



Flash Memory Summit

OakGate and Eclypsium: Zero Trust Capabilities

Presented by:

Corey Hirsh, Teledyne

Dave Obert, Teledyne LeCroy

Michael Thelander, Eclypsium





Dr. Corey Hirsch

About

- Chief Information Security Officer, Teledyne Technologies, 2014 onwards
- Lecturer in Cybersecurity, Columbia University, Masters Program in Technology Management
- Speaker on Cybersecurity, Enterprise Risk Management and Cyberwarfare
- Graduate FBI CISO Academy, Quantico, October 2018
- ISACA CISM
- CIO of LeCroy Corp. 2005 – 2014
- Prior to LeCroy, served 24 years at Tektronix, culminating in VP Europe for Test and Measurement

About the Presenters



Michael Thelander

About

- Director of Product Marketing for Eclypsium, *the Firmware Security Company*
- Previously head of product management and product marketing at Tripwire, iOvation and Venafi
- Speaker on authentication, secure configuration management, and firmware security at BSides, RSA, ISACA, and other events
- Author of articles in *SC Magazine*, *Cyber Defense Magazine*, *Cybersecurity: A Peer-Reviewed Journal* and other publications



David Obert

About

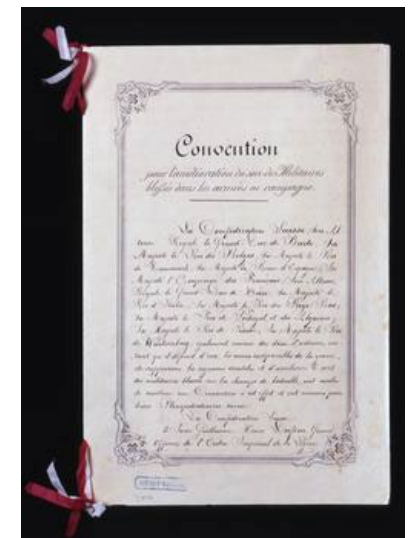
- Sales Development Manager with Teledyne LeCroy, OakGate Products
- Prior to Teledyne LeCroy, 30 years experience as a Marketing Specialist with Hewlett-Packard
- MBA from Drucker School of Management, Claremont Graduate School

In the Fifth Domain



Flash Memory Summit

- Integrating and disruptive technologies tilt the playing field in ***favor of the offense***
- ***Collateral damage is highest*** despite innate targeting capability of weaponry
- ***Institutions*** to govern conflict ***have not yet developed***
 - No Laws of Warfare nor Functional Treaties
 - No Red Cross
 - Little Protection from State Organs
 - Little Justice via Law Enforcement
 - Pronounced Asymmetries and Low Cost of Entry
- ***Technology Leaps, the Law Creeps***
- ***Risks are ambiguous***, controls are disintermediated
- Borders and battle maps are ***virtual*** rather than spatial
- ***There are no non-combatants***



Gerasimov Doctrine and Logic-Bearing Componentry:



Flash Memory Summit

"The role of non-military means of achieving political and strategic goals has grown, and in many cases they have exceeded the power of force of (kinetic) weapons in their effectiveness"

Gen Valery Gerasimov, Chief of the General Staff of the Armed Forces of Russia
Military Doctrine of the Russian Federation



Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

- The first ransomware attack, 1989, "PC Cyborg"
 - 20,000 infected 5.25-inch **floppy disks** mailed to attendees of WHO AIDS Conference
 - On 90th reboot following infection, ransom demand appeared; \$189 (to be paid by mailed check to Panama!)

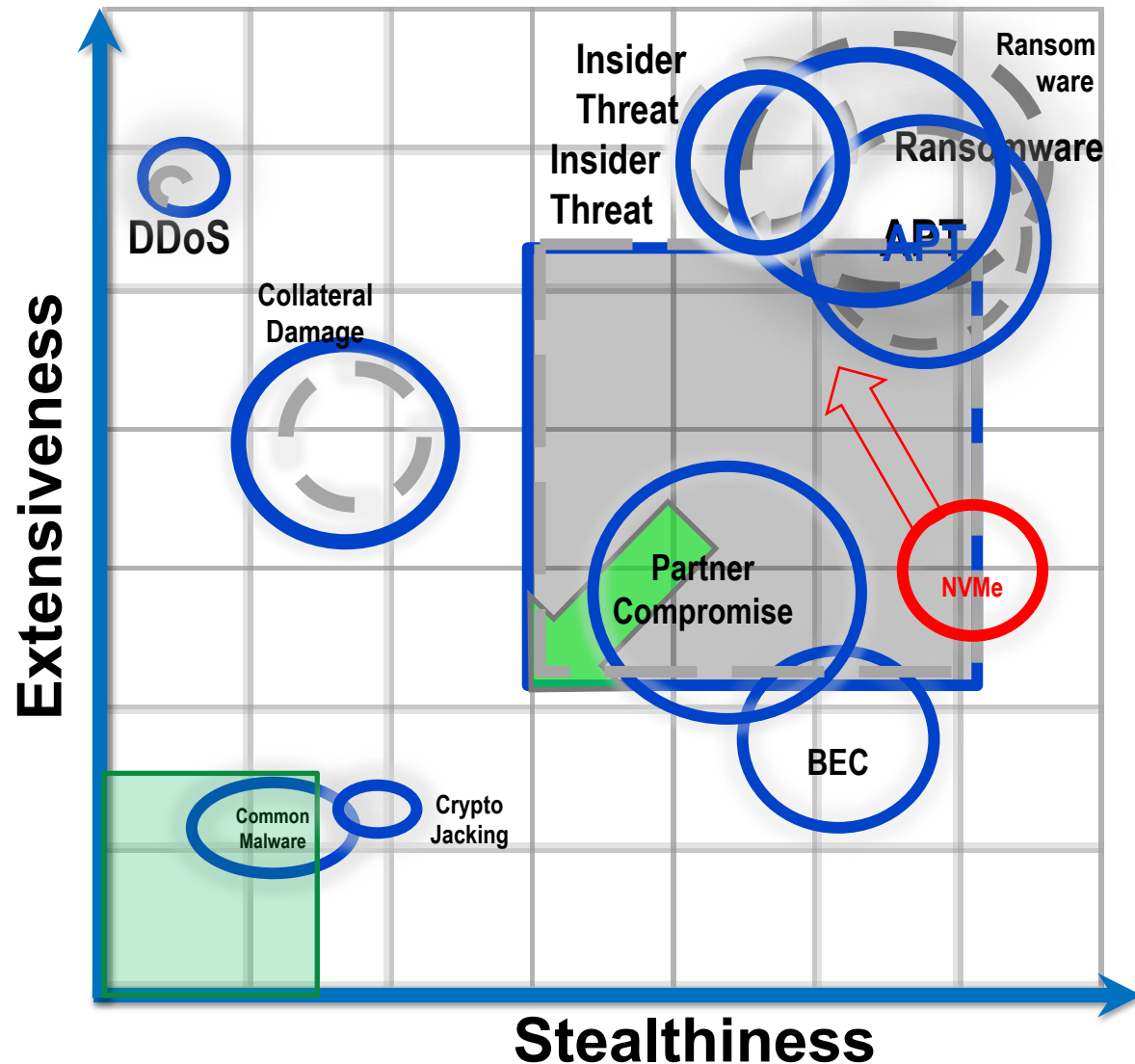
- Stuxnet, 2010: **USB Thumb Drives**
- Super Micro, 2010, 2014, 2015: **Hardware, Software**
- SolarWinds, 2020: **Software Supply Chain**
- MoonBounce, 2022: **Firmware**

NIST Special Publication
NIST SP 800-161r1

**Cybersecurity Supply Chain Risk
Management Practices for Systems
and Organizations**



A 2022 Q3 Cybersecurity Risk Register



This framework embodies the NIST 800-30 risk assessment process. The organizational goal is to reduce aggregate threat surface area (grey square) and move the threats toward the bottom left. Green square is target, i.e., at 5% total risk of incident per quarter. Size corresponds to **Likelihood**. Position corresponds to **Impact**.

Size of threat is calculated based on attack frequency, defensive posture, and recent history. Prominence of threat is distance from origin times size.

This example reflects a NIST 800-171 compliant conglomerate organization of ~20,000 employees. NVMe and related attack chains current and anticipated future arc are shown in red.



Agenda: End to End NVMe Debugging

DMA and Firmware level attacks:

- Firmware role in the operating system
- DMA and load time risks
- DMA attacks

Zero Trust

- What is Zero Trust
- What does Zero Trust mean in terms of DMA attacks

Recommended actions to implement a robust security model

- Applying Zero Trust to upstream supply chain
- Applying Zero Trust to OEM/SI product development
- Applying Zero Trust to the downstream channel



Flash Memory Summit

↑
OS

2

OS





↑ \$147B

-
- 15-20 for each endpoint
 - 30 or more for each server
 - Critical to **every** network devices

\$0



By 2022
70%
of organizations
will be breached

“firmware may be
the next endpoint
battleground”



2000%

increase in VPN attacks
focused on firmware



In the last 2 years

88%

have experienced
a firmware attack





Identify

- Discover devices, servers, endpoints and their firmware
- Build profiles through sub-OS visibility across the network
- Identify firmware and version details for all critical sub-components



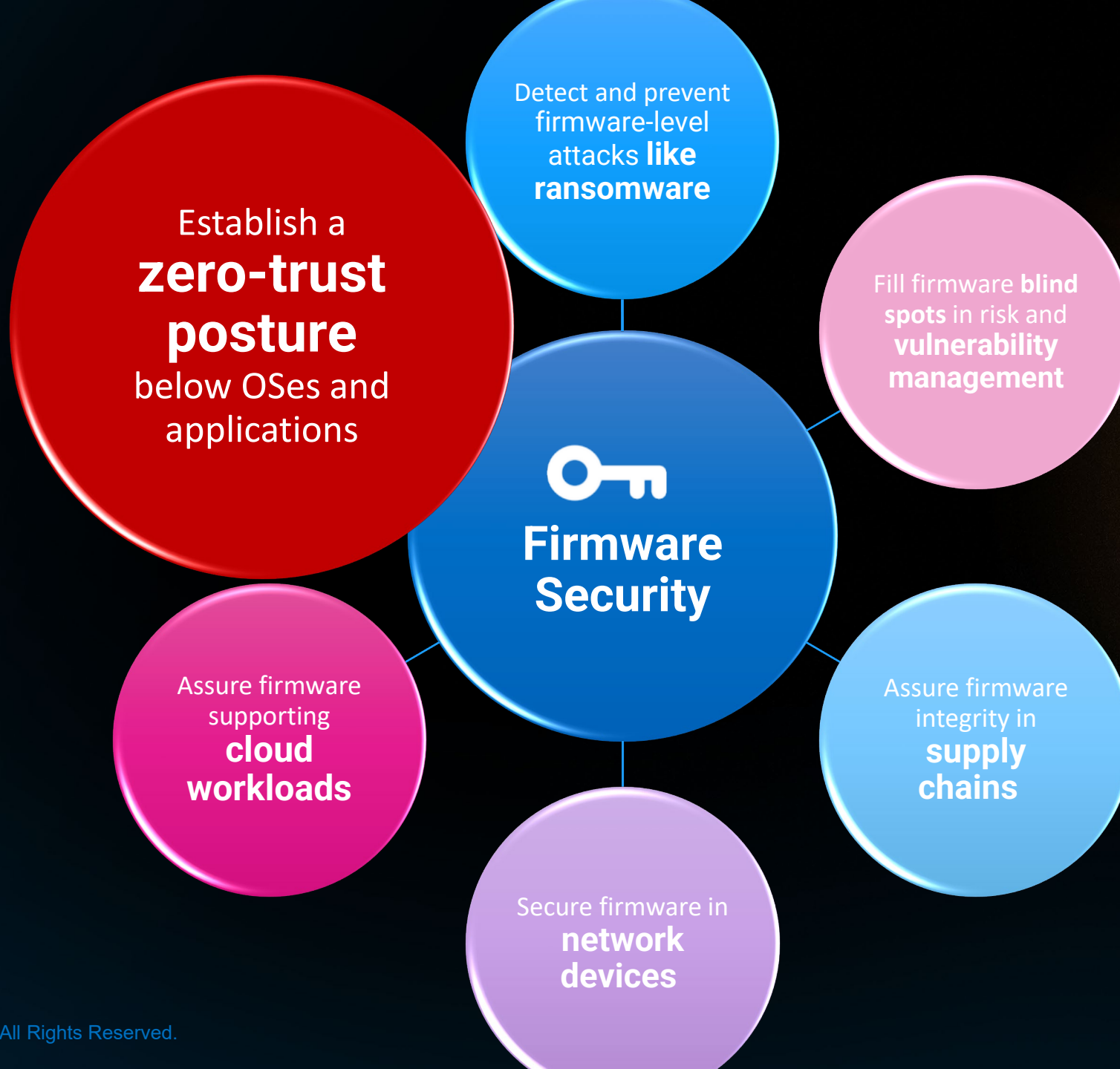
Verify

- Verify against the world's largest firmware database
- Assure integrity and validate baseline details
- Assess and score compliance
- Inventory, classify and prioritize any anomalies



Fortify

- Set a known-good configuration state
- Orchestrate firmware patching and repair
- Automate firmware updates
- Provide actionable alerts on new threats



What is Zero Trust

What does it mean as a government supplier...



1 Default Deny

2 Contextual

3 Granular

4 Dynamic

1 Default Deny

No Inherited Permissions

- Treat every session as a new session, with a new system and a new actor
- Any object joining the network requires its own verification process
- This applies to people, devices, compute systems, and sub-networks



2 Contextual

Not Just “Yes” or “No” ... But *Maybe*

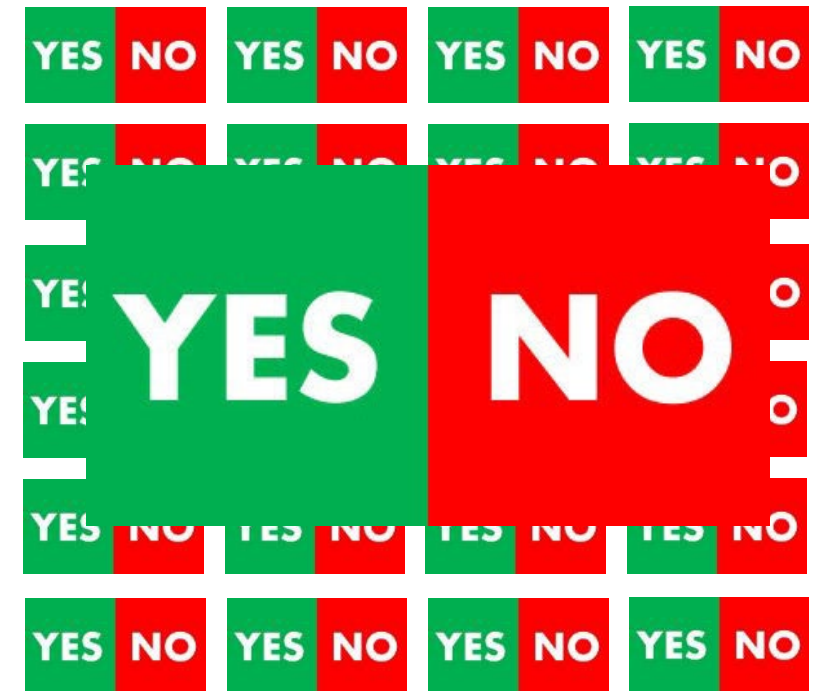
- *Relative **risk*** is a critical measure
- *Relative **value*** is an even more critical measure
- Not every person, system or component can be treated equally
- Prioritize your assets and accounts
- Develop multi-layer tests for authenticity



3 Granular

Many, Many Yes or No Decisions

- Not one “Yes” or “No”, but many
- Break access, connection and permission requests down to the smallest possible pieces
- Each is definitive
- The stream of requests will probably be continuous (see the next point)



4 Dynamic

Faster Than We Ever Imagined

- Digital transformation changed the pace
- We need to make these decisions many times an hour with an absurd number of systems and workloads
- We need to manage fleets of thousands of machines and connected devices
- Take less time to do it all and manage the element of *randomness*



1

Default Deny

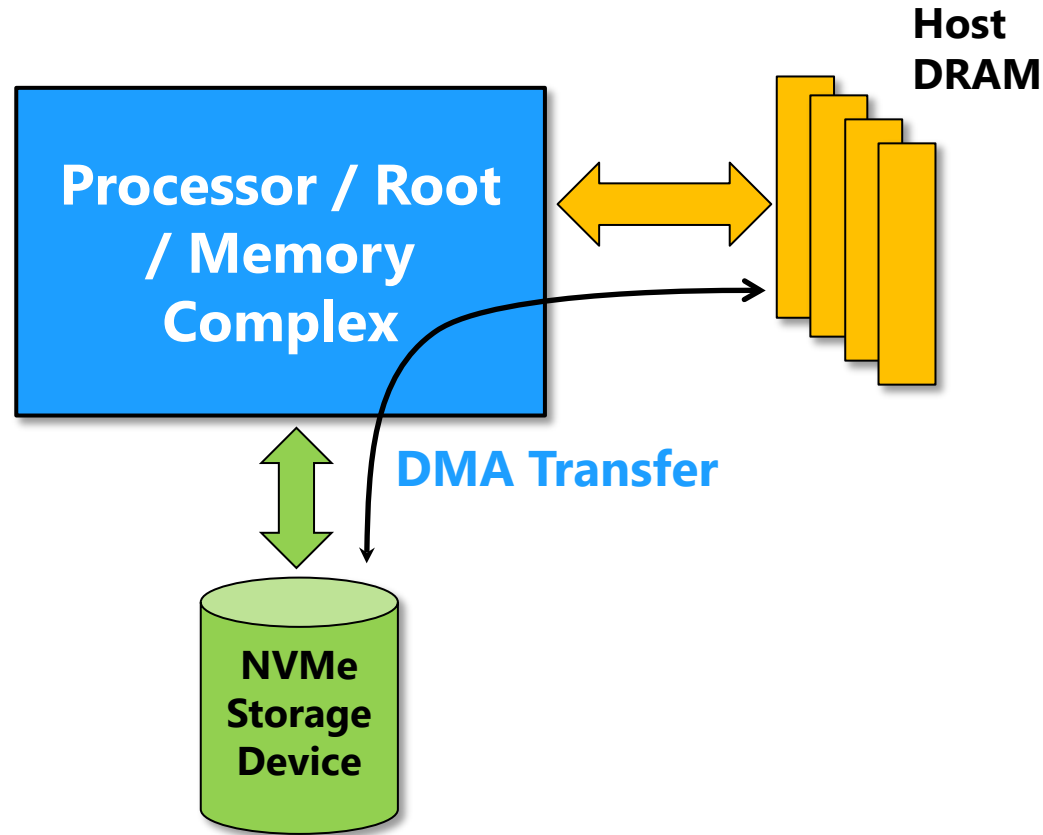
We can't assume trust in our components



The Importance of the SBOM

- The **Software Bill of Materials** becomes the standard for provenance and legitimacy
- It tracks and verifies the libraries, sub-systems, components and parts in complex software
- The SBOM is evolving to include the **FBOM**: the Firmware Bill of Materials

Problem Statement: NVMe and Potential DMA Attacks



Potential Problems

- How do you mitigate risk in an architecture **based on trust**?
- Actual memory accessed by SSD is transparent to processor
- “Trusted Model” – SSD is expected to honor the PRP/SGL Descriptors
- Processor “expects” device to be PCIe/NVMe spec compliant

2

Contextual

Understand and weigh concepts of risk

A



What you need to know

- BMC components in HPE Gen8 and Gen9 servers are actively under attack
- Control over this chip can brick the most critical servers and wipe data
- It's very difficult to determine which systems are compromised



B



What you need to know

- 30 million units across 29 different models
- Which ones are used in high-risk activities or by privileged accounts?

3

Granular

Apply zero trust principles to all components

1



CPU

2



ME/Chipset

3



Network cards

4



BMC

5

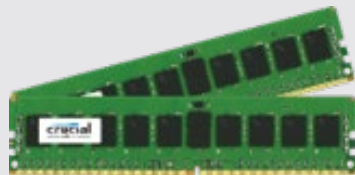


BIOS / UEFI

6



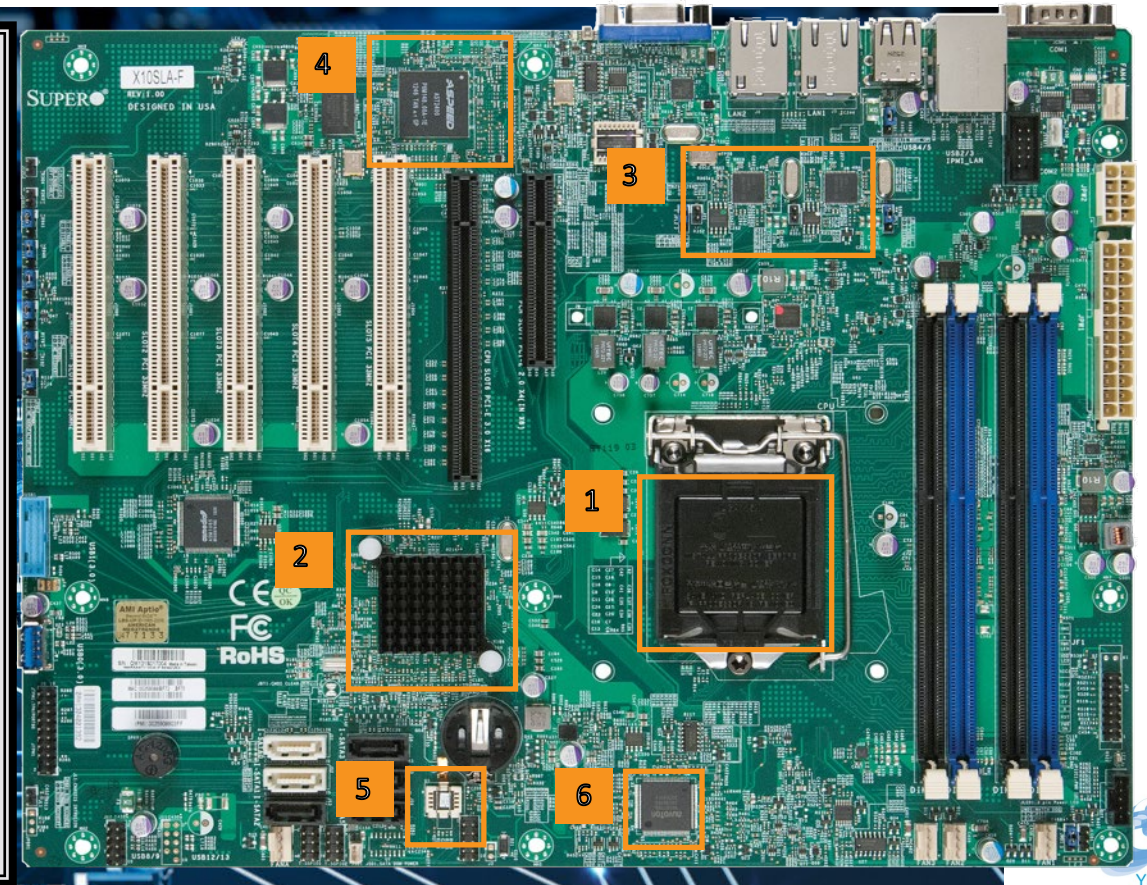
Embedded controllers



RAM / Memory



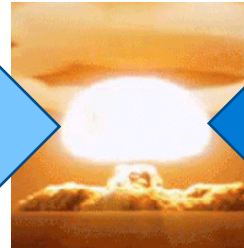
SSD/HD



4 Dynamic

Solve for speed & scale through *automation*

DIGITAL TRANSFORMATION WITH
CLOUD SCALE GROWTH



ZERO TRUST
PRINCIPLES AND PRACTICES

Automation is the answer

- Lifecycle automation of sub-OS firmware and hardware components...
- Driven by a reliable, repeatable process that manages firmware at enterprise scales

- Search and Discover
- Catalogue
- Inventory

Identify

Verify

- Assess vulnerabilities
- Assure integrity and authenticity

- Configure securely
- Update regularly
- Patch as needed

Fortify

Summary

1 Default Deny We can't assume trust in our components

2 Contextual Understand and weigh concepts of risk

3 Granular Apply zero trust principles to all components

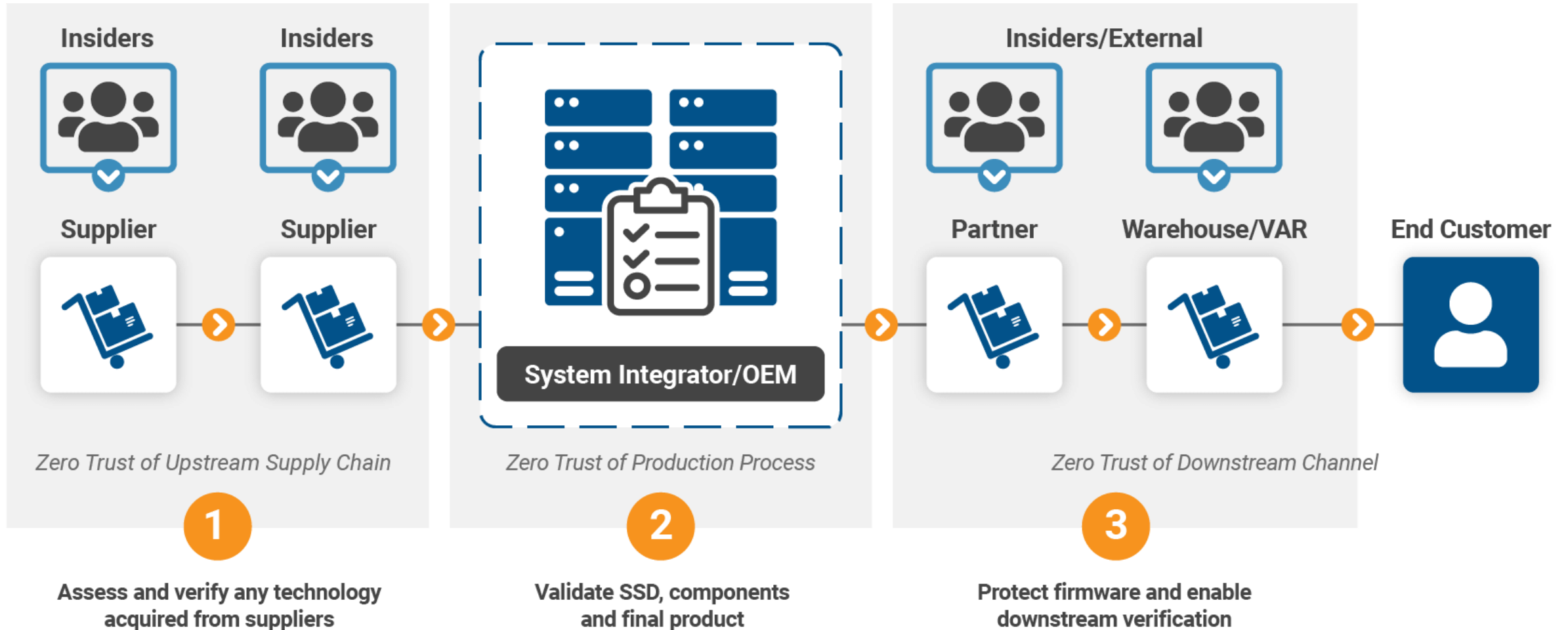
4 Dynamic Solve for speed & scale through *automation*



What can be done

Steps to take across the supply chain...

Trust Should be Implemented Across the Value Chain



Zero Trust Best Practices

Action within Supply Chain	Action for SI/OEM	Actions for Channel
Define the security requirements and expectations of all suppliers	Perform supplier Audits	Verify firmware-level protections and security configurations: Any installed firmware properly signed
Validate suppliers scan outsourced components and firmware for known vulnerabilities and misconfigurations	Repeat scan to verify the integrity of firmware and to identify known vulnerabilities and threats	Establish SBOMs for critical firmware checklist for whenever systems are removed and replaced from box.
Verify integrity of received firmware (Secondary Supplier SBOM)	Observe firmware-level behavior and test for anomalies	Set security requirements for downstream channel partners
Implement Robust Validation Policies	Incorporate Firmware BOM into a System Wide BOM	

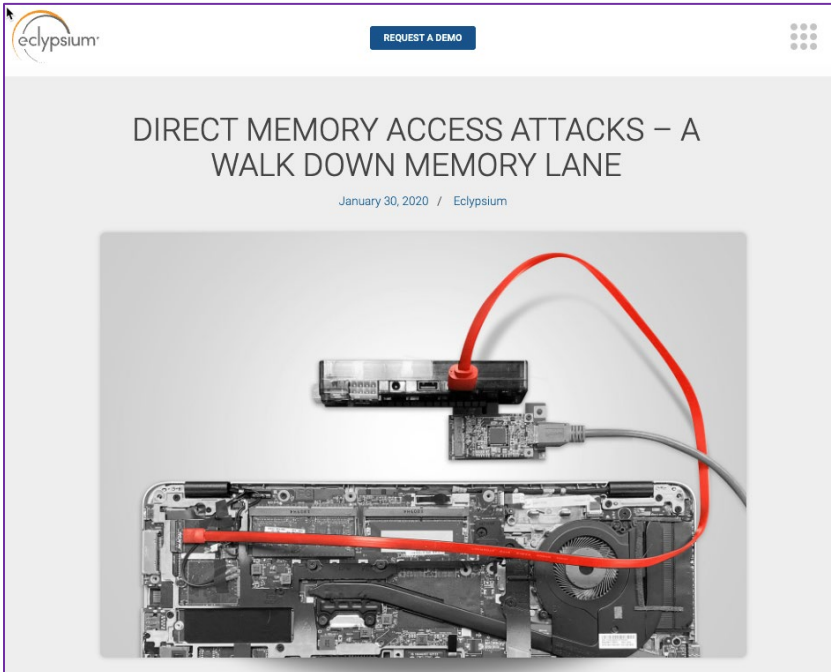
Eclipsium Provides Threat Intelligence, Advice and Tools



Flash Memory Summit

DMA firmware guidance

- A detailed blog post on current attack techniques
- White paper on remediation, repair and mitigation practices
- Built-in product guidance



DEFENDING THE FOUNDATION
OF THE ENTERPRISE

works at this critical time, and has the potential to completely compromise a system, even when other code integrity protections (like HP Sure Start, Intel Boot Guard, or Microsoft Virtualization Based Security with Device Guard) are employed. Extending these protections to also cover DMA attacks is possible, but not necessarily in place on systems already in use.



While the overall process was relatively straightforward, the attack **did require us to open the case of the device**. As noted earlier, such an open-chassis DMA attack would raise the risk from an attacker's perspective, but would still remain plausible for a dedicated adversary.

Once the device was opened, we simply replaced the M.2 wireless card in the system with a Xilinx SP605 FPGA development platform. The FPGA was then connected to our attacking machine and tested the system against a well-known, **public DMA attack technique**. We were able to successfully attack the system and gain control over the device. By using DMA to modify the system RAM during the boot process, we gained arbitrary code execution, thus bypassing the HP Sure Start protections that verify BIOS code integrity before CPU execution starts.



While we specifically tested against the HP ProBook 640 G4 - a new model, available for purchase online still today - it is likely that other laptops are also similarly vulnerable. In fact, pre-boot processes are an area of weakness across all laptops and servers from many manufacturers. In the case of HP, while the machine was not susceptible to a closed-case attack, the version of HP Sure Start in the mode we tested was insufficient to protect against our type of attack. There are many components, from hardware to firmware to the operating system, that all need to work together to prevent pre-boot DMA attacks.

VENDOR MITIGATIONS

HP Sure Start Gen4 and earlier generations of devices didn't include DMA attacks in the threat model. HP Sure Start Gen5 added IOMMU based protection for closed-chassis DMA attacks via Thunderbolt, and in response to our research, HP decided to extend the HP Sure Start Gen5 threat model to now include and protect against open-chassis DMA attacks.

HP released an **updated version of the BIOS** on January 20, 2020.

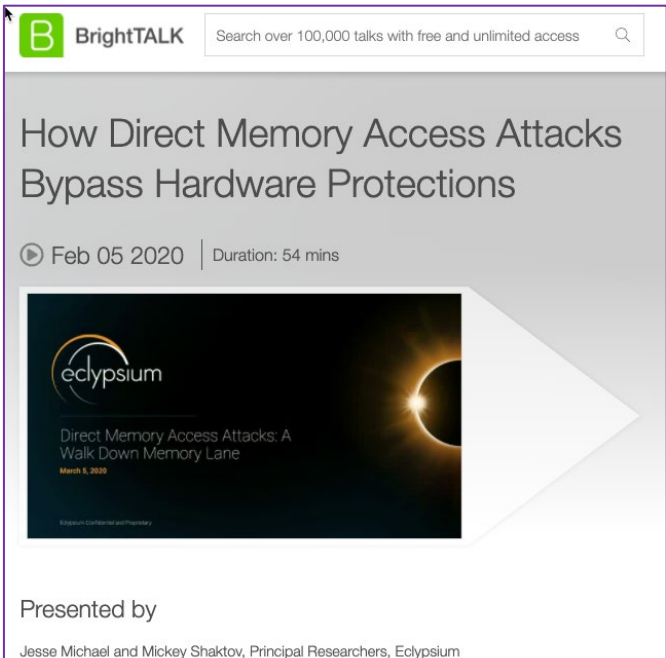
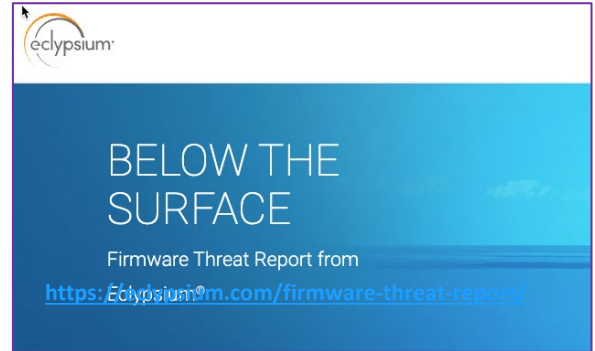
HP has provided Eclipsium with an HP EliteBook 840 G6 that includes the most recent generation of HP Sure Start (Gen 5) and the latest version of BIOS (01.04.02 released on January 20th 2020). The device with this latest version of BIOS successfully protects against our attempts at open-chassis DMA attacks. We performed a number of tests with this latest version of the HP firmware and with the "pre-boot DMA protection" option set to "Thunderbolt only", we were able to reliably get arbitrary code execution during the boot process via DMA using the PCI Leech through the NVME M.2 card slot. However, after setting this option to "Thunderbolt and PCIe expansion card", we made multiple attempts to initiate DMA transactions with the PCI Leech and all attempted DMA read operations failed. When enabled, these new protections appear to mitigate the pre-boot DMA attack or minimize the window so that we weren't able to perform the attack.

SOFTWARE AND REMOTE DMA ATTACKS

It is important to note that DMA is a powerful technique that does not necessarily require the attacker to have physical access to the device. In fact, data centers and cloud environments can be at the greatest risk for remotely enabled DMA attacks.

Parallel computing clusters often need to share large volumes of information between systems with extremely low latency. In the same way that DMA allows fast direct access between peripherals and system memory on a device, Remote DMA or RDMA provides similar direct access to memory between devices over Ethernet and other network interconnects. And once again, this direct access to memory can provide an avenue for attack. The **Throwhammer** exploit developed by VUSec provides a perfect example. In the case of Throwhammer, the VUSec team notes that:

©2020 Eclipsium, Inc.



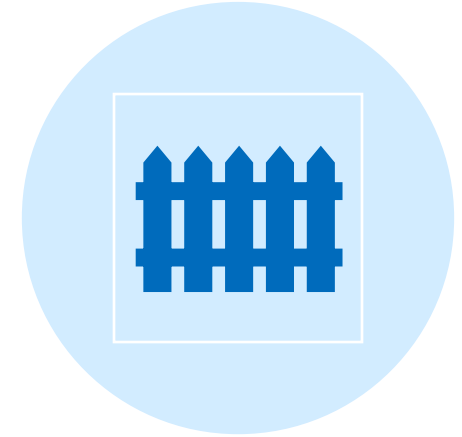
How OakGate helps Firmware-level Behavior and Test



OCP BASED DIRECTED TESTS
TO ENSURE YOUR DRIVE
MEETS THE OCP SPEC



FIRMWARE DOWNLOAD
CAPABILITY TO VALIDATE THE
FIRMWARE DOWNLOAD
PROCESS



MEMORY FENCING
TECHNOLOGY TO IDENTIFY
WHEN/IF THE SSD HAS
VIOLATED THE MEMORY
MAPPING

What's New? OCP – Open Compute Project



Flash Memory Summit

- ✓ Validation against the Datacenter NVMe SSD Specification ensures the target device complies with the wide array of common requirements across multiple datacenter customers
 - ✓ Common & deterministic SSD functionality in-system
 - ✓ Numerous datacenter opportunities from one leveraged SSD design



OPEN
Compute Project

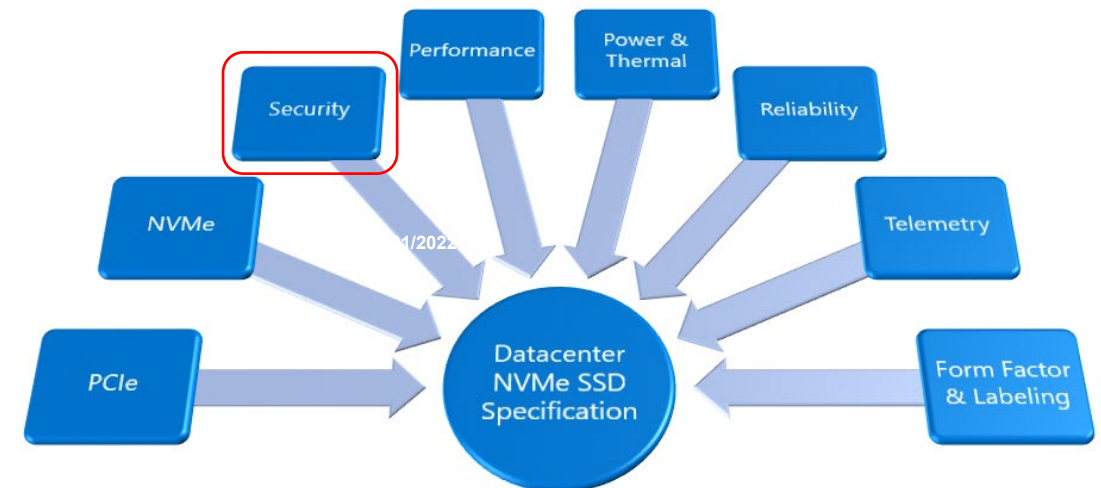
Teledyne LeCroy
8,684 followers
7mo •

Need #OCP #Cloud #SSD Qualification #Testing? #TeledyneLeCroy's #AustinLabs has the solution! Click <https://lcry.us/3vgSlkQ> to learn more.
#TestingServices #OpenComputeProject #PCIe #PCIExpress #NVMe

Austin Labs
TELEDYNE LECROY

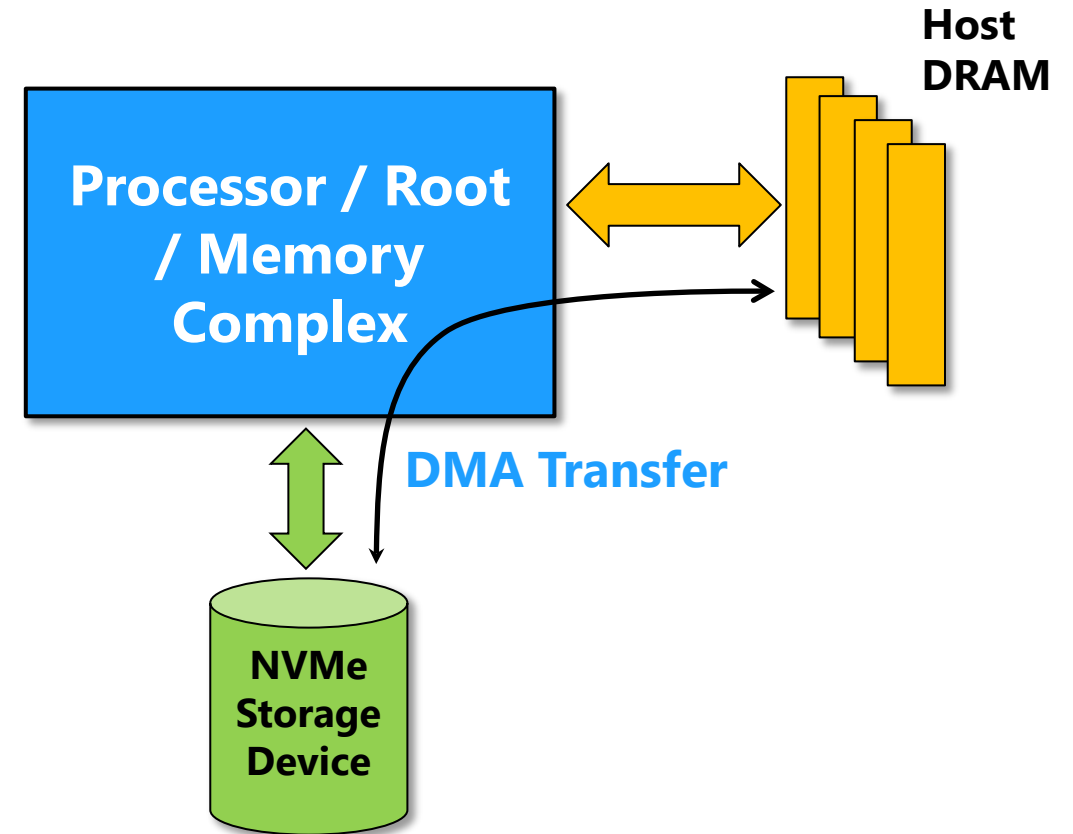
Open Cloud Project (OCP)
SSD Cloud Testing Services

TELEDYNE LECROY
Everywhere you look



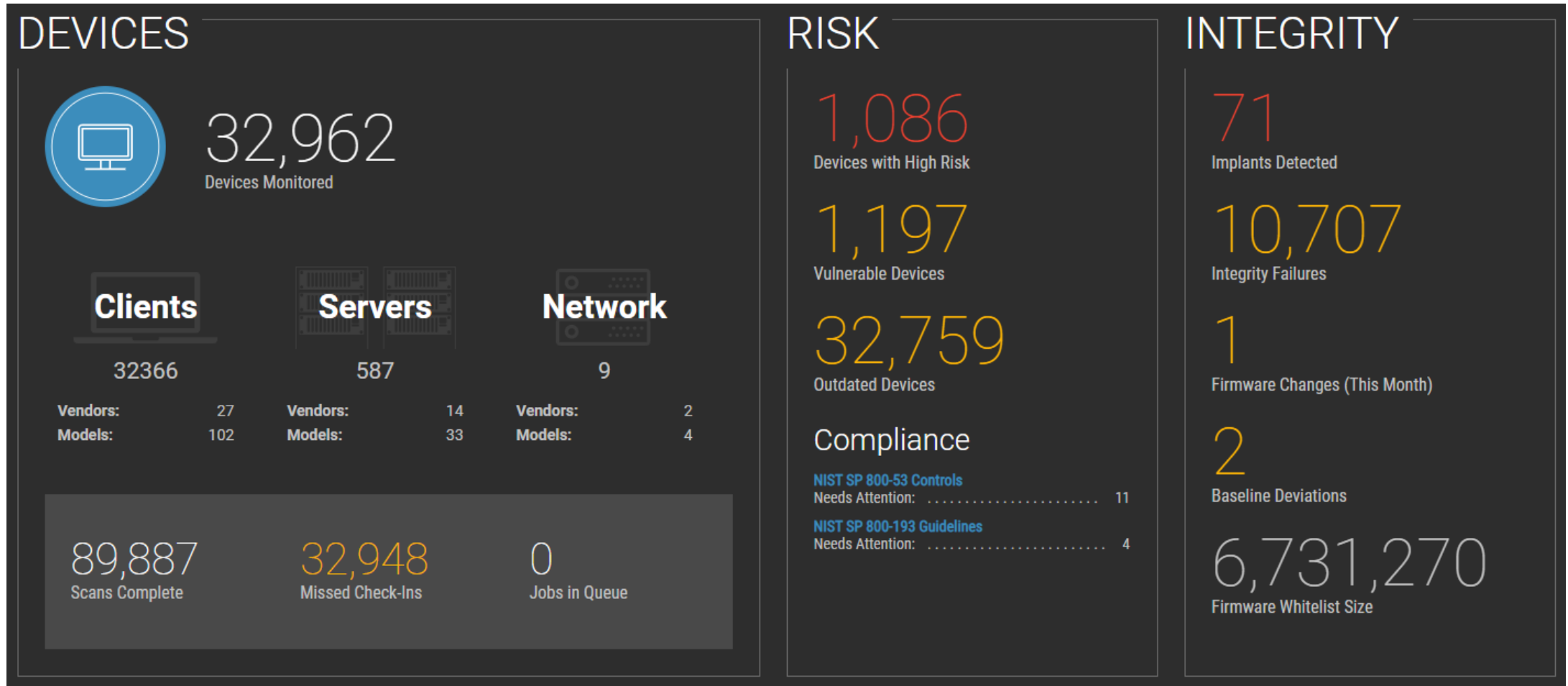
OakGate Memory Fencing Solution

- The Teledyne LeCroy OakGate Test Appliance detects functional errors that occur when a device with a Direct Memory Access (DMA) engine accesses memory space outside of the area specified by the device driver
- With OakGate's IO Exerciser users can create simulated workloads that simulate the lifetime use of a drive including safe and unsafe power cycles.
- OakGate's Replay capability also let's users replay real world workflows against the drive to simulate actual use.



Eclypsium Creates an SBOM That Includes Firmware

Using the Eclypsium Platform for firmware security



Eclypsium Creates an SBOM That Includes Firmware

Using the Eclypsium Platform for firmware security

Component Firmware

DRAC (Dell Remote Access Controller) Version: 38.5 Date: December 16, 2020 [HASH](#)

SATA drives

Version: 7004 Date: January 21, 2021 [HASH](#)

This package contains the firmware for Intel SSDPEMKF256G8 256 GB, SSDPEMKF512G8 512 GB, and SSDPEMKF010T8 1 TB solid-state drives, revision 7004. Storage firmware is a microcode that is embedded on storage devices such as hard drives or solid-state drives. The firmware manages the functionality of the devices.

Version: 1115.0012 Date: January 11, 2021 [HASH](#)

This package contains the firmware for the Western Digital Corp SN730 256 GB, 512 GB, and 1 TB, Revision 11150012. Storage firmware is a microcode that is embedded on storage devices such as hard drives or solid-state drives. The firmware manages the functionality of the devices. It is recommended that you update this firmware using Dell Update or Dell Command Update.

Version: 7004 Date: January 21, 2021 [HASH](#)

This package contains the firmware for Intel SSDPEMKF256G8 256 GB, SSDPEMKF512G8 512 GB, and SSDPEMKF010T8 1 TB solid-state drives, revision 7004. Storage firmware is a microcode that is embedded on storage devices such as hard drives or solid-state drives. The firmware manages the functionality of the devices.

System Firmware



Vendor: Dell
Model: latitude-14-5480-laptop
Current Version:
1.3.3

Firmware: **Outdated**
Days since update: 1262
Date:
May 8, 2017

To update this device's firmware, please check, download and install updates from the vendor website.
System firmware update package includes updates for UEFI firmware and other components on your device.



New Version:
1.18.2

Date:
October 20, 2020

[HASH](#)



CVEs Fixed in this Update: CVE-2018-3655, CVE-2017-5705, CVE-2019-11100, CVE-2019-0166, CVE-2018-12200, CVE-2019-11131, CVE-2019-11090, CVE-2017-13080, CVE-2018-3629, CVE-2019-11135, CVE-2018-12190, CVE-2019-0094, CVE-2019-0154, CVE-2019-0165, CVE-2018-3639, CVE-2018-3616, CVE-2018-12127, CVE-2019-0117, CVE-2018-12167, CVE-2018-12199, CVE-2019-11132, CVE-2019-0170, CVE-2019-11088, CVE-2017-13078, CVE-2017-5715, CVE-2019-11147, CVE-2019-11104, CVE-2018-12196, CVE-2018-12198, CVE-2018-12185, CVE-2018-12203, CVE-2019-14607, CVE-2019-0090, CVE-2018-12191, CVE-2018-12130, CVE-2019-11091, CVE-2018-3632, CVE-2017-13077, CVE-2019-0153, CVE-2019-11157, CVE-2019-0169, CVE-2019-0093, CVE-2018-12201, CVE-2017-5712, CVE-2019-11087, CVE-2018-3627, CVE-2018-12192, CVE-2018-3636, CVE-2018-3628, CVE-2019-11101, CVE-2019-0168, CVE-2018-12188, CVE-2019-0092, CVE-2019-0096, CVE-2018-3640, CVE-2018-3643, CVE-2018-3644, CVE-2018-3657, CVE-2017-5711, CVE-2017-5708, CVE-2019-11106, CVE-2019-0086, CVE-2019-0091, CVE-2019-0098, CVE-2019-0097, CVE-2018-12126, CVE-2019-0131, CVE-2019-0123.

Change Logs

SATA drives

Thunderbolt controller

Version: 4.40.33.001 Date: May 13, 2019 [HASH](#)

TPM (Trusted Platform Module)

Version: 5.81.2.1 Date: August 20, 2017 [HASH](#)

Eclypsium Creates an SBOM That Includes Firmware

Using the Eclypsium Platform for firmware security

Hash ?	GUID	Name	Reputation Check	Code Anomaly Check
hash	Enter GUID	Enter name		
e85b2...7 ... a0aef2e1	BDCE85BB-FBAA-4F4E-9264-501A2C249581	(blank)	Failed	Failed
fba1190f ... 1f3ee26c	90CB75DB-71FC-489D-AACF-943477EC7212	(blank)	Ok	Ok
fbcb13c9 ... f32e012e	D95D6B4F-92FA-4E78-9C48-C68C0813688E	(blank)	Ok	Ok
fbcb7b4e5 ... 0ffcb0763	8F0B5301-C79B-44F1-8FD3-26D73E316700	(blank)	Ok	Ok
f86cfd27 ... 6f9bfc3f	DC571B6D-D570-4862-A95F-299B28FDC2D2	(blank)	Ok	Ok
f8b0136d ... 15da25f0	43E7ABDD-E352-4CFB-A230-4CDC1D350E5C	(blank)	Ok	Ok
f8d2839c ... 34fea04b	571D1ED1-C2D9-418E-953A-248EBC687048	(blank)	Ok	Ok
facb9c75 ... 7380c203	038CE287-B806-45B6-A819-514DAF4B91B9	(blank)	Ok	Ok
d15ae43e ... d2a378e7	628A497D-2BF6-4264-8741-069DBD3399D6	(blank)	Ok	Ok
d1d18f39 ... ccf203bd	89E549B0-7CFE-449D-9BA3-10D8B2312D71	(blank)	Ok	Ok

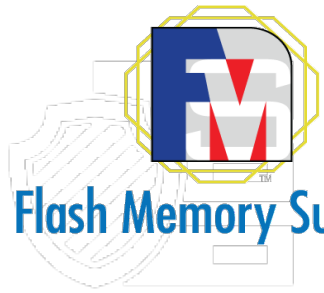
Show 1 - 10 of 523

10

< < > >

In Summary:

- DMA-level firmware **provides unique threat risks** that vendors concerned with Zero Trust must consider and plan for
- Mitigation strategies **should protect against “insider threats”** within downstream suppliers and threats that may occur within delivery channels to your customers
- Teledyne LeCroy and Eclypsium **provide hardware-based and software-based solutions** for the challenges of managing hardware- and firmware-level risks



SNIA STORAGE
SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

Flash Memory Summit

Questions

Contact Teledyne LeCroy



Flash Memory Summit



Summit M5x Analyzer/Jammer
Gen 4 up to x16 (Gen 5 Capable up to x8)



Summit T416 Analyzer
Gen 4 up to x16



Summit T516 Analyzer
Gen 5 x16



Summit T3-16 Analyzer



Summit T54 Analyzer
Gen 5 up to x4



Summit T48 Analyzer
Gen 4 up to x8



Summit Z416 Exerciser
Gen 4 up to x16



Summit T28 Analyzer



Summit T3-8 Analyzer



Summit T3-16 Exerciser
with Test Platform



Summit Z516 PCIe 5.0/CXL Exerciser
Gen 5 up to x16



Summit Z58 5.0 Exerciser/Analyzer
Gen 5 up to x8

PCI 
EXPRESS®

38 | ©2022 Flash Memory Summit. All Rights Reserved.

Email Sales: protocolsales@teledynelecroy.com

Phone Support: 1-800-553-2769

www.teledynelecroy.com

Flash Memory
INNOVATION