Protecting your system at the core

"In the world of cyber security, the last thing you want is to have a target painted on you."

Gerard Saverimuthu
gerard@sg.ibm.com

Thanks to: Debapriya Chatterjee and Sandeep Korrapati

Threat Landscape is evolving

$4.35M

Global average cost of a data breach

2.6%
Increase from 2021

83%
Percentage of organizations that have had more than one breach

45%
Share of breaches that occurred in the cloud

19%
Frequency of breaches caused by stolen or compromised credentials

Top cost mitigating efforts

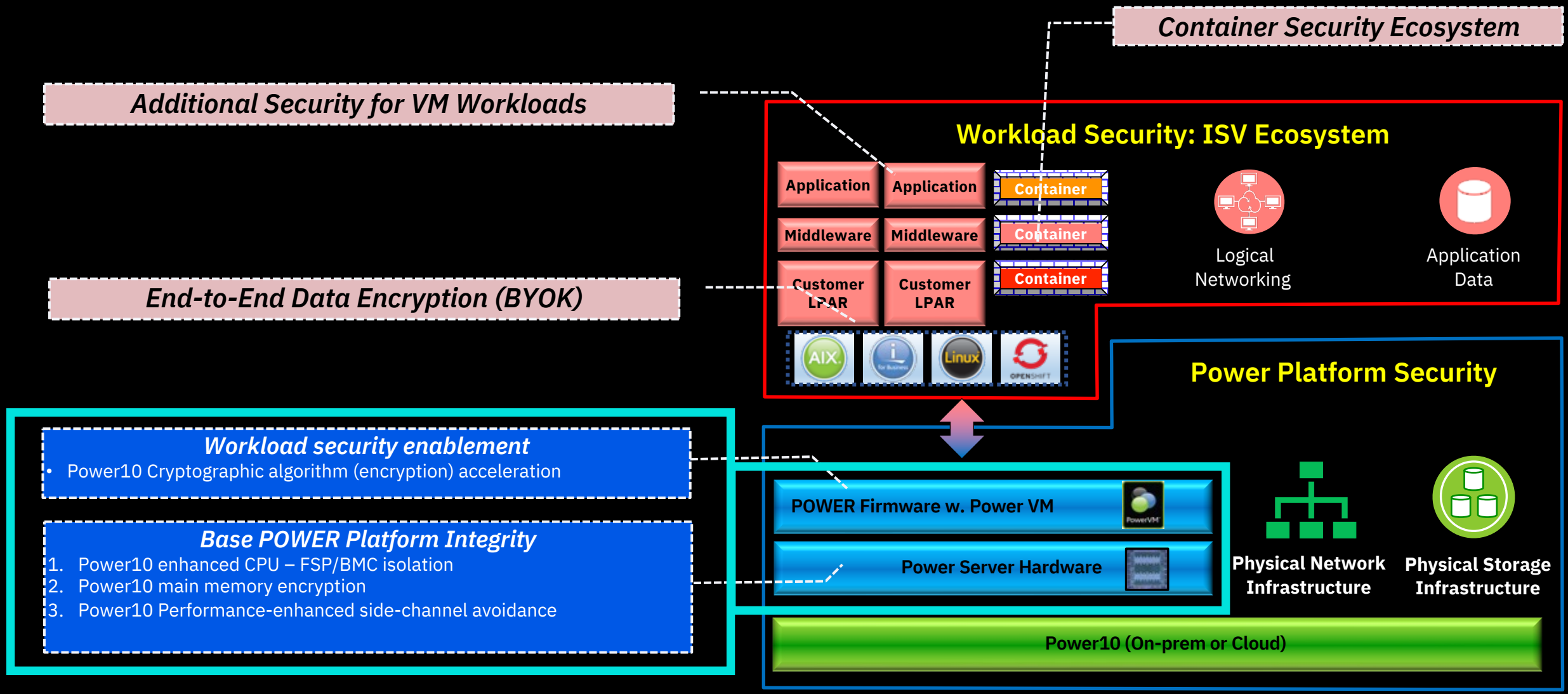
1. AI platforms
2. Encryption
3. Formation of the IR team

Top cost amplifying factors

1. Compliance failures
2. System complexity
3. Cloud migration

Source: “Cost of a Data Breach Report 2022” https://www.ibm.com/reports/data-breach

Power10 Security Ecosystem: Platform & Workloads



1. Stop: Micro-architectural side-channel attacks

Exploits speculative execution and other processor design oversights

Patches mostly impact performance


tom's HARDWARE

Intel CPUs Suffer Performance Hit From New Spectre-v2 Mitigations

By Zhiye Liu published March 11, 2022

Guess who's back?


wccftech

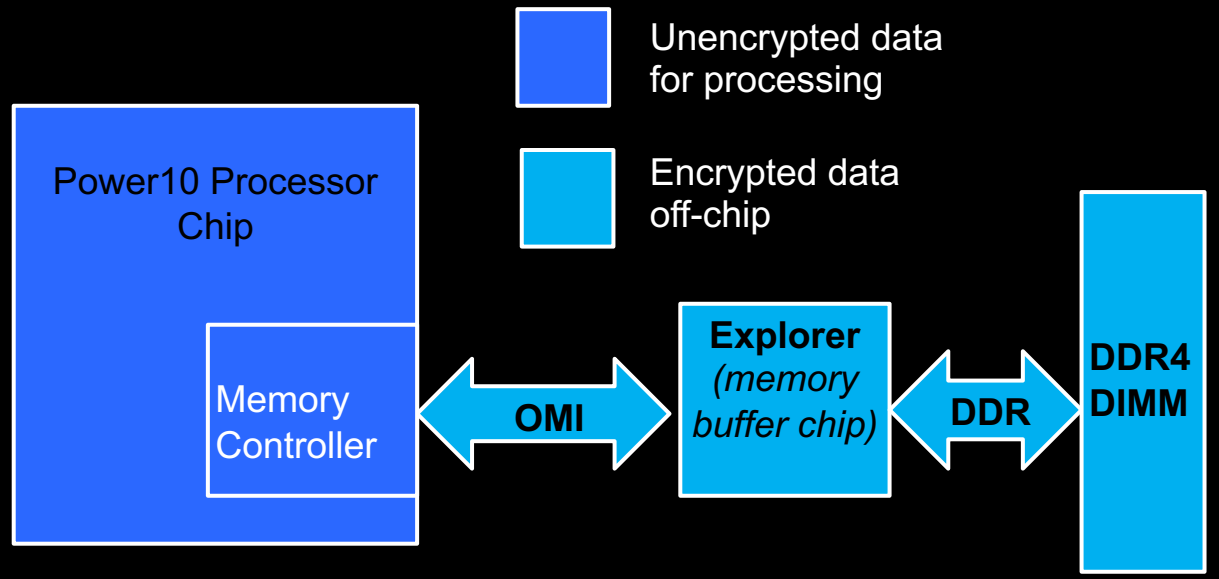
Intel Hardware Level Speculative Execution To Blame For Kernel Bug – KPTI Workaround Introduces Performance Hits Up To 23% On Average

Usman Pirzada • Jan 3, 2018, 11:34 AM EST

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

2. Encrypt your main memory

Power10 Processor provides support for encryption of main memory off chip

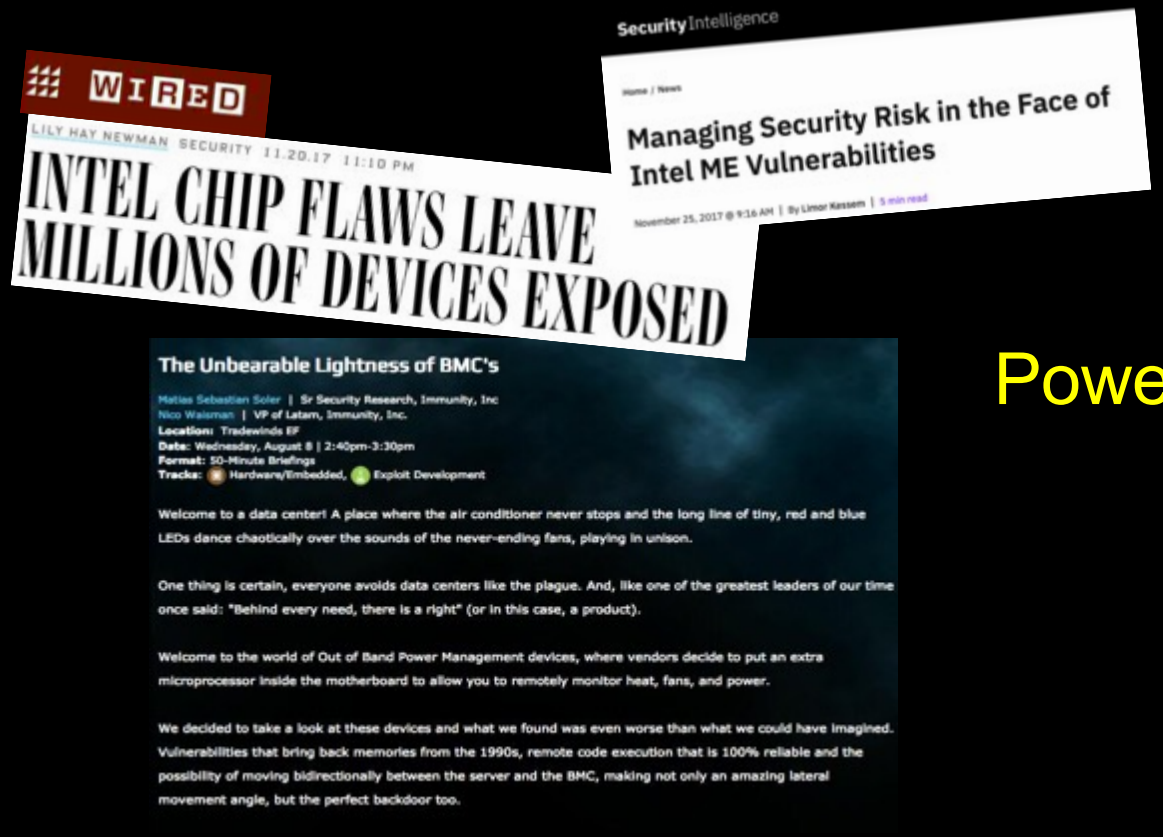


This security enhancement prevents:

1. Bus probing attacks
2. Cold boot attacks
3. Data theft by dumping DIMM contents
4. Provides pathway for secure adoption of non-volatile memory technologies for main memory

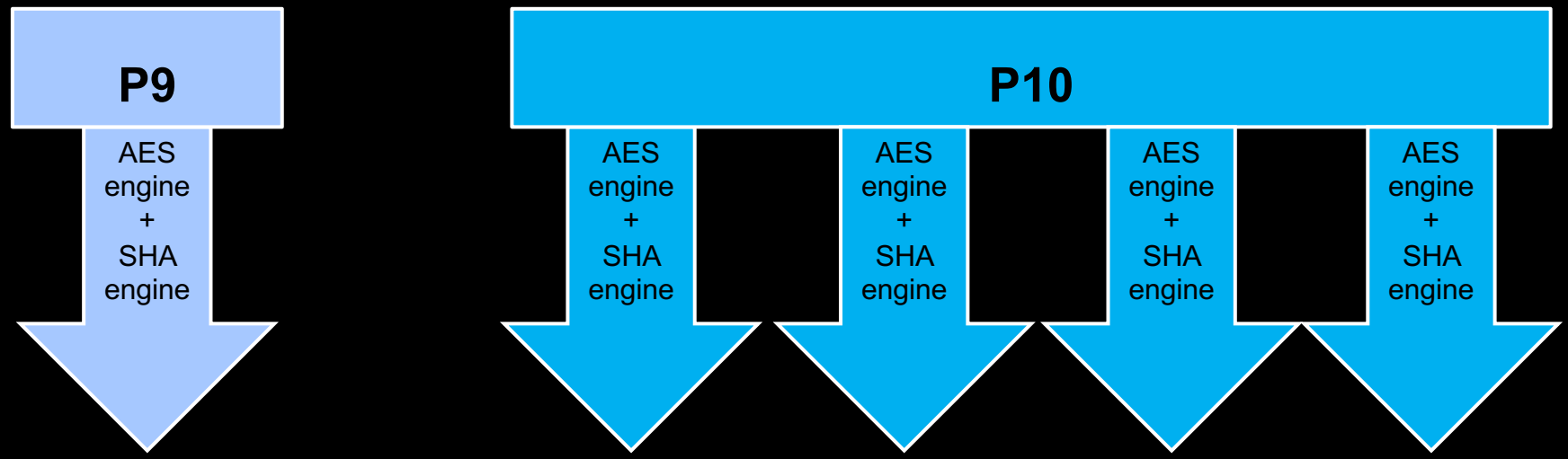
3. Enhance Separation of CPU and Service Processor Trust Domains

The importance of Service Processor Security



Power10 design limits access of BMC/FSP

4. Enhanced Cryptography Algorithm Acceleration



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

Improved encryption benefits:

1. AIX LV encryption,
2. IBM i ASP encryption,
3. Linux LUKS

IBM i Tip of the Month

Authority Collection was added to IBM i in V7.3 and enhanced in V7.4.
Let's look at 3 scenarios for Authority Collection.

1. **Profiles with too much authority**
2. **Troubleshoot authority failures**
3. **Determine/troubleshoot where authority is coming from**

Next steps… (example)
Turn on the Authority Collection for the profile: STRAUTCOL.
You can turn on the collection for every object the service account is going to access
You can also narrow down the collection and only log the access of *FILE objects for e.g. in LIB PROD1.

Call to Action:

1. Technology update workshop (~2 hours)
2. Zero Trust - Security Workshop
3. Ask about access to demos

Contact:
gerard@sg.ibm.com

#Letscreate Power10 solutions