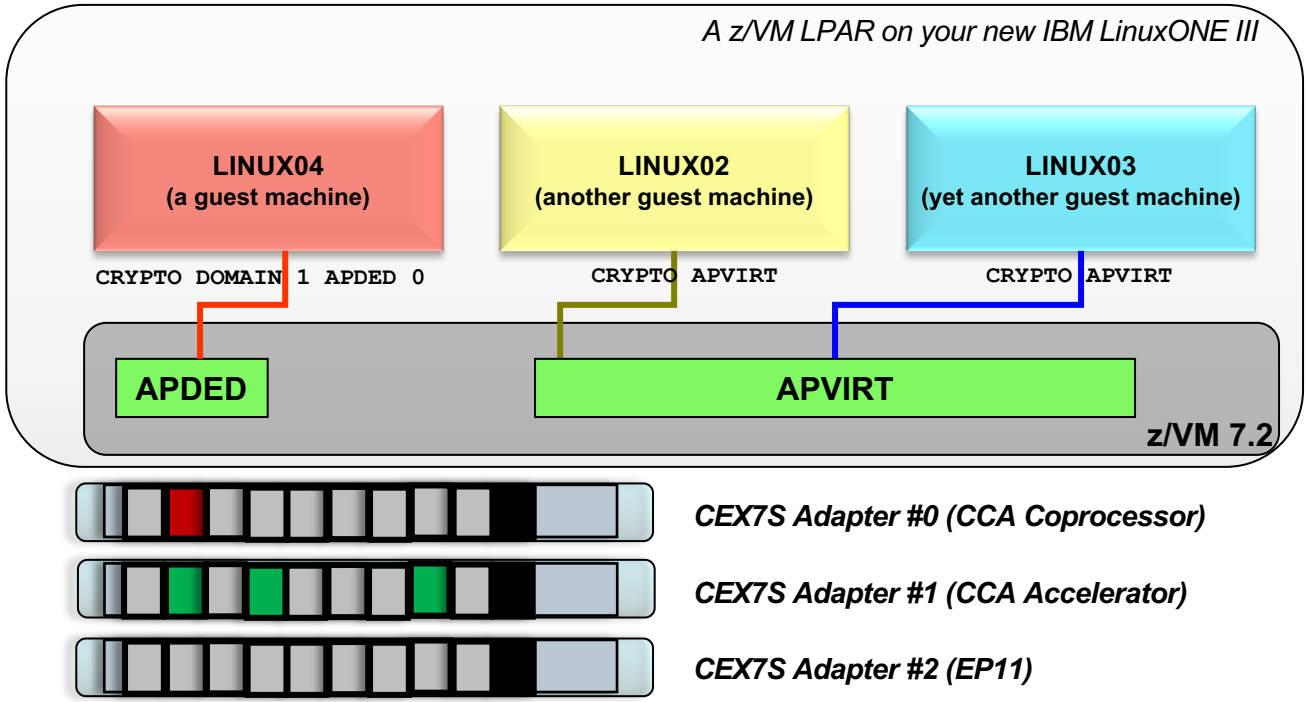
Protects data and applications against misuse of privileged Infrastructure Admin credentials – by internal or external threats

Simplifies solution deployment via Secure Service Container foundation – Reduces end user management of low level execution environment

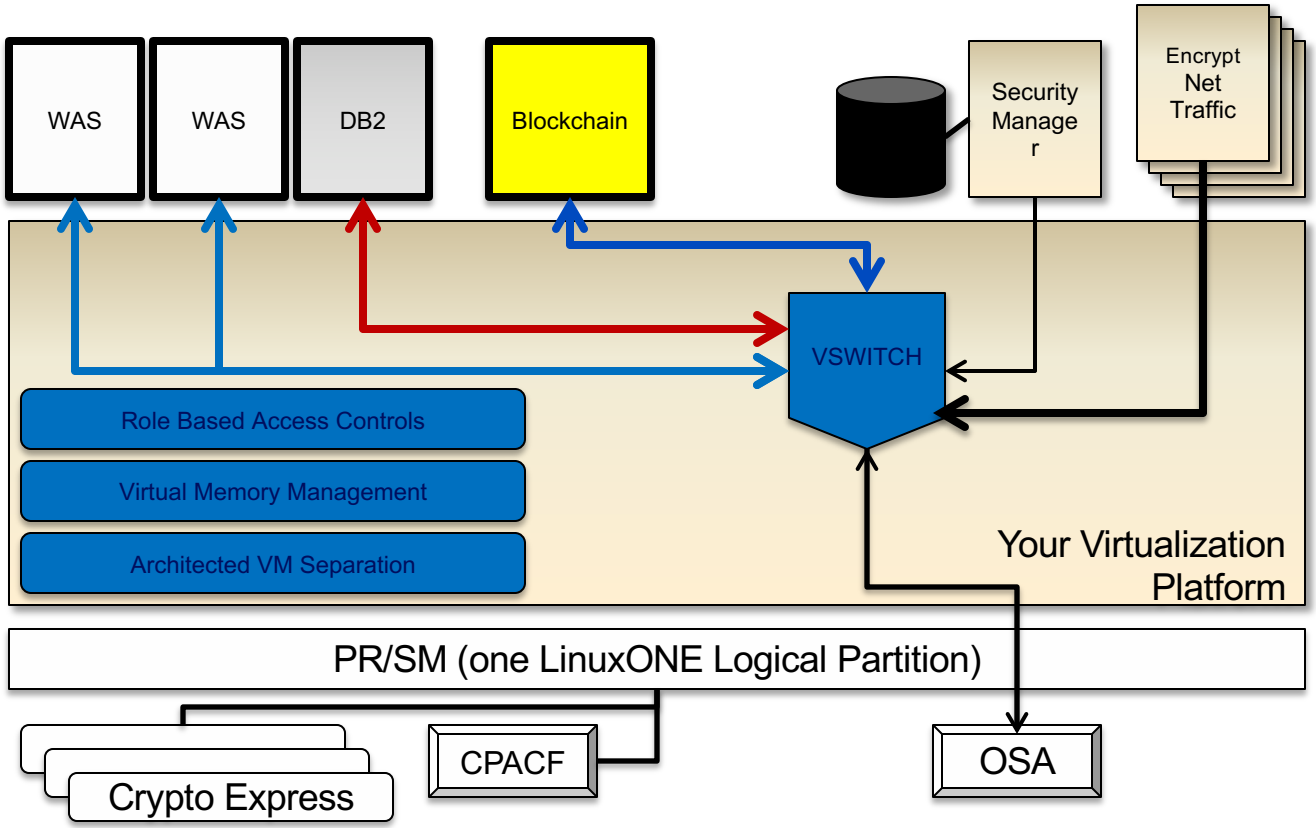
Supports the cloud platform, management tooling, and containerized application ecosystem

# Virtualized Crypto Express devices for z/VM virtual machines

*(similar capability exists for KVM environments)*

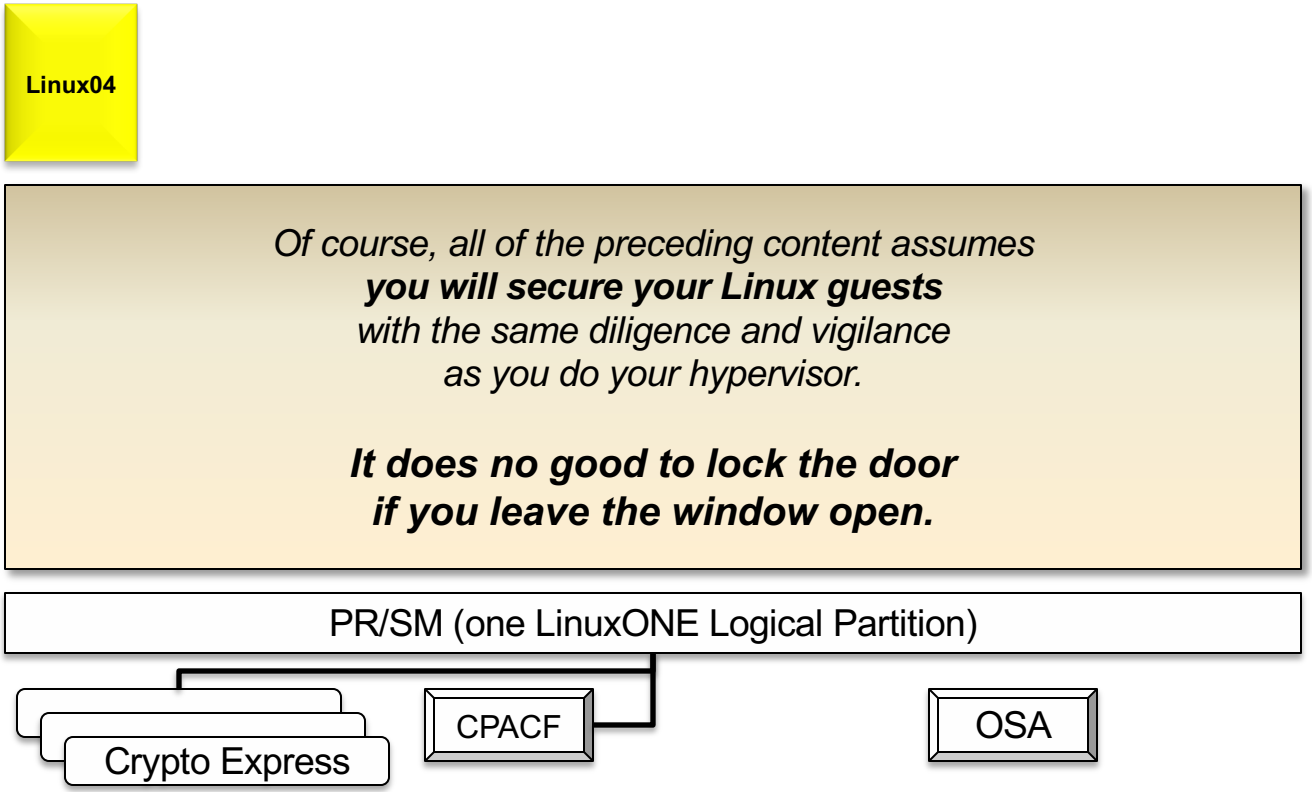


# This is your LinuxONE System On Lockdown.



# Linux Guest Security





# Linux on LinuxONE is More Secure


Linux is Linux
- Linux security features and tools available to all architectures
- Differences only in
  - architecture specifics
  - device support

Thorough open source review of key components
- Security is and was always a focus of kernel development
- Core Infrastructure Initiative (a.o. sponsored by IBM) focuses on supporting security relevant packages (like openSSL)
- IBM involvement with open-source communities (platform, distros, products)

Benefits stem from the platform
- Strong guest isolation
- Cryptographic hardware support

# Linux is More Secure on LinuxONE


Linux is Linux
- Linux security features and tools available to all architectures
- Differences only in
  - architecture specifics
  - device support

Thorough open source review of key components
- Security is and was always a focus of kernel development
- Core Infrastructure Initiative (a.o. sponsored by IBM) focuses on supporting security relevant packages (like openSSL)
- IBM involvement with open-source communities (platform, distros, products)

Benefits stem from the platform
- Strong guest isolation
- Cryptographic hardware support

# Introducing IBM Secure Boot for Linux

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

- New with 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** (future support for SLES 15 SP2)

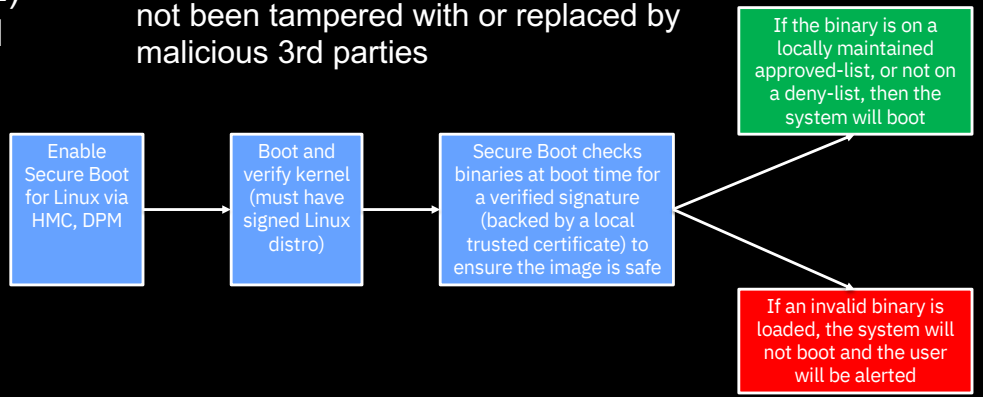
***Only on IBM LinuxONE III***

### 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



# LinuxONE and Open Source Security

*(the starter list)*

Linux

**SELinux** for access control (see also: **AppArmor**)

- A foundational component of Linux security (that's why KVM has sVirt)
- Used to define policies for security within a Linux guest

**sudo** and **cgroups** for resource control — **<< you didn't give out root, right?**

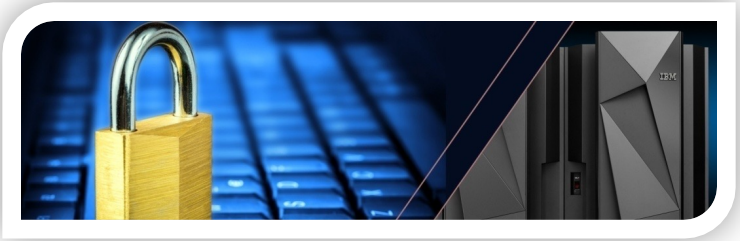
**openLDAP** for open identity management — **<< or find a SAML solution**

**openSSL** and **openSSH** for secure communication — **<< don't forget httpd.conf**

**IPtables / NetFilter** for firewalls — **<< if you run them inside these boxes …**

**dm-crypt / LUKS, eCryptFS** for file-system encryption — **<< we'll cover this soon …**

**Lynis, Tiger,** or **openSCAP** for system hardening — **<< measure your guest vs baselines**



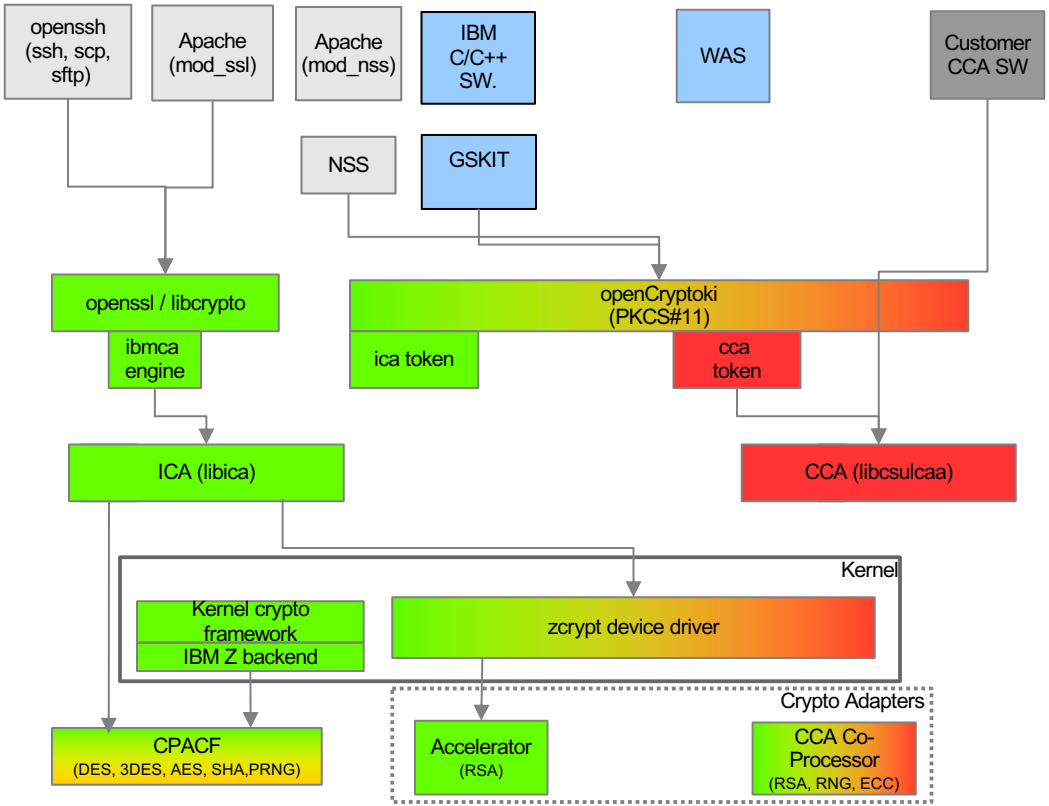
# Bringing Pervasive Encryption to LinuxONE

*Bringing Pervasive Encryption to Linux on Z involves …*

Pushing crypto modifications upstream

Extending crypto usage both for data-in-flight and data-at-rest

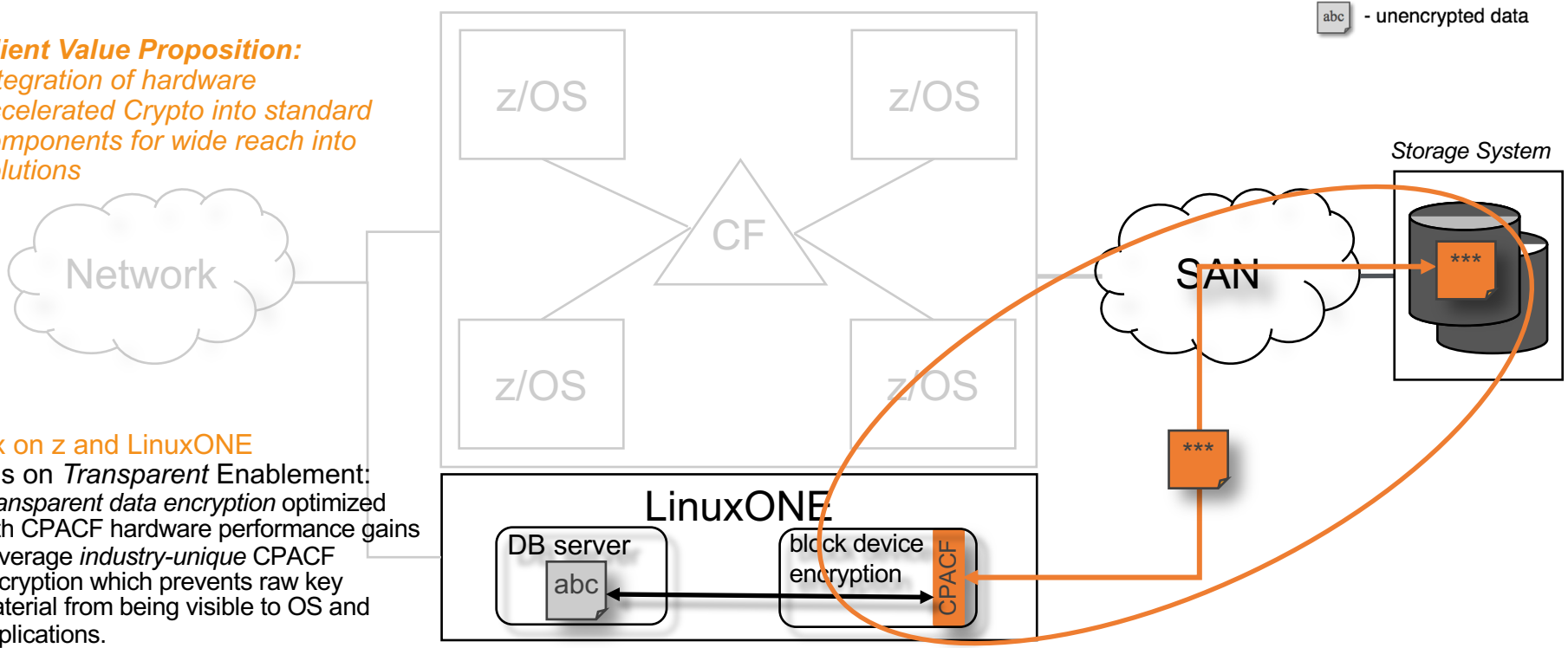
Key usage and cryptographic access should be as transparent to the administrator as possible


openssh
(ssh, scp,
sftp)
Apache
(mod_ssl)
Apache
(mod_nss)
IBM
C/C++
SW.
WAS
Customer
CCA SW
NSS
GSKIT
openssl / libcrypto
ibmca
engine
openCryptoki
(PKCS#11)
ica token
cca
token
ICA (libica)
CCA (libcsulcaa)
Kernel
Kernel crypto
framework
IBM Z backend
zcrypt device driver
Crypto Adapters
CPACF
(DES, 3DES, AES, SHA,PRNG)
Accelerator
(RSA)
CCA Co-
Processor
(RSA, RNG, ECC)

# Data Protection // LinuxONE File System Encryption

*Protection of data at-rest*

***Client Value Proposition:***
*Integration of hardware accelerated Crypto into standard components for wide reach into solutions*




Linux on z and LinuxONE

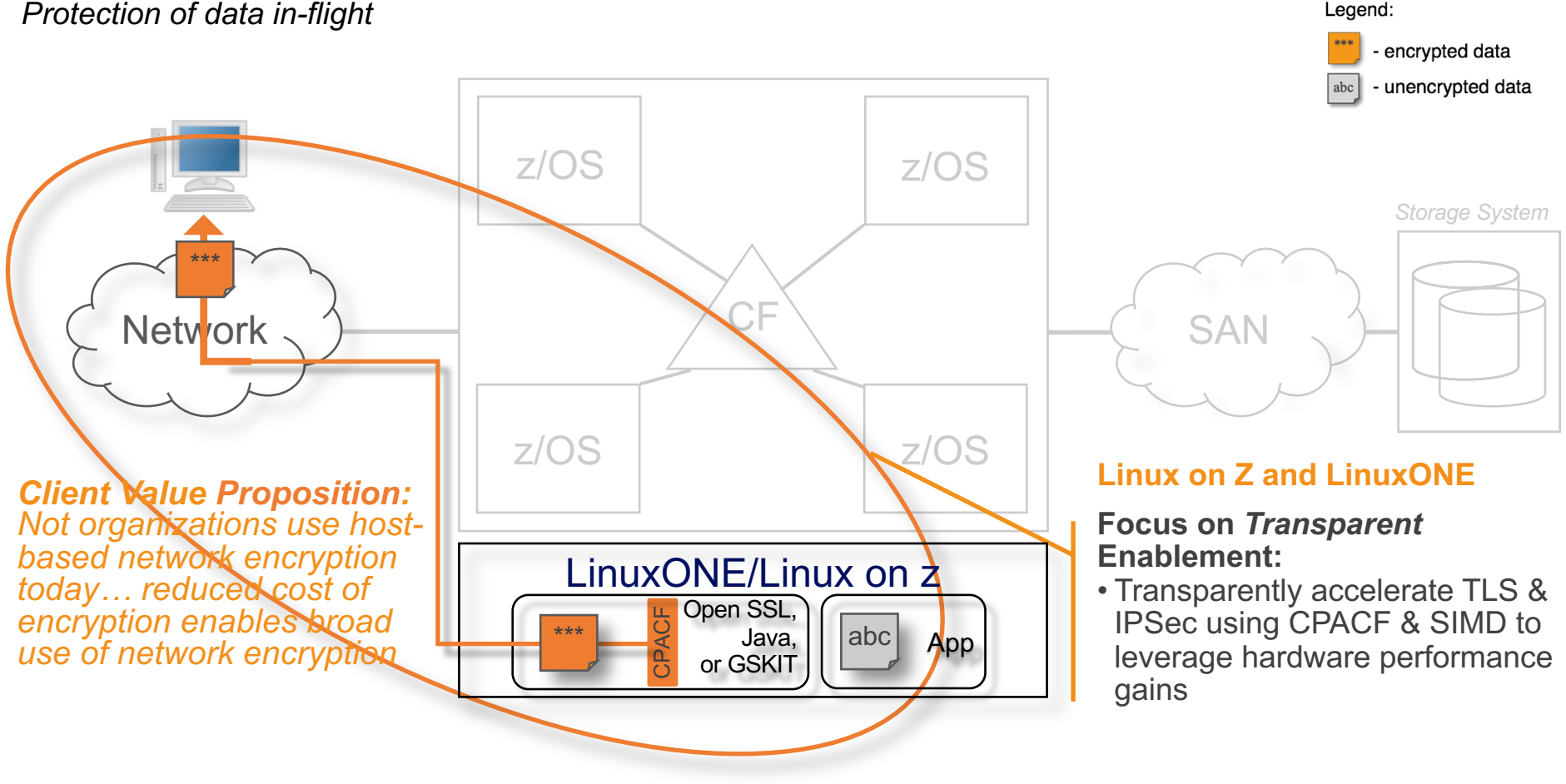
Focus on *Transparent* Enablement:

- *Transparent data encryption* optimized with CPACF hardware performance gains
- Leverage *industry-unique* CPACF encryption which prevents raw key material from being visible to OS and applications.

# Data Protection // LinuxONE Network Security

*Protection of data in-flight*

Submitted Upstream




***Client Value Proposition:***
*Not organizations use host-based network encryption today… reduced cost of encryption enables broad use of network encryption*

## Linux on Z and LinuxONE

**Focus on *Transparent* Enablement:**

- Transparently accelerate TLS & IPSec using CPACF & SIMD to leverage hardware performance gains

# Leveraging the platform to Centralize Security Function

Take advantage of the proximity of LinuxONE systems to other LinuxONE or IBM Z machines to streamline certain functionality, such as …

- **Centralized Identity, Authentication, and Audit**
  - ITDS (LDAP Server) for z/VM or z/OS, using DB2, BFS, or RACF as a back-end
  - PAM plug-ins for Linux machines (regardless of architecture)
  - Additional plug-ins to auditd for centralized audit – pushes events out to SMF records
- **Password Synchronization**
  - Using ITDI (IBM Tivoli Directory Integrator), LDAP, and RACFVM
- **PKI Services** (z/OS PKI Services, connected to Linux guests)

# IBM Z Multi-factor Authentication

Support for identity management across multiple LinuxONE systems

Logon factors such as RADIUS, Yubikey, RSA SecurID, TOTP, ldap-bind into existing directory solutions

LinuxONE support runs as a LinuxONE hypervisor guest or in its own partition

**V2.1:** Supports logon to z/VM and HMC today

**V2.2:** Support for Linux guests, KVM, and Linux-hosted applications through PAM updates

# Managing Your Secure Virtualization Platform

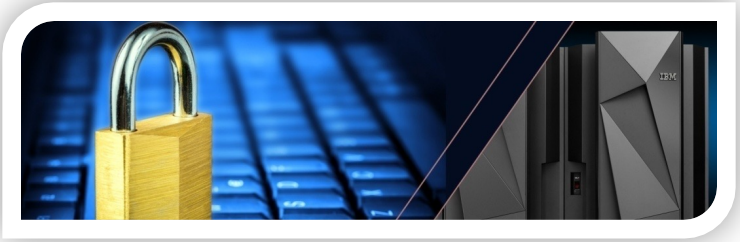
Controlling your virtual infrastructure (and its security) will eventually necessitate automation and tooling.

z/VM Supports:

- **IBM Cloud Infrastructure Center (ICIC):** for IaaS workload management
- **Operations Manager for z/VM**: for automation of management and alert-based actions.
- **IBM Security zSecure for RACFVM:** policy management and auditing

KVM Supports:

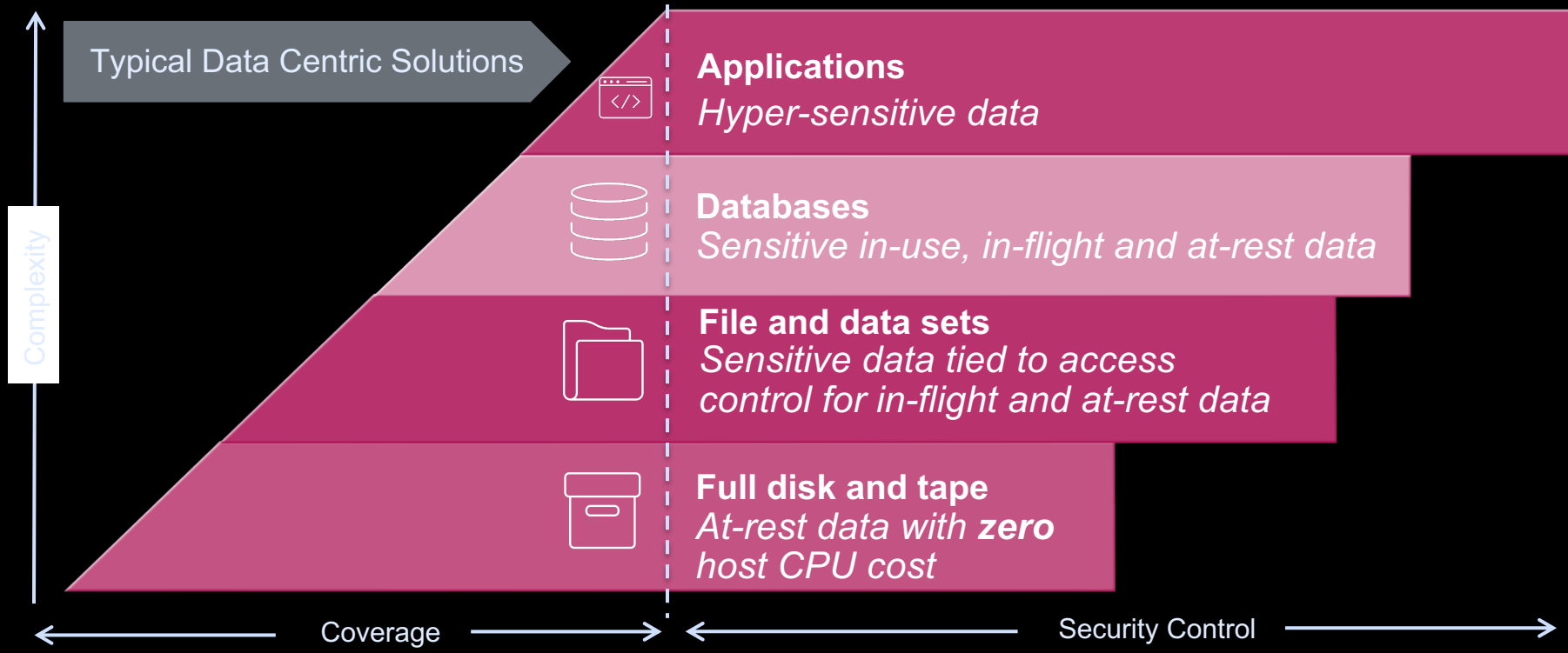
- **IBM Cloud Infrastructure Center (ICIC):** for IaaS workload management
- **virt-manager**: the VMM graphical interface
- Native **OpenStack** support through libvirtd




OPEN
MAINFRAME
PROJECT
IBM
suse
ca
technologies
THE
LINUX
FOUNDATION
MARIST
University of
Bedfordshire
Compuware
North Carolina
Agricultural and Technical
State University
L3C
VICOM Infinity
RSM
PARTNERS
bmc
ADP

# Achieving Data Centric Protection with Hyper Protect Data Controller

- Typical application level protection is extremely costly and only protects a small number of fields
- Can you have security control with broader coverage and less complexity?



# Zero Trust level characteristics

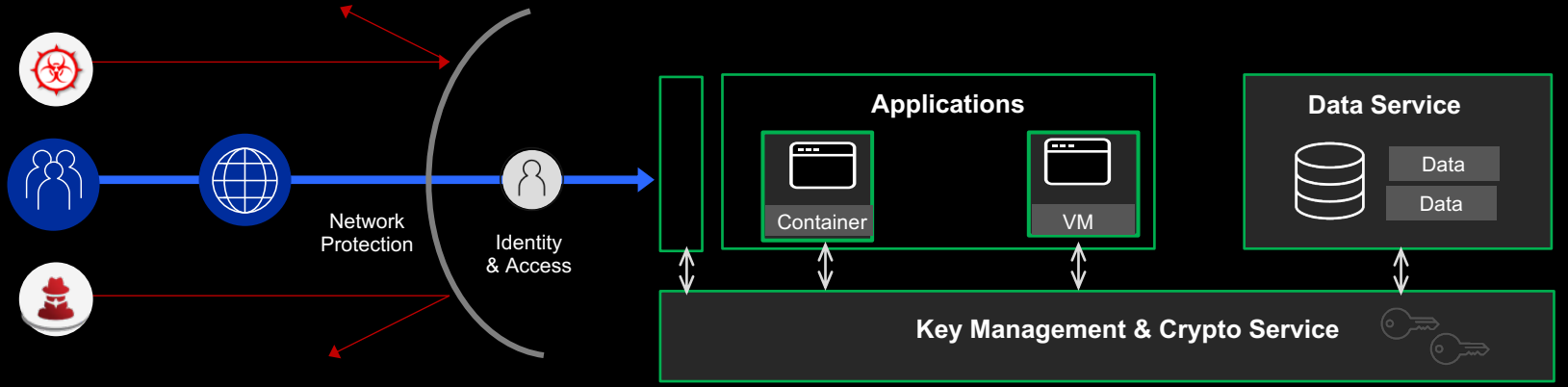
| | Preparing for ZT | Basic ZT | Intermediate ZT | Advanced ZT |
|---|---|---|---|---|
| | **Ad hoc processes** | **Defined processes and best practices** | **Repeatable processes and best practices** | **Automated** |
|  | Multiple, on premises identity providers<br>No cloud-on premises identity integration<br>Limited visibility into identity risk | Cloud identity federates with on premises<br>Conditional access policies enabled | Cloud identity federates with on premises<br>Conditional access policies enabled<br>Analytics run to improve visibility | Passwordless authentication enabled<br>ID, device, location analyzed in real time to determine risk & for ongoing protection |
|  | Devices must be on the network to access apps and data<br>Devices are network managed | Devices registered in inventory<br>Access only for registered devices | Devices registered in inventory<br>Access only for registered devices<br>Policies are enforced for all devices | Endpoint threat detection monitors device risk<br>All devices have access gated based on device risk |
|  | Apps accessed via physical network or VPN<br>Critical cloud apps available to users | Apps configured with SSO<br>Some on premises apps are “internet” facing | On premises apps are internet facing, cloud apps use SSO<br>Risk assessment used to control critical apps | All apps use least privilege access with continual verification and analysis<br>Dynamic controls for all apps with monitoring and automated response |
|  | Separate manual permissions | Manual permissions across environments<br>Configuration management of ”VMs” where workloads are running | Workloads monitored for abnormal behavior with alerting<br>Every workload has an app Identity | Unauthorized deployment blocked/reported<br>Workloads have granular visibility & controls<br>Segmented user/resource access for each workload |
|  | Access governed at the data set level | Access governed at data level, not based on data sensitivity<br>Sensitivity labels manual, with inconsistent classifications | Data classified and labeled using regex/keyword methods<br>Access governed by encryption | Classification augmented by ML/AI<br>Access governed by policy engine<br>Data securely shared with encryption and tracking |
|  | Minimal endpoints, flat network<br>No encryption of internal traffic | Few endpoints, flat network<br>Static traffic filtering, minimal protection<br>No encryption of internal traffic | Many micro perimeters w/ some micro segmentation<br>Filtering and protection for known threats<br>User to app traffic encrypted | Distributed micro perimeters w/ deep micro segmentation<br>AI based filtering and protection<br>All traffic encrypted |

# LinuxONE in the Zero Trust level characteristic

White = IBM Z Solution
Black = IBM Security Solution
Orange = Device specific

| | Preparing for ZT | Basic ZT | Intermediate ZT | Advanced ZT |
|---|---|---|---|---|
| | **Ad hoc processes** | **Defined processes and best practices** | **Repeatable processes and best practices** | **Automated** |
|  | RACF for z/VM<br>openLDAP and ISDS | IBM Z Multi-factor Authentication | IBM Security Verify | IBM zSecure Manager for RACFVM |
|  | IBM LinuxONE has no offerings to secure devices, unless the device is an IBM LinuxONE system, then what is below for infrastructure would fit here | | | |
| | Corporate login policies | IBM IAM Services | IBM Security MaaS360 | MaaS360 Mobile Threat Management |
|  | OMEGAMON for z/VM<br>z/VM Performance Toolkit | IBM Cloud Infrastructure Center | RedHat OpenShift Container Platform | Application Dependency Discovery Manager |
|  | CPACF<br>Crypto Express Adapters | SELinux and sVIRT<br>Secure Execution<br>Secure Service Container partitions | z/VM Infrastructure Suite<br>(includes Operations Manager,<br>Backup and Restore Manager) | Red Hat Insights |
|  | Pervasive Encryption<br>Virtual machine hardware isolation | Linux filesystem encryption (dm-crypt)<br>Fibre Channel Endpoint Security<br>EKMF Web | Hyper Protect Crypto Services<br>Hyper Protect DBaaS | Hyper Protect Data Controller<br>QRadar |
|  | Fibre Channel Endpoint Security | SSI Channel Isolation<br>TLS Encryption of SDNs | QRadar Incident Forensics | QRadar Network Insights<br>X-Force Exchange |

# Full Stack.  End to end.  Zero Trust.




| NETWORK SECURITY | IDENTITY & ACCESS | APPLICATION & ENDPOINT SECURITY | DATA PROTECTION |
|---|---|---|---|
| Crypto Express 7S | RACF, SELinux, IAM | | Pervasive Encryption and CPACF |
| TLS Endpoint Protection | IBM Z MFA V2.1 | | Hyper Protect Data Controller |
| | IBM zSecure for RACFVM | | |

# Cyber Resiliency: Where Resilience and Security Meet

**IDENTIFY**
Risks and vulnerabilities

**PROTECT**
Your critical applications and data

**DETECT**
Data corruption and configuration anomalies

**RESPOND**
To changes in configuration and data

**RECOVER**
Access to critical applications and data

**CyberResiliency Goals:**

- Anticipate
- Withstand
- Recover
- Adapt

**Cyber Resiliency Objectives:**

- Understand
- Prevent/Avoid
- Prepare
- Continue
- Constrain
- Reconstitute
- Transform
- Re-architect

https://doi.org/10.6028/NIST.SP.800-160v2

# CyberResiliency for LinuxONE

## IDENTIFY

**Risks and vulnerabilities**

- Dynamic Partition Manager
- IBM zSecure for RACF/VM
- QRadar for SIEM

## PROTECT

**Your critical applications and data**

- GDPS Support
- RACF for z/VM
- IBM zSecure Manager for RACF/VM
- Hyper Protect Data Controller
- Pervasive Encryption for Linux filesystems

## DETECT

**Data corruption and configuration anomalies**

- Linux Audit
- IBM Security zSecure Manager for RACF/VM
- IBM QRadar for SIEM
- Operations Manager for z/VM

## RESPOND

**To changes in configuration and data**

- Dynamic Memory Add
- Single System Image
- HyperPAV
- Dynamic I/O Reconfig
- GDPS Support
- Operations Manager for z/VM

## RECOVER

**Access to critical applications and data**

- System Recovery Boost
- Pacemaker/Corosync
- HyperPAV
- Linux Auto-IPL
- OCP Quorum Management
- Backup/Restore for z/VM

# Constantly Extending LinuxONE Security Leadership

*Leveraging integration to deliver robust security*

**Integrated Crypto HW**

Massive secure transaction throughput

**Encrypting Storage**

Self encrypting tape and disk drives

**Secure Service Container**

Secure deployment of software appliances

2006

2017


**Fibre Channel Endpoint Security**

Ensure data integrity on the hardware level

SOD

2019

**Hyper Protect Data Controller**

Data centric protection and enforcement on and off LinuxONE

**Secure Execution for Linux**

Secure the guests the malicious admins

# Thank you

Brian Hugenbruch, CISSP
IBM Z Security for Virtualization and Cloud
bwhugen@us.ibm.com

Pradeep Parameshwaran
IBM LinuxONE Security Lead
Pradeep@de.ibm.com


**Please complete the session evaluation!**

# Notices and disclaimers



**U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

**Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**

Performance  data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those

customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

# Notices and disclaimers

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**
- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.
- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml


IBM