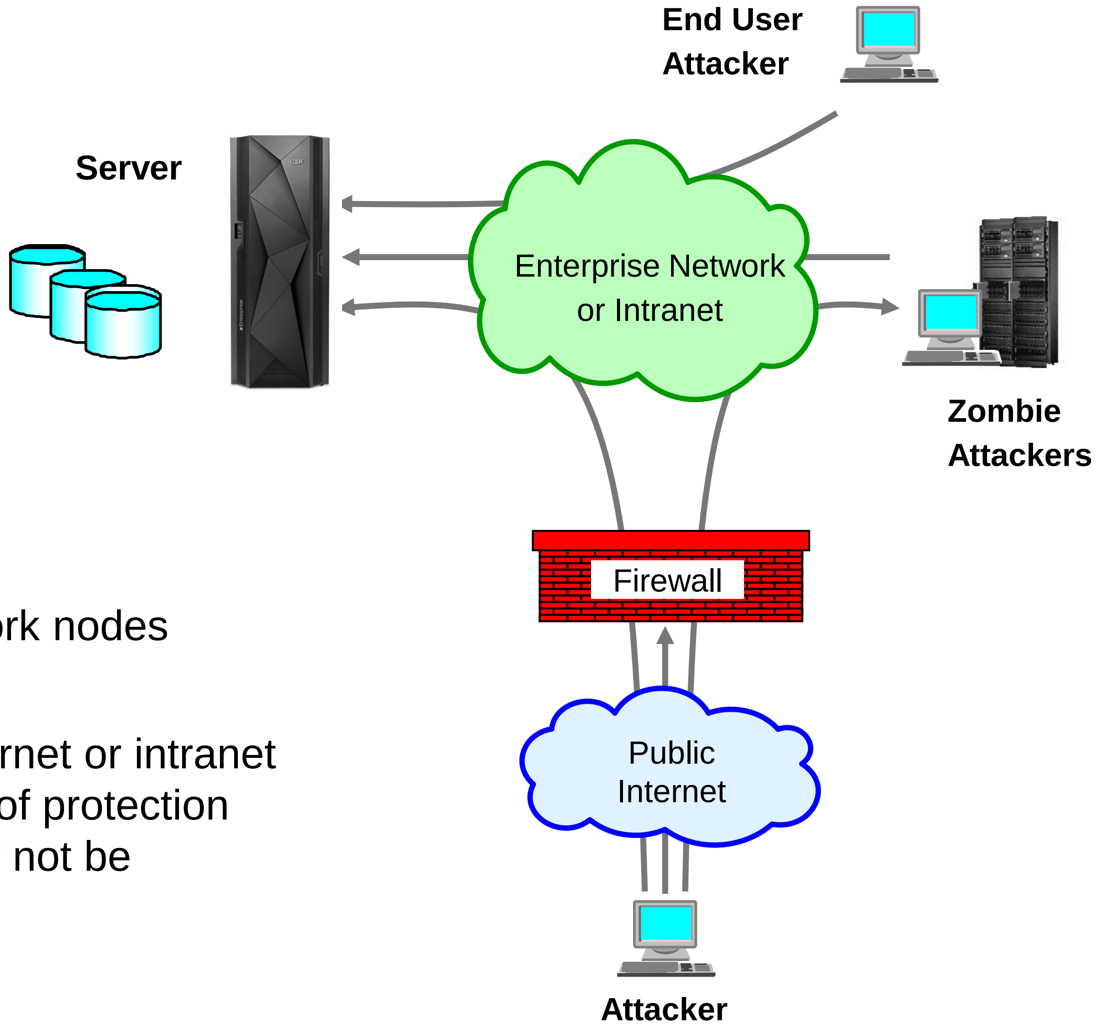
IBM Competitive Project Office

The New zEnterprise – A Cost-Busting Platform

Security on System z – Inspector "z" and the Case of the Web Intrusion

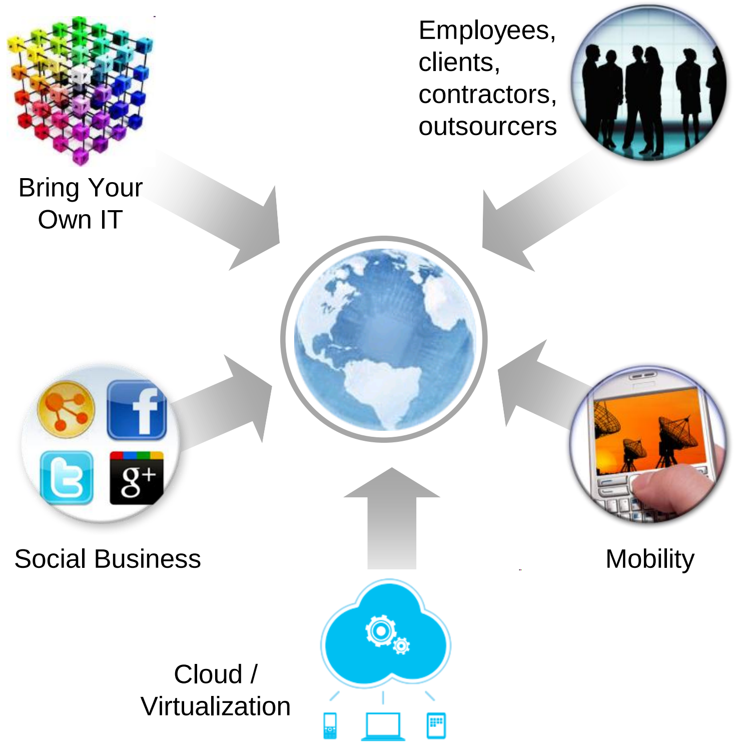
Destructive cyber intrusions can vary in style, intention and origin

- What is an intrusion?
  - Information Gathering
  - Eavesdropping
  - Impersonation
  - Theft
  - Denial of Service
- Some are deliberate, some are unintentional
  - Malicious intent from outside or internal bots
  - Unintentional errors on network nodes
- Intrusions can originate from Internet or intranet
  - Firewalls provide some level of protection
  - Perimeter security alone may not be sufficient



Cyber vulnerabilities have increased dramatically with the emergence of mobile, cloud, BYOD, Web 2.0, etc.

Embracing New Technologies, Adopting New Business Models



Bring Your Own IT

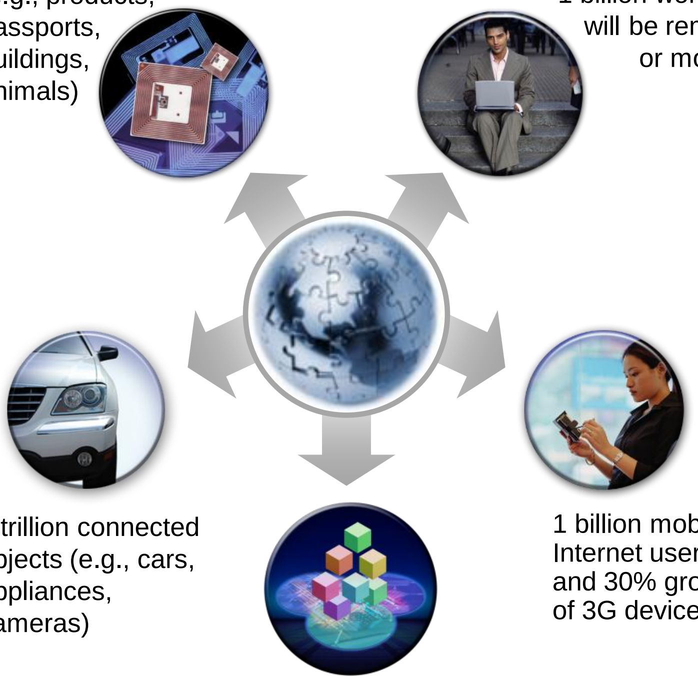
Employees, clients, contractors, outsourcers

Social Business

Mobility

Cloud / Virtualization

Exploding and Interconnected Digital Universe



30 billion RFID tags (e.g., products, passports, buildings, animals)

1 billion workers will be remote or mobile

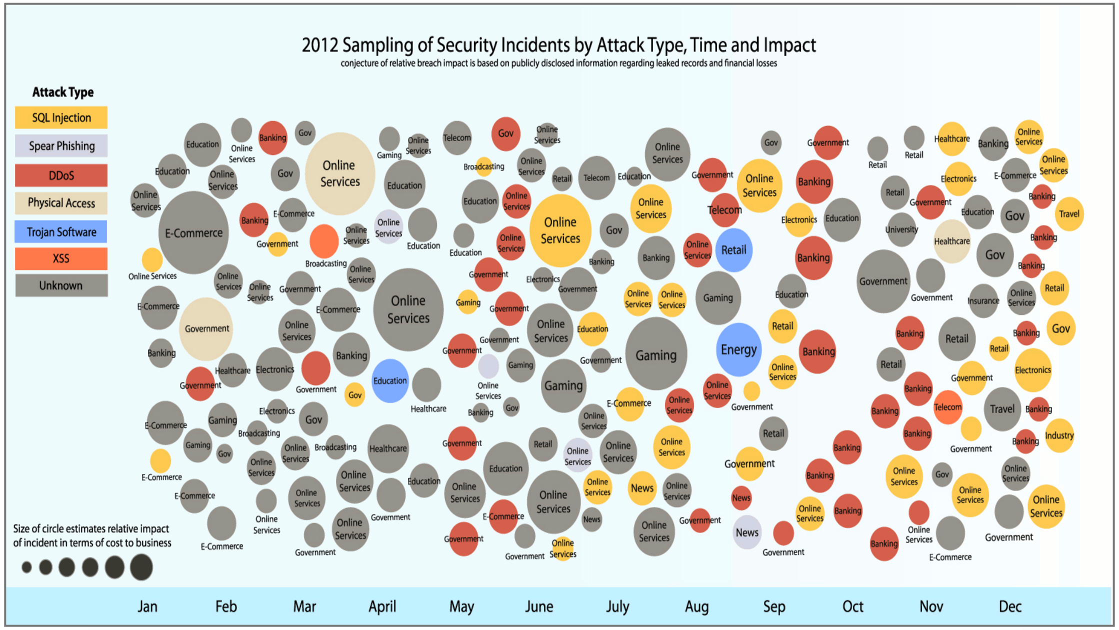
1 trillion connected objects (e.g., cars, appliances, cameras)

1 billion mobile Internet users, and 30% growth of 3G devices

33% of all new business software spending will be Software as a Service

Cyber attacks are on the rise

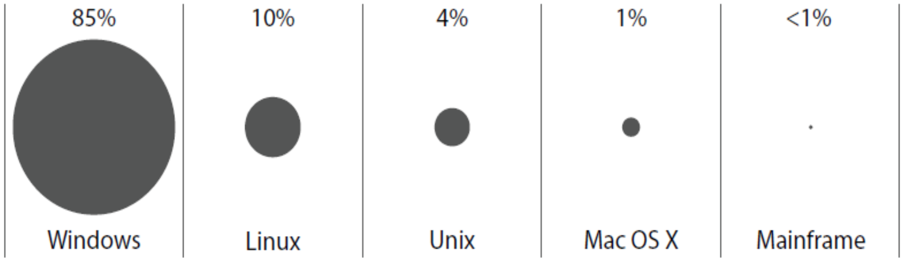
- All industries targeted
- Vary in style, attack type and platform (operating system)
- Large in number, and increasing over time
- Always leveraging new technologies
- Often new vulnerabilities are exploited faster than fixes can be developed



2012 Sampling of Security Incidents by Attack Type, Time and Impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

Distribution of Data Breaches by Operating Systems



Source: Verizon 2011 Data Breach Investigations Report

Source: X-Force Research 2011 Trend Report; X-Force Research 2012 Trend Report

A recent study shows organizations incur staggering costs from data breaches

Data Breach Costs

$136
Average per record

$157
Malicious/criminal breaches

Industries with highest cost per record:

$233
Healthcare

$215
Financial

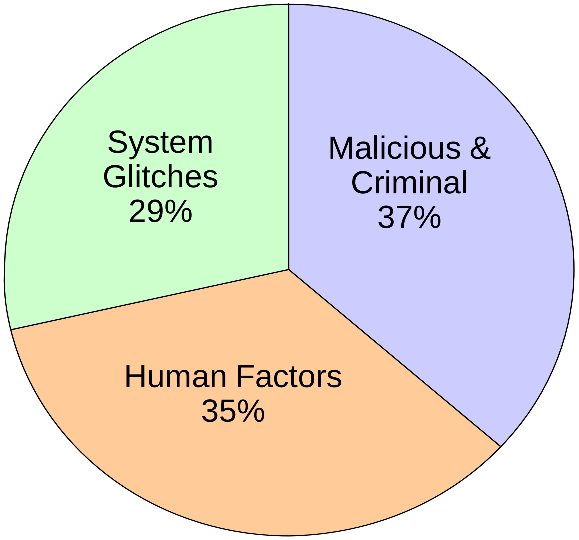
Average total costs (trend is up Y/Y)

$5.4M
United States

$4.8M
Germany

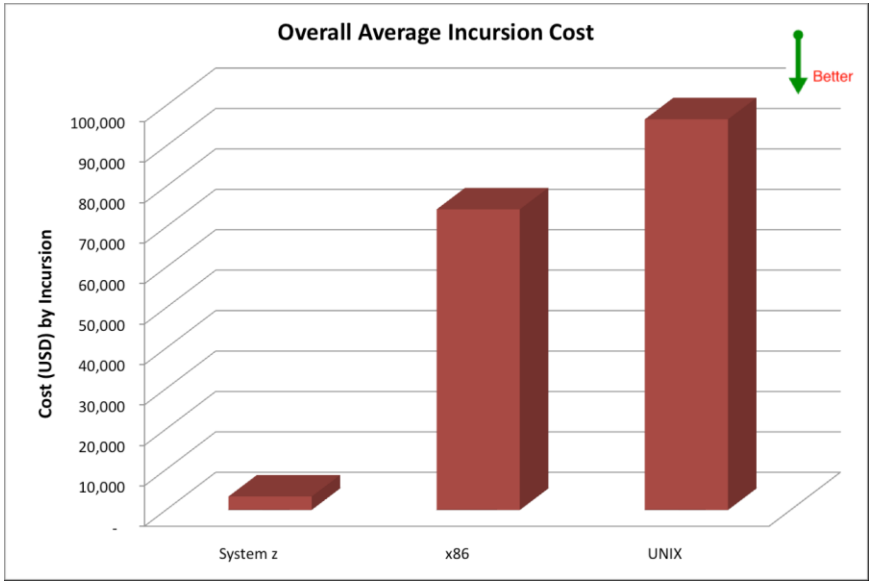
2.4 – 4.4%
Increase in lost customers

Data Breach Causes



Source: Ponemon 2013 Cost of Data Breach Study. Survey of 277 organizations across 9 countries

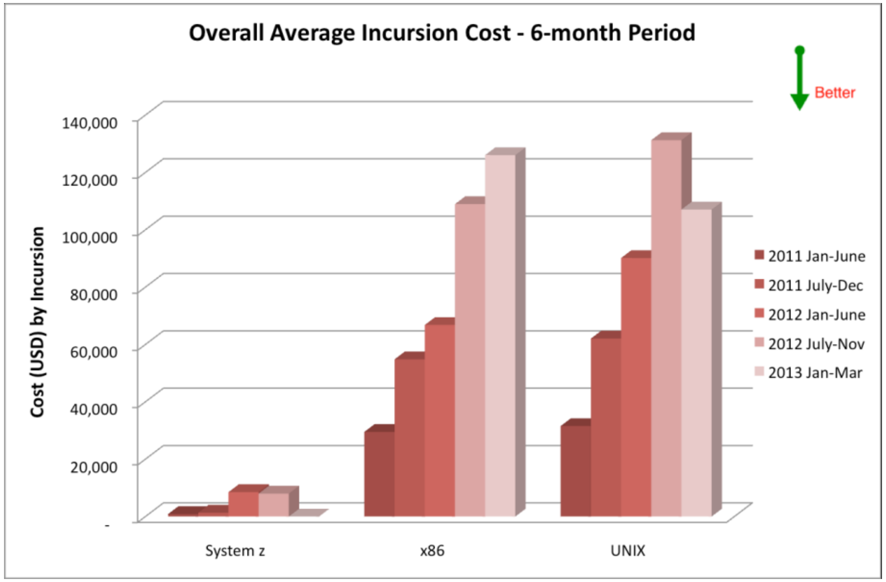
Average incursion costs on System z are lower than other platforms



Customer surveys show System z average incursion costs are significantly lower than distributed platforms

Average incursion costs are increasing

- More attack points
- Highly skilled attackers



Source: “Tracked, Hacked and Attacked?”
© 2013, Solitaire Interglobal Ltd. https://www.ibm.com/services/forms/signup.do?source=stg-web&S_PKG=ov14292

Why would a thief choose to attack a heavily protected target?

“…because that's where the money is”

Willie Sutton (1901-1980) – notorious and prolific American bank robber

How do you know when you have been robbed?

When something of value is missing!

What about your data?

Nothing is “missing”…

Most likely, something has been added to provide future access…

Why are mainframes high value targets?

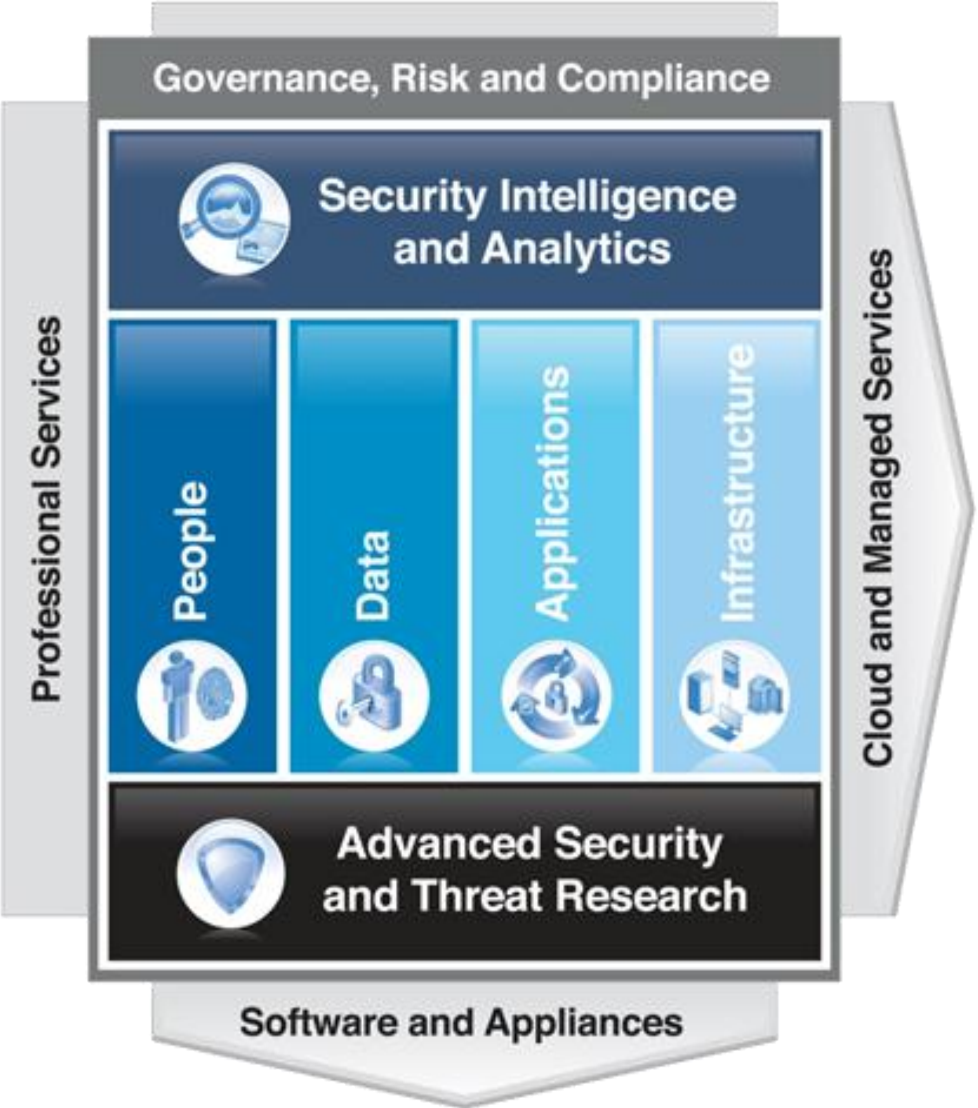
"…because that's where the data is"

60-70% of the world's corporate data resides on mainframe servers

- Credit card and other account records
- Other tax / financial records
- Patient medical records
- Design documentation
- Trade secrets

Data is the ultimate target

Today’s enterprise security requires many elements



Governance, Risk and Compliance
Professional Services
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Cloud and Managed Services
Software and Appliances

System z is the industry’s most trusted platform

IBM’s Premier Security Platform: zEnterprise

- Extremely secure platform for virtual environments and workloads
- Security at every level
- Complies with security related regulatory requirements
- Extensive Security Certifications (e.g., Common Criteria and FIPS 140)

Security begins with System z secure processing

- Workload isolation
  - Isolation of users address spaces
  - Processing integrity with LPAR separation
  - Separate system and user spaces
- HiperSocket secure LPAR communications
- Authorized Program Facility (APF)
  - Executable code can be invoked only by authorized users
  - Cross memory services prevents unauthorized access
- System Integrity Statement
  - IBM accepts responsibility for integrity exposures found by customers

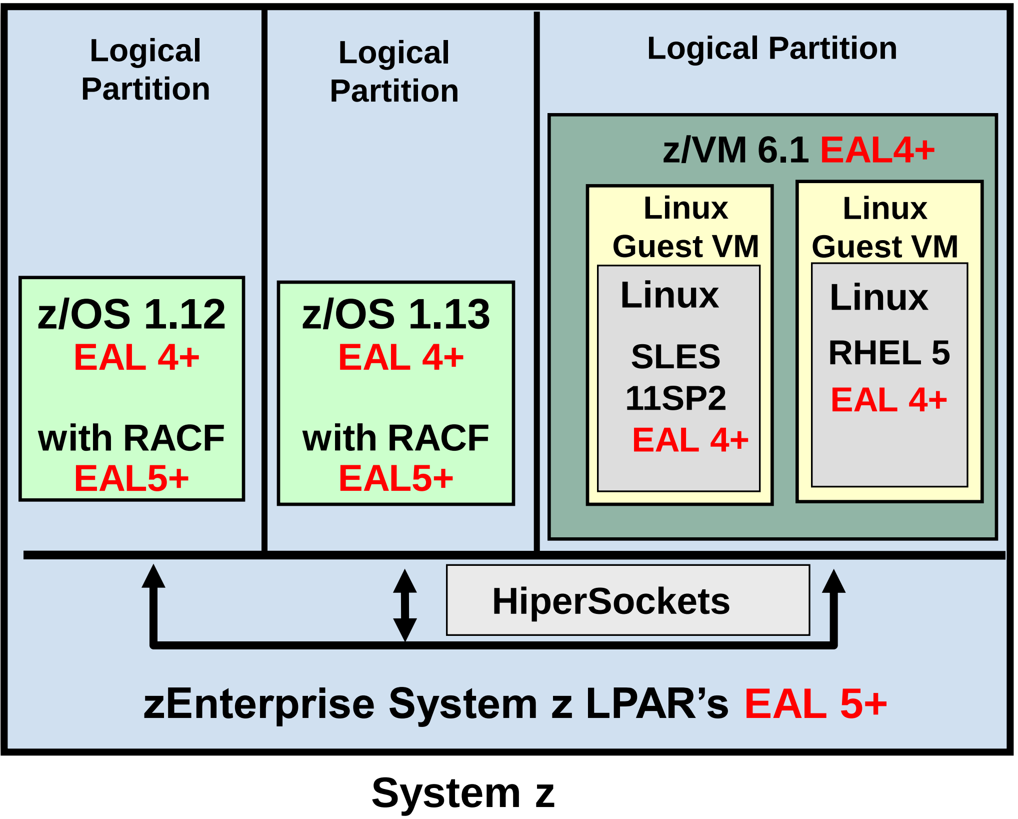
Viruses are non-existent in System z architecture

- Strict division between privileged and non-privileged instructions
- Strict division between configuration hardware (SE) and runtime hardware
- Minimized attack surface => Difficult to infect
- Firmware
  - Delivered with system
  - Digitally signed and verified
  - Upgraded over secured network

System z platform security Common Criteria EAL certifications lead the industry

Common Criteria EAL

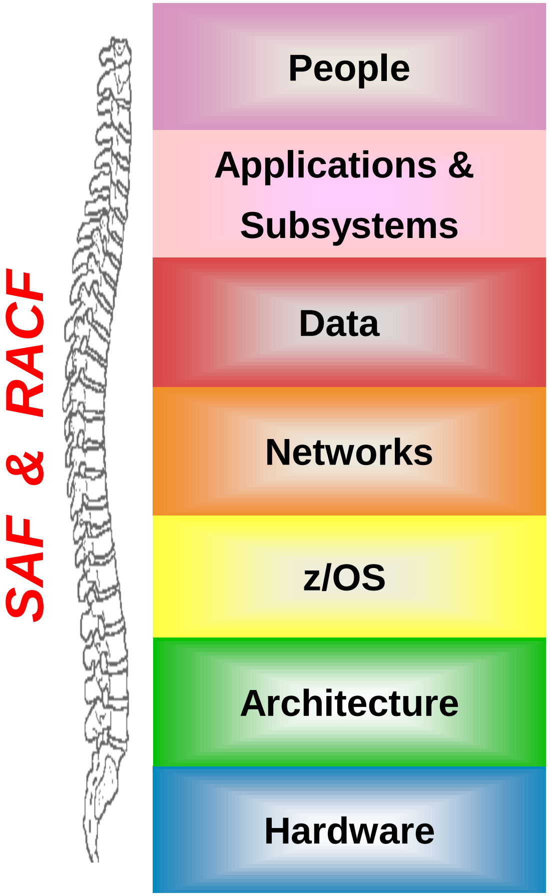
- Accepted computer systems security standard
- Based on functional and assurance requirements
- Higher Evaluation Assurance Level (EAL) rating is more secure



IBM System z holds the highest EAL grades in Common Criteria!

EAL Ratings: https://www.bsi.bund.de/SharedDocs/Zertifikate/CC/Betriebssysteme/0852.html

RACF is the backbone of security



SAF & RACF

People

Applications & Subsystems

Data

Networks

z/OS

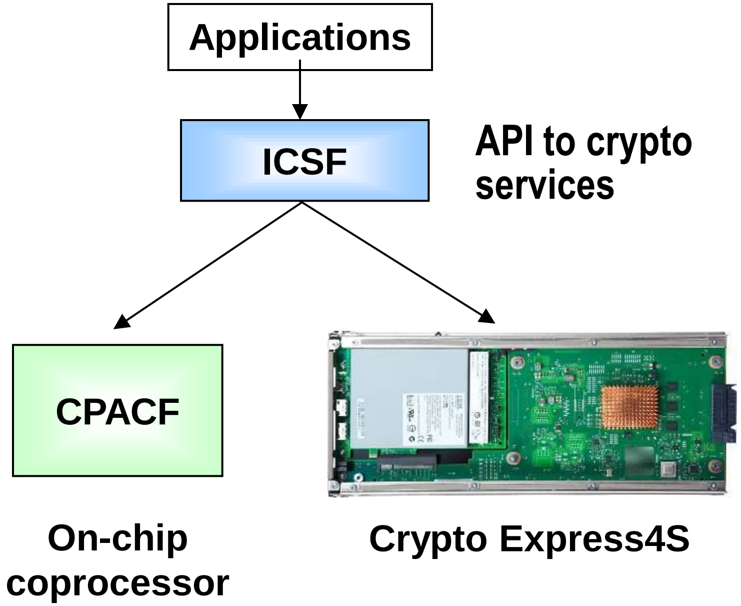
Architecture

Hardware

RACF and z/OS SAF provide security throughout the stack

- Tools, reporting, auditing
- Access control to all classes of resources
- Integrated into the operating system
- Provides Enterprise Identity Management
- Supports cryptographic services
- Supports digital certificates

zEnterprise hardware accelerators used for encryption



Transparently use whichever accelerator is available

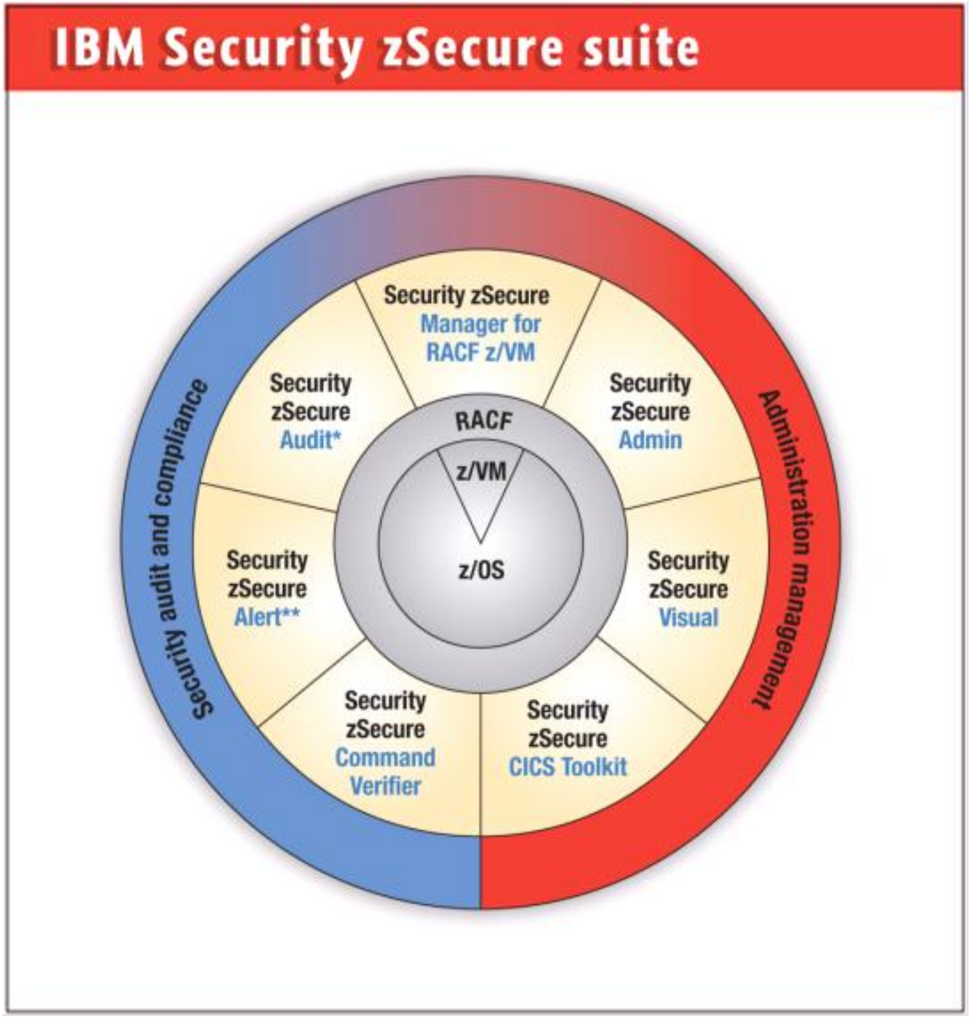
- Central Processor Assist for Cryptographic Function (CPACF)
  - One coprocessor per core
  - Included free of charge
  - 290-960 MB/sec bulk encryption rate
  - Support DES, SHA-1/2, AES

- Crypto Express4S Card (optional)
  - For SSL and Internet Key Exchange (IKE) acceleration, clear key RSA operations
  - FIPS 140-2 Level 4

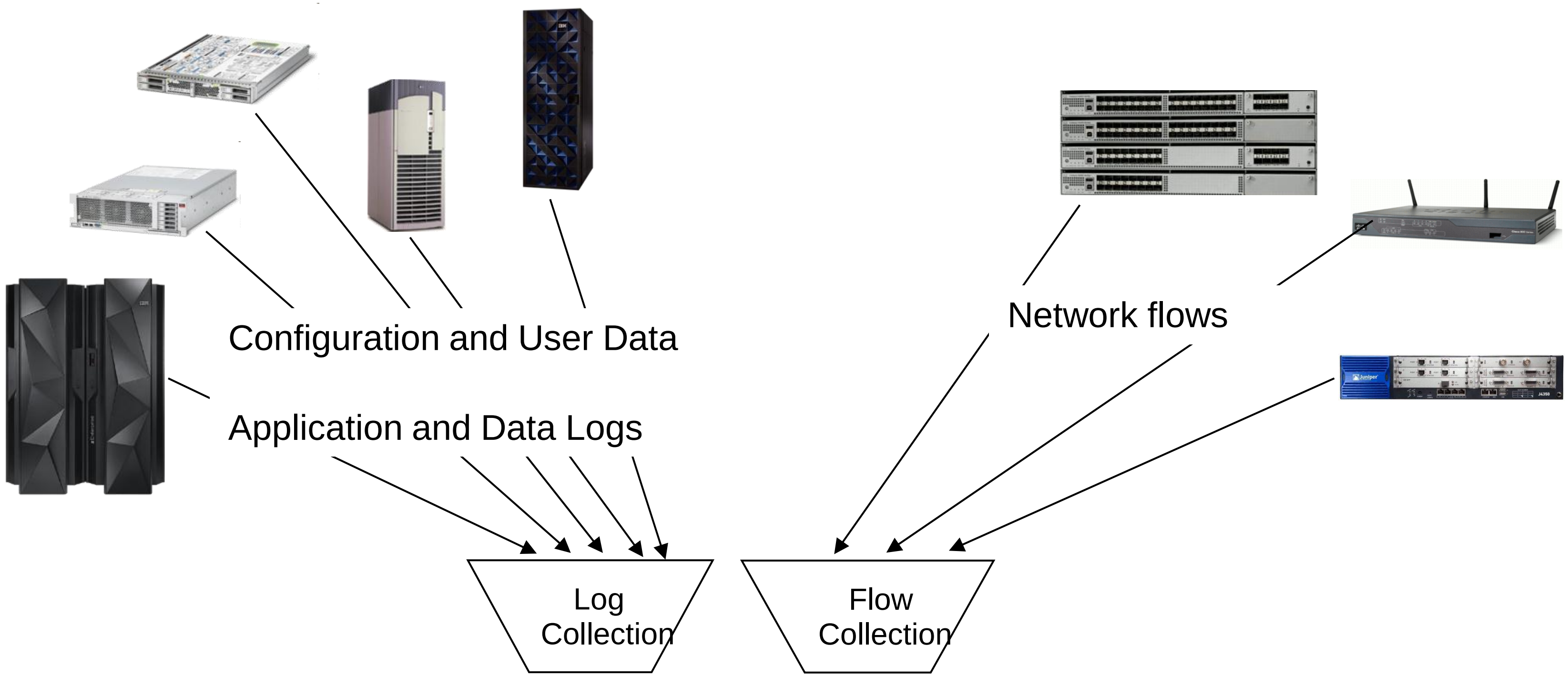
Integrated Cryptographic Service Facility (ICSF)

IBM zSecure Suite provides a full breadth of business benefits

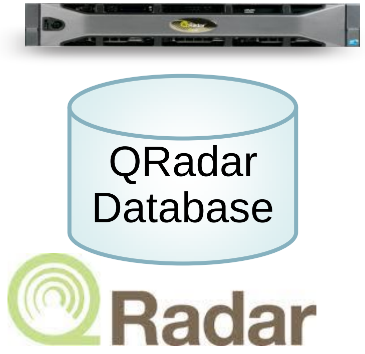
- Helps to reduce cost and improves resource utilization
- Improved system availability with automated analysis and detection of threats and configuration changes
- Proactive compliance monitoring
- Improves efficiency and quality


IBM Security zSecure suite
Security audit and compliance
Administration management
Security zSecure Manager for RACF z/VM
Security zSecure Audit*
Security zSecure Admin
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
RACF
z/VM
z/OS

QRadar SIEM Data Collection Overview



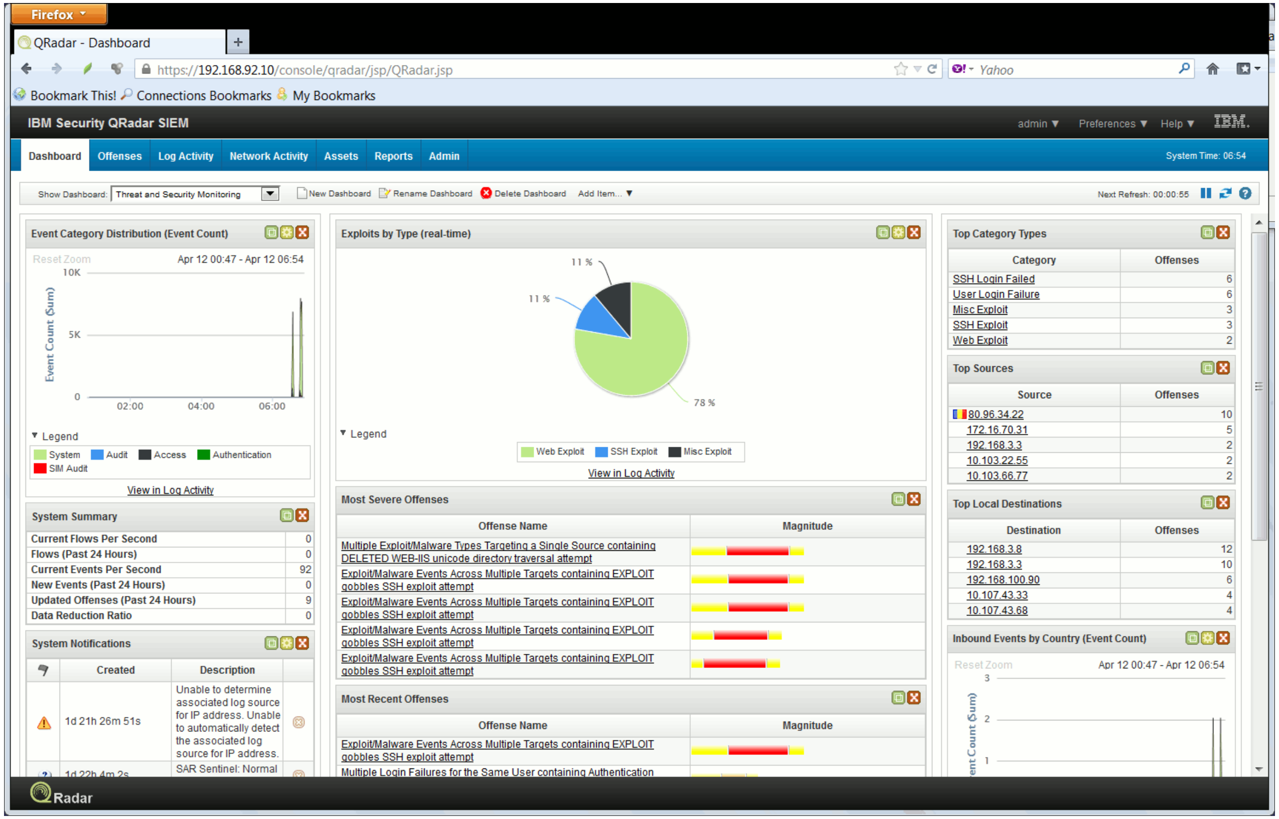
- QRadar collects, normalizes, and stores data from selected nodes
- Enables real time monitoring and dashboard



- Provides analysis and reporting on historical data
- Enables a deeper understanding by collating across nodes

DEMO: QRadar Security Information and Event Management

- Use QRadar SIEM to analyze network traffic flows
- Identify source and type of suspect traffic


Firefox
QRadar - Dashboard
https://192.168.92.10/console/qradar/jsp/QRadar.jsp
Yahoo
Bookmark This! Connections Bookmarks My Bookmarks
IBM Security QRadar SIEM
admin ▼ Preferences ▼ Help ▼ IBM.
Dashboard Offenses Log Activity Network Activity Assets Reports Admin
System Time: 06:54
Show Dashboard: Threat and Security Monitoring
New Dashboard Rename Dashboard Delete Dashboard Add Item... ▼
Next Refresh: 00:00:55
Event Category Distribution (Event Count)
Reset Zoom
Apr 12 00:47 - Apr 12 06:54
10K
5K
0
Event Count (Sum)
02:00
04:00
06:00
▼ Legend
System Audit Access Authentication SIM Audit
View in Log Activity
Exploits by Type (real-time)
11 %
11 %
78 %
▼ Legend
Web Exploit SSH Exploit Misc Exploit
View in Log Activity
Inbound Events by Country (Event Count)
Reset Zoom
Apr 12 00:47 - Apr 12 06:54
3
2
1
ent Count (Sum)
Radar

System Summary

Current Flows Per Second	0
Flows (Past 24 Hours)	0
Current Events Per Second	92
New Events (Past 24 Hours)	0
Updated Offenses (Past 24 Hours)	9
Data Reduction Ratio	0

System Notifications

	Created	Description	
⚠	1d 21h 26m 51s	Unable to determine associated log source for IP address. Unable to automatically detect the associated log source for IP address.	☒
?	1d 22h 4m 2s	SAR Sentinel: Normal	☒

Most Severe Offenses

Offense Name	Magnitude
Multiple Exploit/Malware Types Targeting a Single Source containing DELETED WEB-IIS unicode directory traversal attempt	
Exploit/Malware Events Across Multiple Targets containing EXPLOIT gobbles SSH exploit attempt	
Exploit/Malware Events Across Multiple Targets containing EXPLOIT gobbles SSH exploit attempt	
Exploit/Malware Events Across Multiple Targets containing EXPLOIT gobbles SSH exploit attempt	
Exploit/Malware Events Across Multiple Targets containing EXPLOIT gobbles SSH exploit attempt	

Most Recent Offenses

Offense Name	Magnitude
Exploit/Malware Events Across Multiple Targets containing EXPLOIT gobbles SSH exploit attempt	
Multiple Login Failures for the Same User containing Authentication	

Top Category Types

Category	Offenses
SSH Login Failed	6
User Login Failure	6
Misc Exploit	3
SSH Exploit	3
Web Exploit	2

Top Sources

Source	Offenses
80.96.34.22	10
172.16.70.31	5
192.168.3.3	2
10.103.22.55	2
10.103.66.77	2

Top Local Destinations

Destination	Offenses
192.168.3.8	12
192.168.3.3	10
192.168.100.90	6
10.107.43.33	4
10.107.43.68	4

Full disk encryption is standard on IBM DS8000 storage

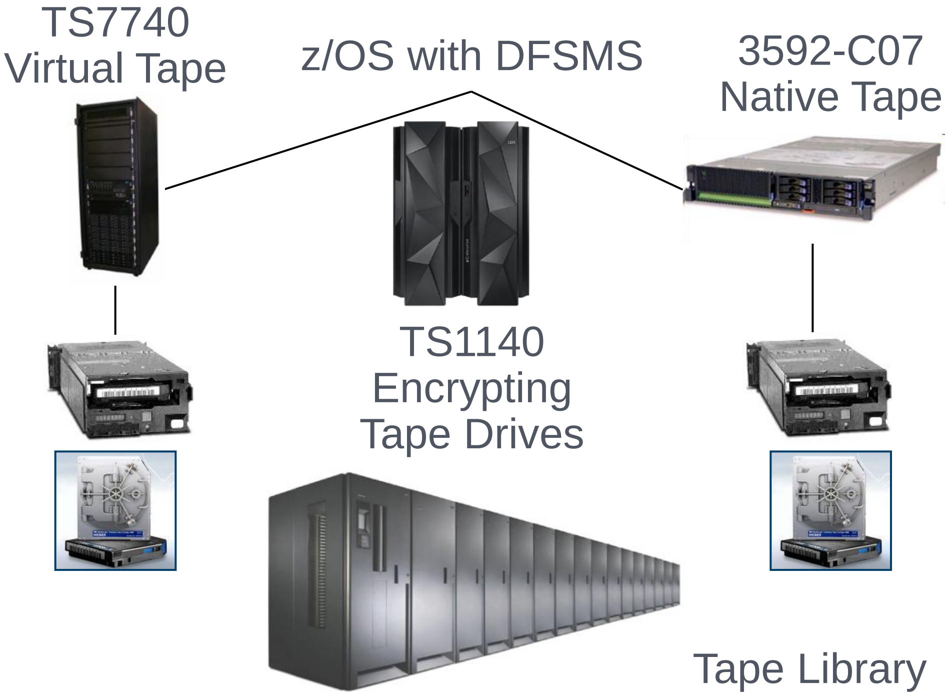
- Full Disk Encryption options across all drive tiers
- Same performance as standard drives
- Supports Easy Tier environments
- Standards-based key management software supports key management interoperability protocol (KMIP)
- Key manager supports both disk and tape
- Encryption is the least expensive data disposal technique

"Within five years, all HDDs and SSDs will be shipped preloaded with some kind of industry-standard FDE technology"

– Gartner Hype Cycle for Storage, July 2012

IBM System z tape offerings

- System z Tape Encryption is managed via DFSMS (System Managed Storage)
- Controlled via Storage
- Simple key management that leverages RACF
- Secure exchange of data with BPs and customers - No sharing of private keys
- FIPS 140-2 certified



TS7740 Virtual Tape

z/OS with DFSMS

3592-C07 Native Tape

TS1140 Encrypting Tape Drives

Tape Library

IBM’s Encryption Solution

- Encryption controlled on a per volume basis
- The same IBM tape drive can encrypt or decrypt on a per volume basis
- An individual tape can encrypt one time, not encrypt the next
- Uses the same key management as other IBM products
- Open Systems tape uses the same key store

Competition’s solutions:

- Require dedicated tape drives for encryption
- Require separate set of tapes for encryption
- Encryption controlled by volser range
- Key manager requires specific vendor supplied server

IBM Enterprise Key Management Foundation

Provide a centralized key management solution that leverages client's investments in IBM System z Hardware Cryptography for the ultimate protection of sensitive keys and meeting compliance standards

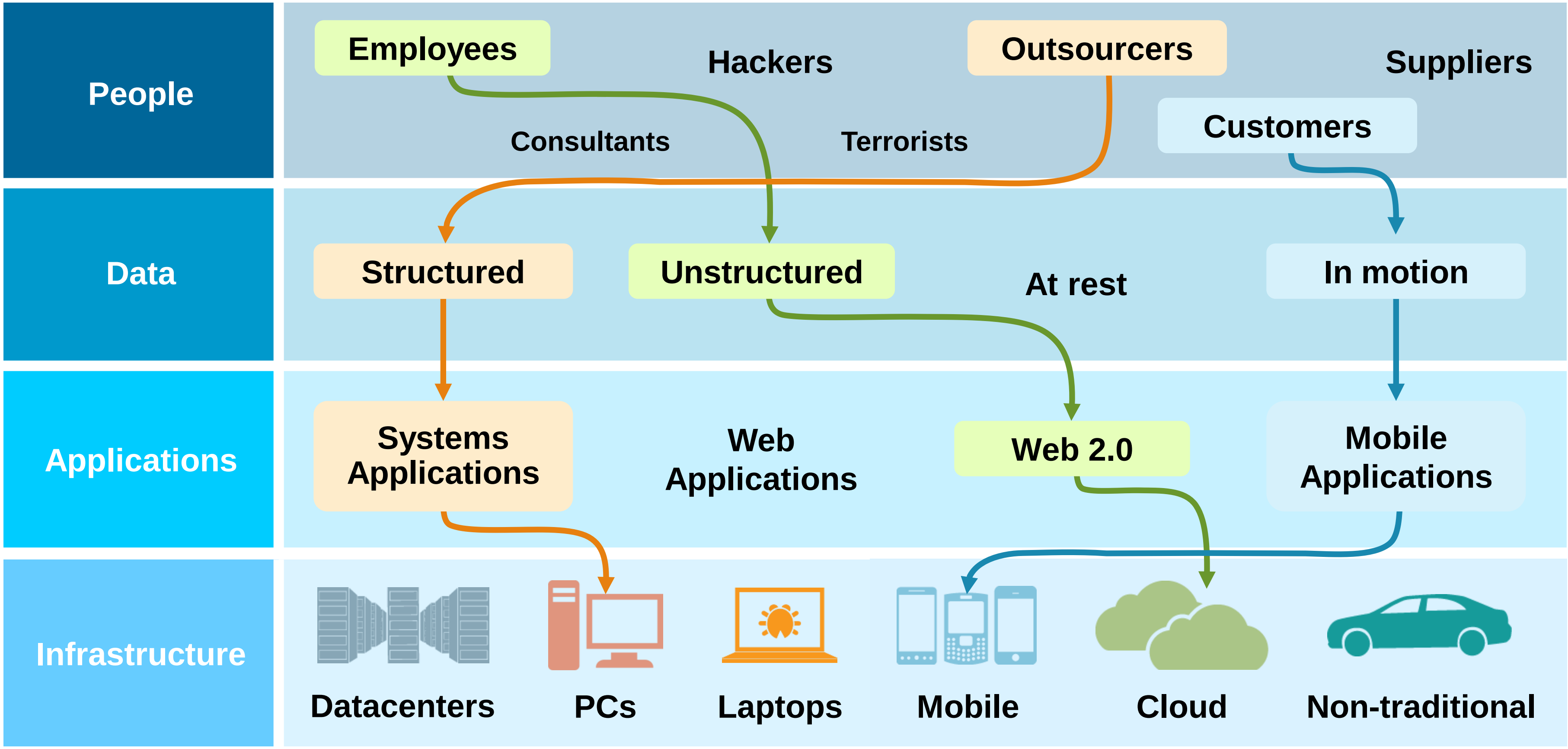
Solution Summary

- A simple centralized key management system
- Adheres to industry standards
- Customizable
- Includes crypto analytic capabilities that help identify compliance issues

Solution Benefits

- Efficient key management and automation
- Higher quality of service
- Leverages existing System z hardware
- Simplifies management of mission critical key material

Security as a complex, four-dimensional puzzle



Attempting to protect the perimeter is not enough – point products and traditional defenses cannot adequately secure the enterprise

The new security reality

- Perimeter protection, intrusion detection, and good practices are required…
  - *…but **no longer** sufficient!*

> ***“It's not a question of if, but when, your organization will experience a serious security breach”***
>
> ***- Kindervag and Holland, Forrester Research***

- ***Prepare to be breached!***
  - Encrypt sensitive data
  - Use secure hardware
  - Use well planned security processes
  - Have a response plan
  - Use a System Information and Event Manager (SIEM)

Meet Dan, a web administrator at a mid-sized enterprise…

- Locks down the Web server…
- Keeps firewalls current, applications patched, and data encrypted…
- Works closely with the security team who use zSecure and QRadar from IBM

I try to understand the new reality. I try to keep our enterprise as secure as possible…

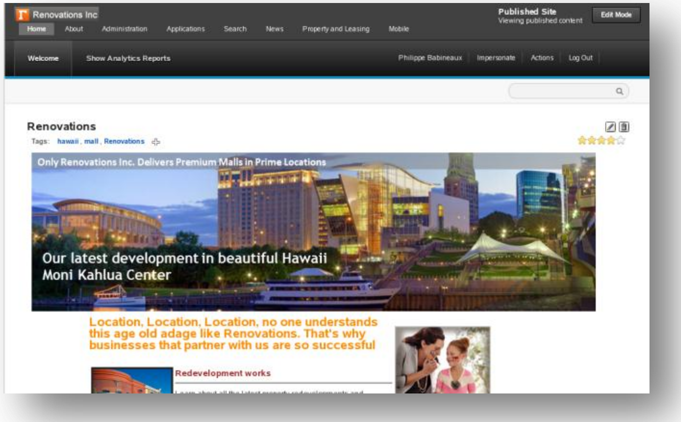
But he knows at some point a breach is going to happen…

Dan Misawa, Web administrator

Inspector “z” and The Case of the Web Intrusion

One day a suspicious event does occur!

- An attempt is made to alter the company home page…
- But the attempt failed, and no damage was done!



Renovations

Only Renovations Inc. Delivers Premium Malls in Prime Locations

Our latest development in beautiful Hawaii
Moni Kahlua Center

Location, Location, Location, no one understands this age old adage like Renovations. That's why businesses that partner with us are so successful

Redevelopment works

I need to know who did this, why and how! I’ll call in my friend **Inspector z**, the security administrator!

“Let the investigation begin!”

"Let's look at the information that's provided…"

1. zSecure logged event information including
a user id,
the files targeted,
and the time of attack

"Dan, it was *your* Web server user id used in the attack… and the attack happened in the middle of the night! "

"Could someone have gained access to my machine via a remote connection?"

"I think we know what happened…"

2. QRadar shows no network traffic at the time of the attack!

The attack came from inside!

3. Cron scheduler for the Web server shows a task scheduled for 1AM every day!

"Dan, this cron job is executing a Javascript that does a lot of damage…"

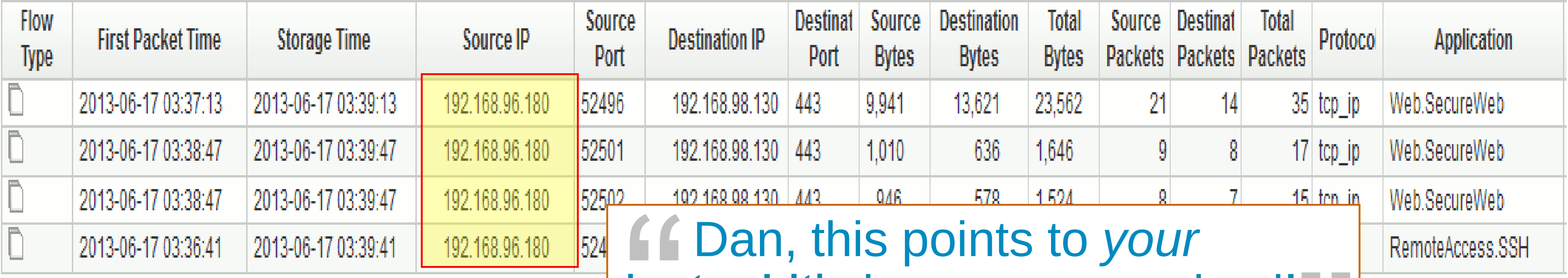
"If the attack had succeeded, visitors to our Web site would have been redirected to a rogue site for further attack!"

“Now let’s figure out how this happened…”

4. First remove all traces of the attack from the Web server file system

5. Then using QRadar, look for the time stamp of the cron table update

6. The data shows remote access… but from which machine?



Flow Type	First Packet Time	Storage Time	Source IP	Source Port	Destination IP	Destinat Port	Source Bytes	Destination Bytes	Total Bytes	Source Packets	Destinat Packets	Total Packets	Protoco	Application
🗋	2013-06-17 03:37:13	2013-06-17 03:39:13	192.168.96.180	52496	192.168.98.130	443	9,941	13,621	23,562	21	14	35	tcp_ip	Web.SecureWeb
🗋	2013-06-17 03:38:47	2013-06-17 03:39:47	192.168.96.180	52501	192.168.98.130	443	1,010	636	1,646	9	8	17	tcp_ip	Web.SecureWeb
🗋	2013-06-17 03:38:47	2013-06-17 03:39:47	192.168.96.180	52502	192.168.98.130	443	946	578	1,524	8	7	15	tcp_ip	Web.SecureWeb
🗋	2013-06-17 03:36:41	2013-06-17 03:39:41	192.168.96.180	524										RemoteAccess.SSH

“Dan, this points to *your* laptop! It’s been compromised!”

Case closed - Learning from mistakes is important

I *never* use the company laptop remotely…um… except at home when managing the company blog…

I dug deeper. Something attacked your computer when you were blogging… *and you did not even know!*

Attackers will find the weakest link

Even security-aware people can be hacked

Firewalls can't protect against something going around it

Security tips at the office

- Make breaching your defenses difficult
- Keep system up to date with patches
- Keep antivirus/anti malware software current
- Make pivoting after a breach difficult
- Establish and test an attack recovery plan
- Encrypt important data
  - Render breached data useless
- Use SIEM/analytics/database/security

Use the IBM System z Security Portal

Receive the latest information on System z security including associated Common Vulnerability Scoring System (CVSS) V2 ratings for new APARs

Register for access to the Security Portal
http://www-03.ibm.com/systems/z/advantages/security/integrity_sub.html

Security tips at home

- Stay patched (OS, browser, plug-ins, applications)
- Avoid plug-ins and browser add-ons to the extent possible
- Avoid open wireless hotspots if possible
- Use WPA2 or better encryption – never use WEP
- Use a unique wireless SSID – no default passwords
- Use a secure tunnel (VPN)
- Use separate hardware or browser to do admin work
- Don’t get tricked into infecting yourself
- What you do at home can wreak havoc at work
- Use good judgment with eMail, web surfing, social media. Check before clicking
  - http://www.google.com/safebrowsing/diagnostic?site=abc.com
- If prompted to install third party code, ***don’t!***
  - Open a separate window or tab and download the code directly from the software provider’s site
- **Everything** on social media **will** be used by someone targeting you

Don’t be the weak link!