Flash Memory Summit

OakGate and Eclypsium: Zero Trust Capabilities

Presented by:

Corey Hirsh, Teledyne

Dave Obert, Teledyne LeCroy

Michael Thelander, Eclypsium

About the Presenters

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

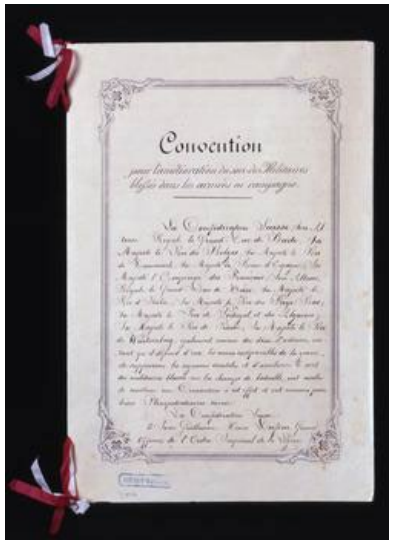
David Obert

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

- 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***

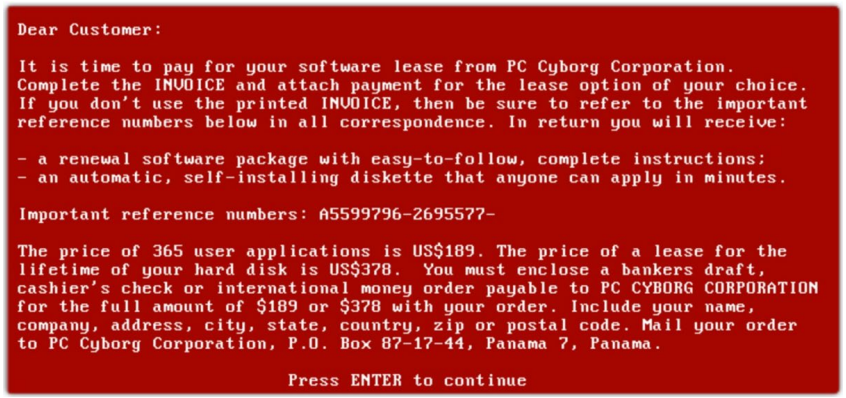


Gerasimov Doctrine and Logic-Bearing Componentry:

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



- 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!)

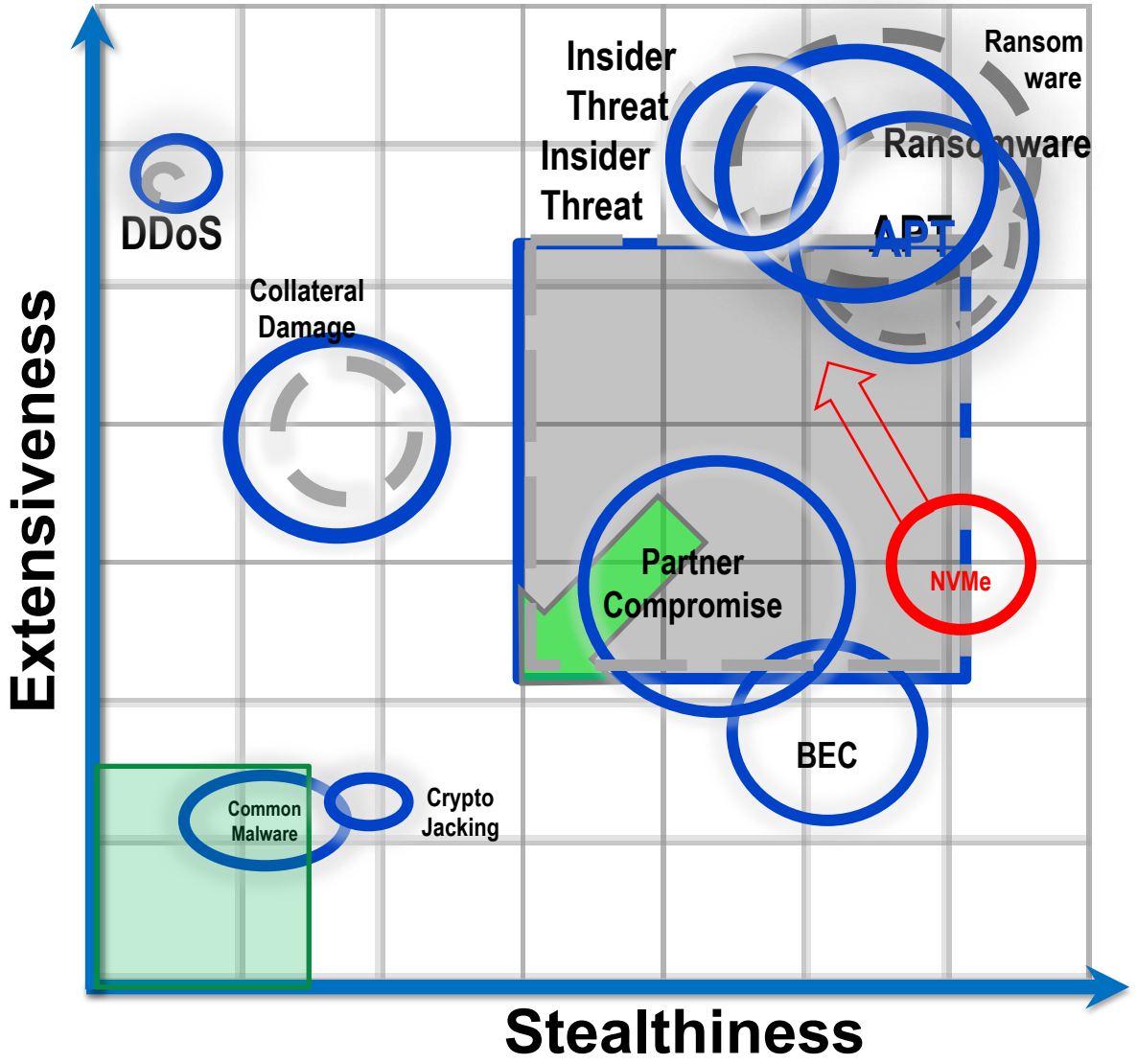
- Stuxnet, 2010: **USB Thumb Drives**
- Super Micro, 2010, 2014, 2015: **Hardware, Software**
- SolarWinds, 2020: **Software Supply Chain**
- MoonBounce, 2022: **Firmware**

NIST Special Publication
NIST SP 800-161r1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

35 YEARS OF NAND FLASH MEMORY INNOVATION

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

Flash Memory Summit

DMA and Firmware level attacks:

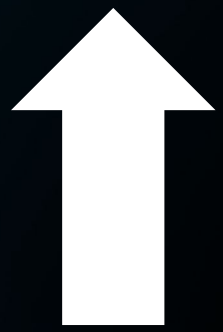
- Firmware role in the operating system
- DMA and load time risks
- DMA attacks

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



$147B

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

$0

Gartner

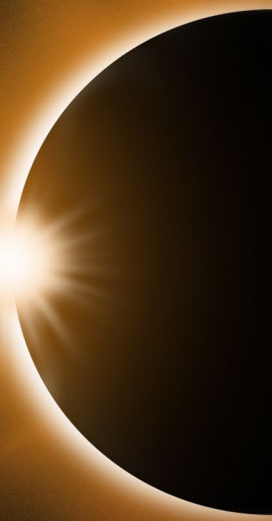
Flash Memory Summit

By 2022

70%

of organizations will be breached

"firmware may be the next endpoint **battleground**"



35 YEARS OF NAND FLASH MEMORY INNOVATION

2000%

increase in VPN attacks focused on firmware

HELPNETSECURITY

In the last 2 years

88%

have experienced a firmware attack

VansonBourne

eclypsium

Identify

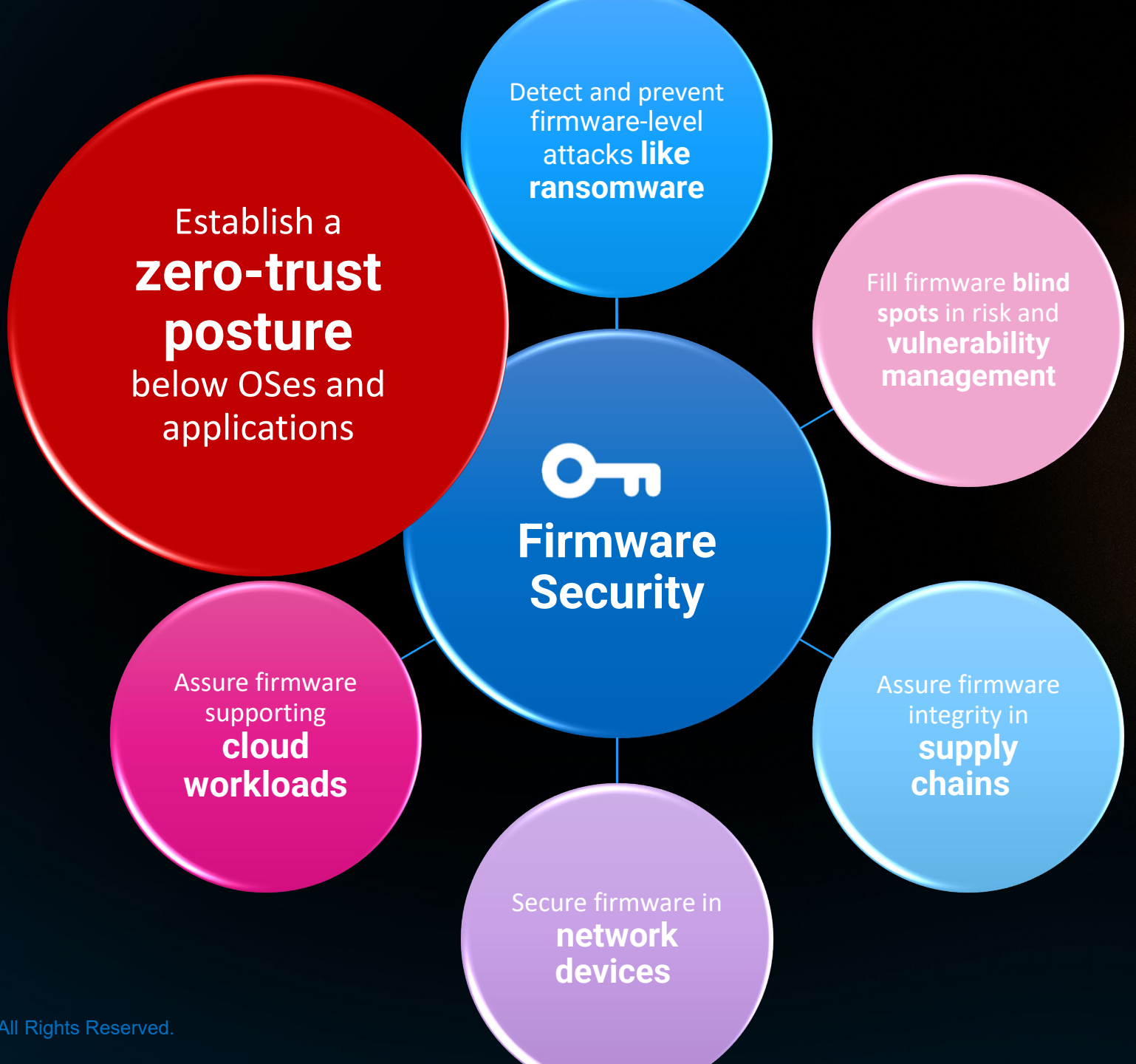
- Discover devices, servers, endpoints and their firmware
- Build profiles through sub-OS visibility across the network
- Identify firmware and version details for all critical sub-components

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
THE WHITE HOUSE
WASHINGTON
eclypsium.com

Breaking Down Zero Trust

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

Breaking Down Zero Trust

Flash Memory Summit

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

35 YEARS OF NAND FLASH MEMORY INNOVATION

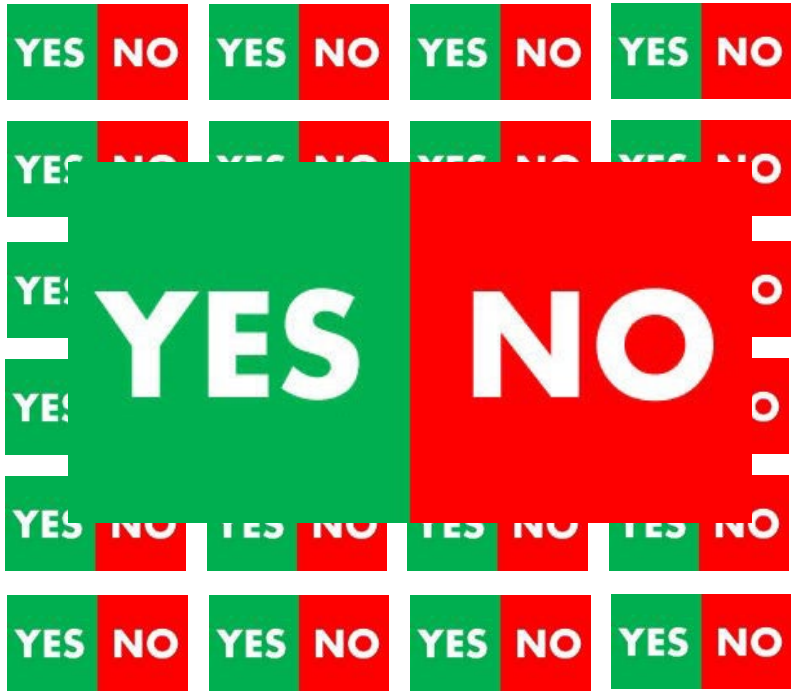
Breaking Down Zero Trust

Flash Memory Summit

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)



35 YEARS OF NAND FLASH MEMORY INNOVATION

Breaking Down Zero Trust

Flash Memory Summit

4 Dynamic

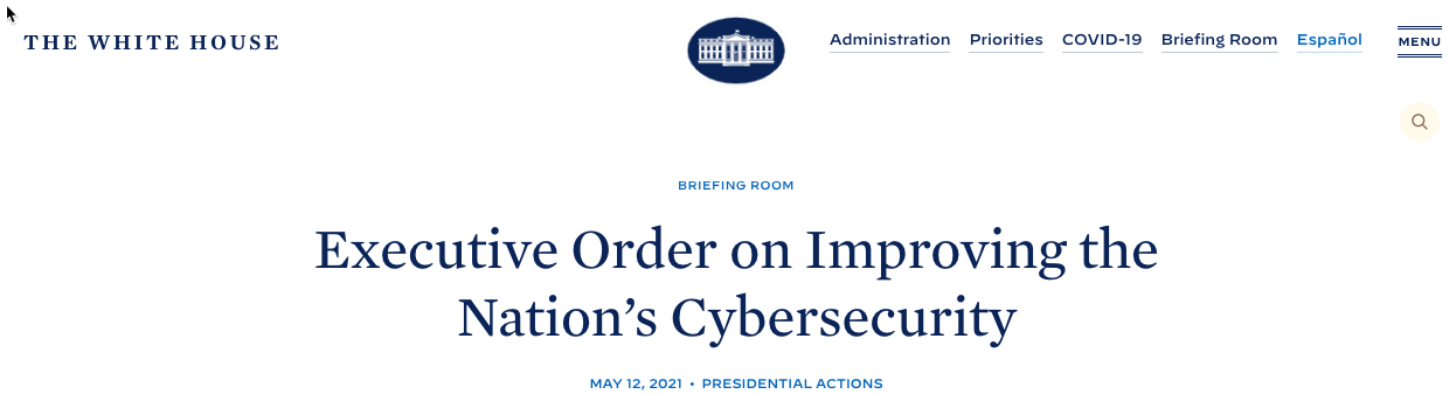
Faster Than We Ever Imagined

- 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*

Zero Trust and Firmware

Flash Memory Summit

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

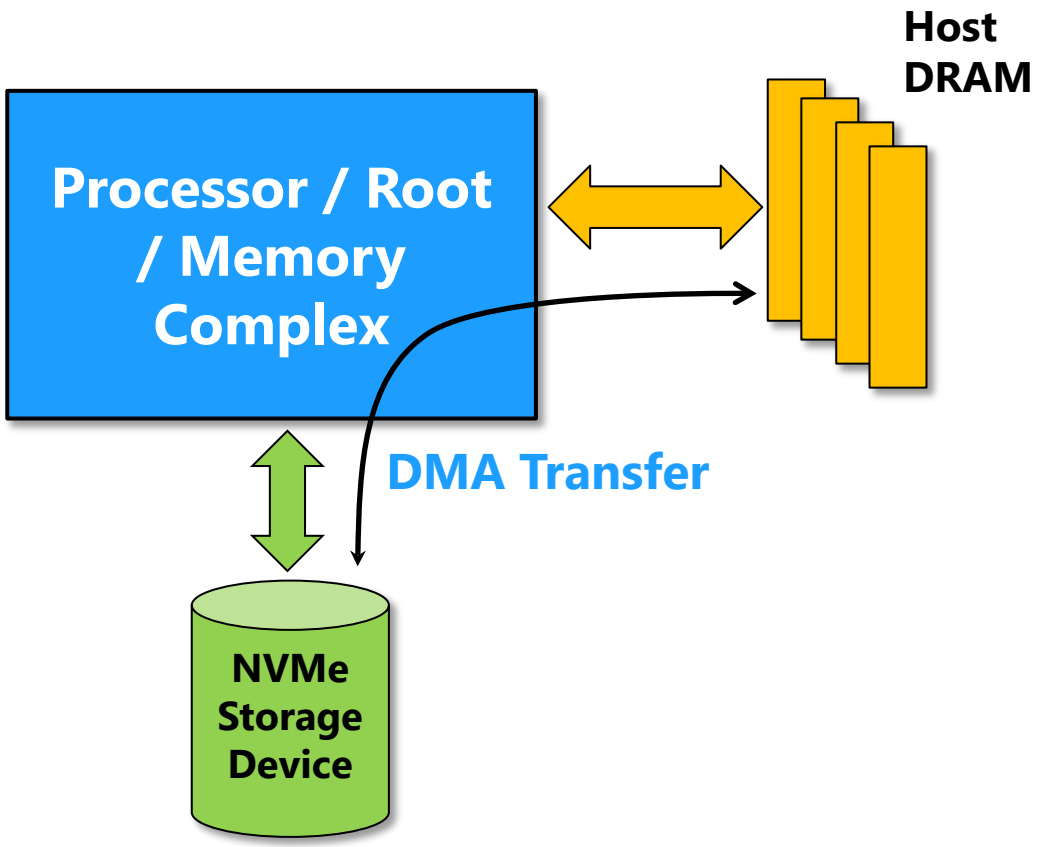


The Importance of the SBOM

- 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

35 YEARS OF NAND FLASH MEMORY INNOVATION

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

Zero Trust and Firmware

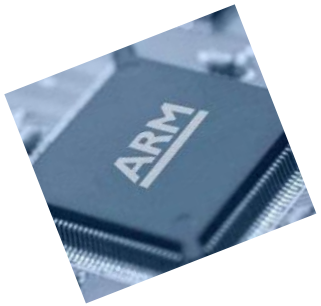
Flash Memory Summit

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?

Zero Trust and Firmware

Flash Memory Summit

3 Granular

Apply zero trust principles to all components

1 CPU

2 ME/Chipset

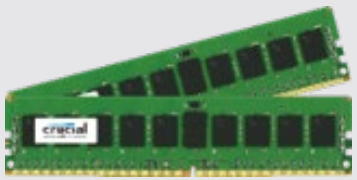
3 Network cards

4 BMC

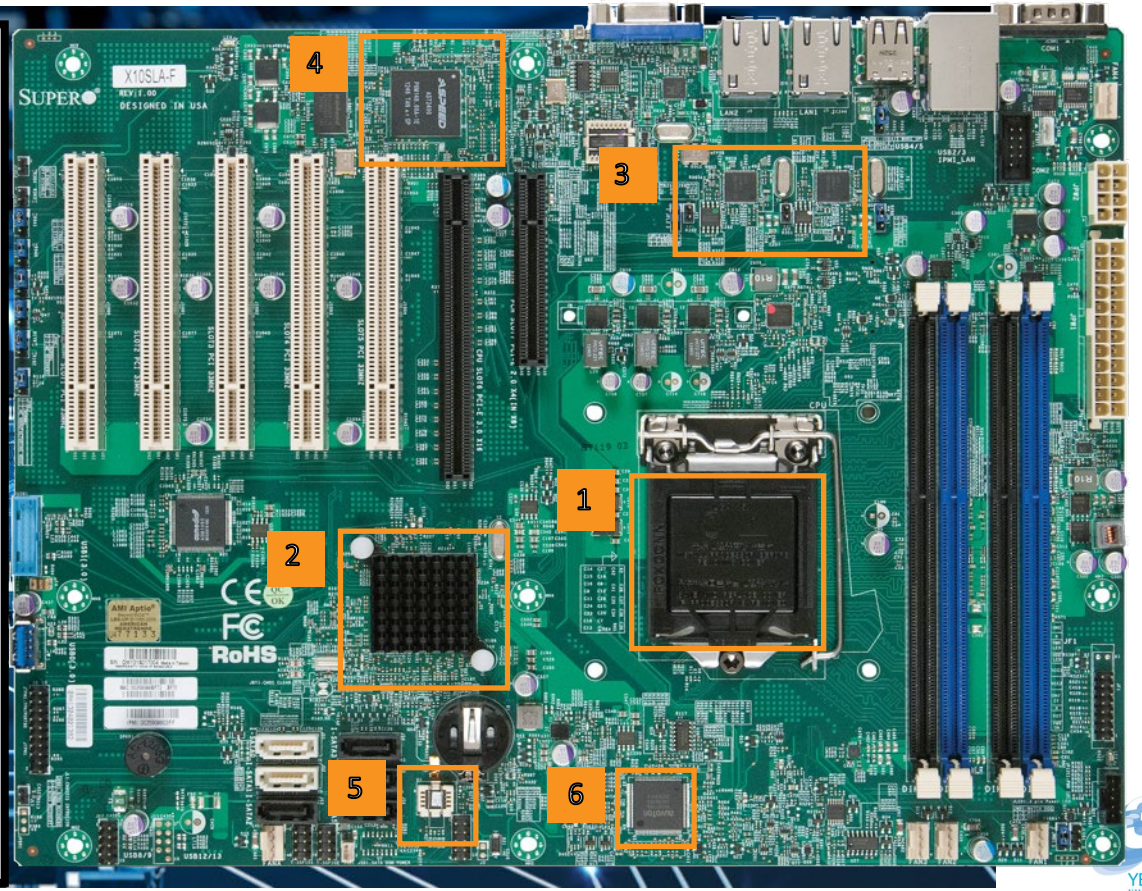
5 BIOS / UEFI

6 Embedded controllers

RAM / Memory



SSD/HD

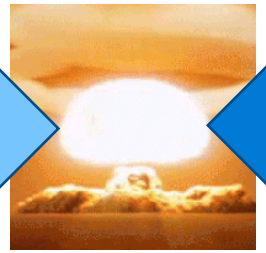


Zero Trust and Firmware

Flash Memory Summit

4 **Dynamic** Solve for speed & scale through *automation*

DIGITAL TRANSFORMATION WITH CLOUD SCALE GROWTH



ZERO TRUST PRINCIPLES AND PRACTICES

Automation is the answer

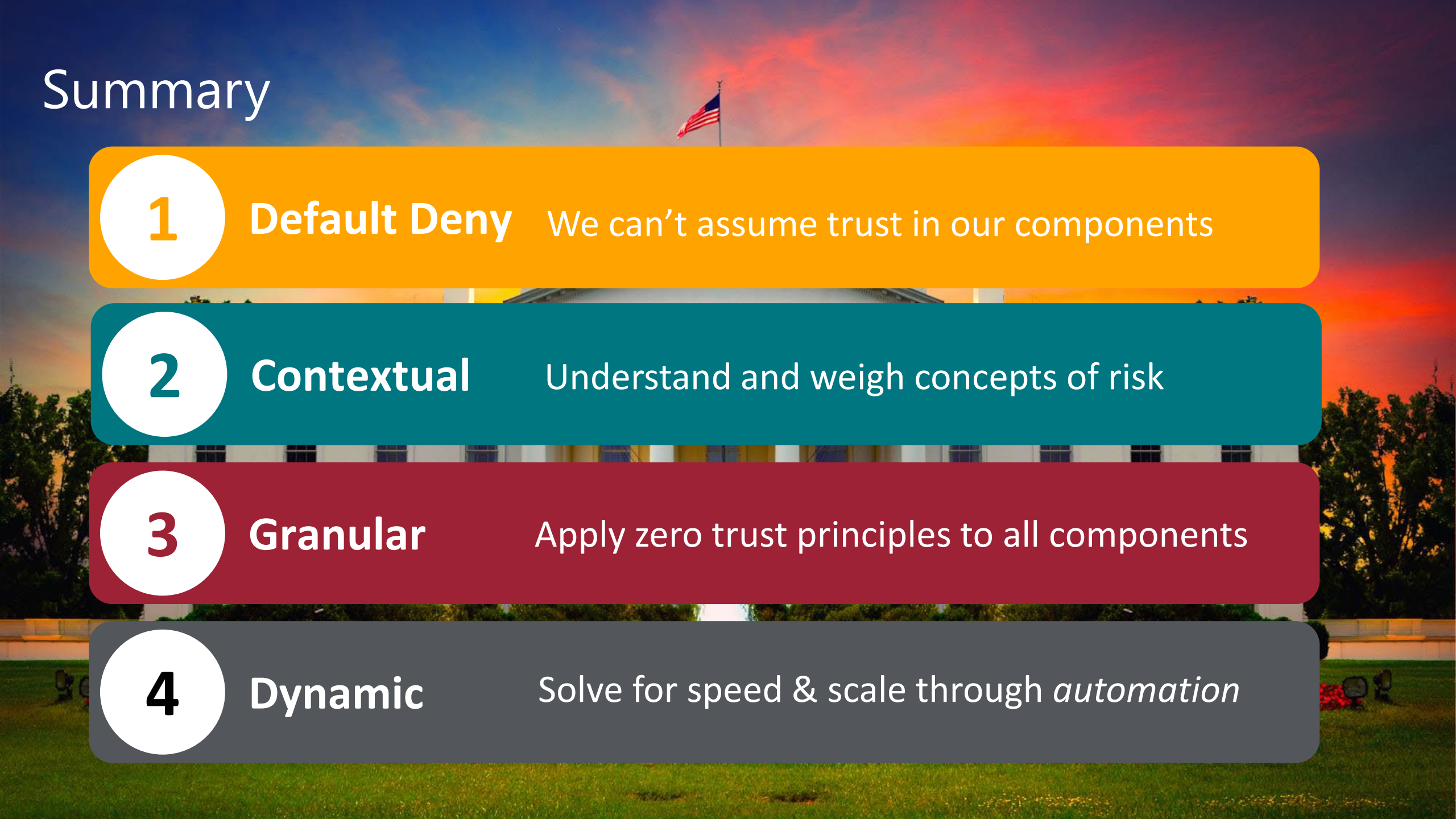
- Lifecycle automation of sub-OS firmware and hardware components…
- Driven by a reliable, repeatable process that manages firmware at enterprise scales

Identify
- Search and Discover
- Catalogue
- Inventory

Verify
- Assess vulnerabilities
- Assure integrity and authenticity

Fortify
- Configure securely
- Update regularly
- Patch as needed

Summary

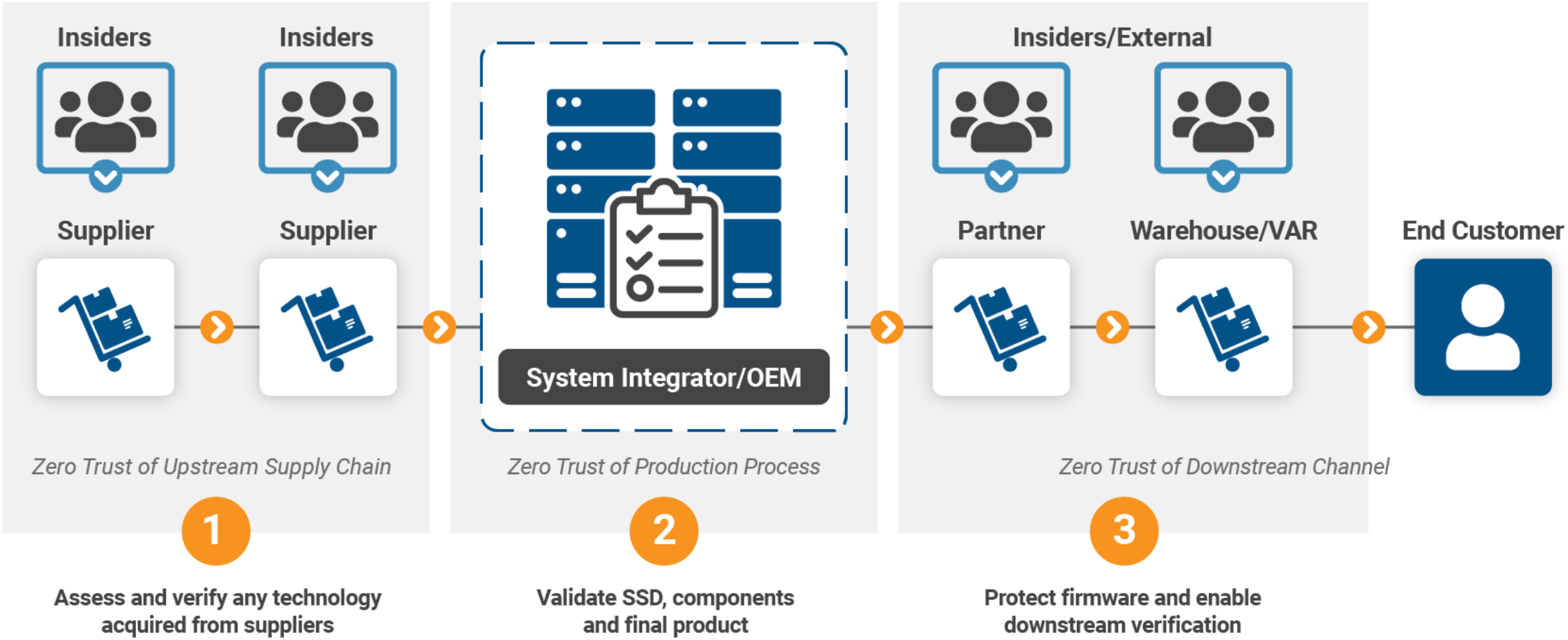


1. **Default Deny** — We can't assume trust in our components
2. **Contextual** — Understand and weigh concepts of risk
3. **Granular** — Apply zero trust principles to all components
4. **Dynamic** — Solve for speed & scale through *automation*

What can be done

Steps to take across the supply chain…

Trust Should be Implemented Across the Value Chain



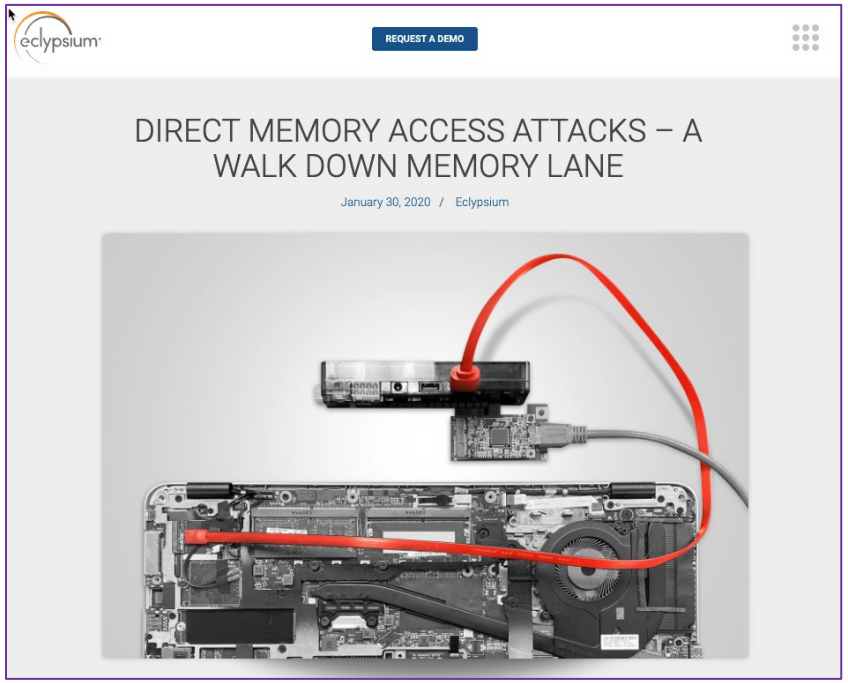
Zero Trust Best Practices

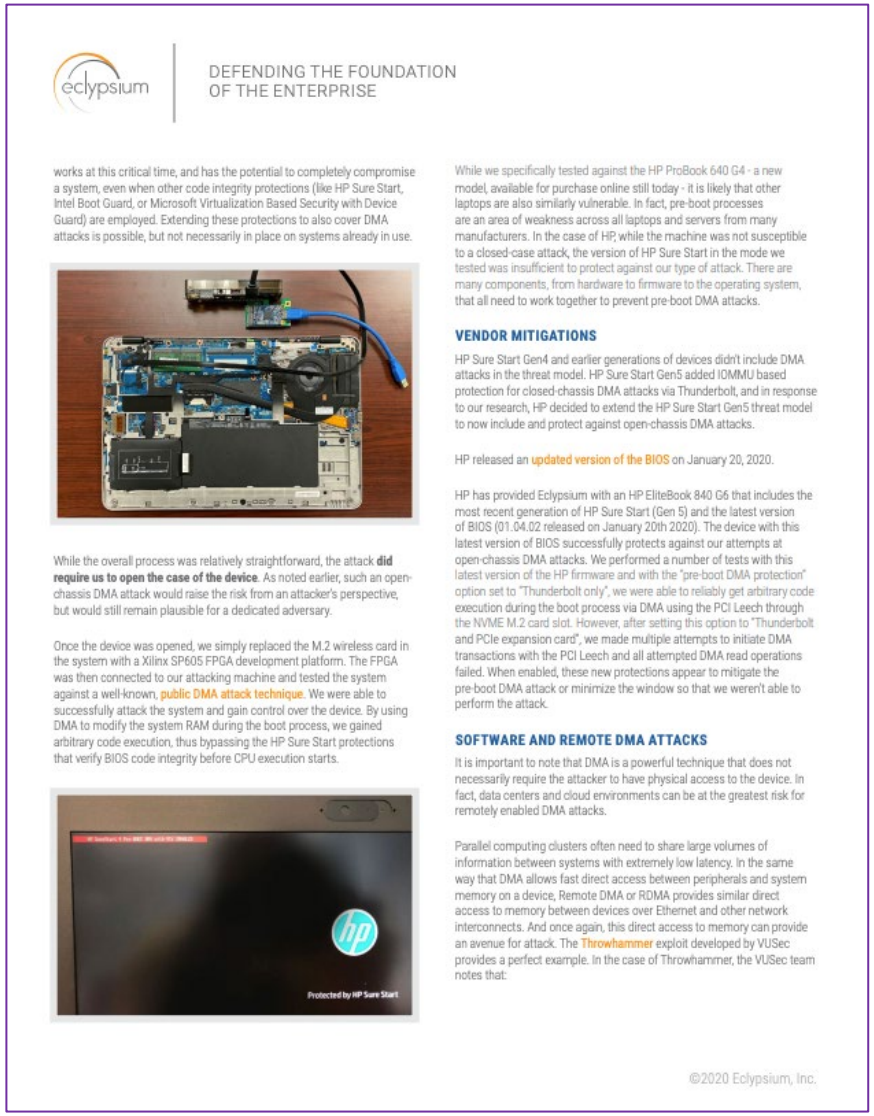
Action within Supply Chain	Action for SI/OEM	Actions for Channel
Define the security requirements and expectations of all suppliers	Perform supplier Audits	Verify firmware-level protections and security configurations: Any installed firmware properly signed
Validate suppliers scan outsourced components 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	

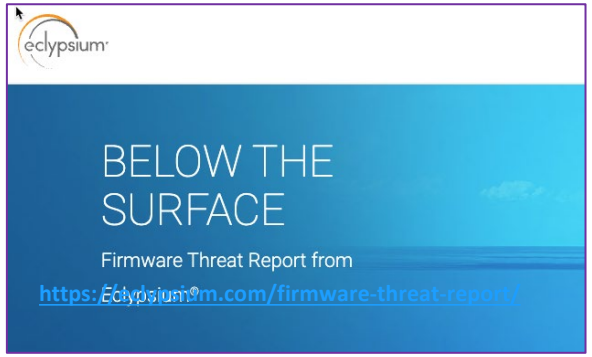
Eclypsium Provides Threat Intelligence, Advice and Tools

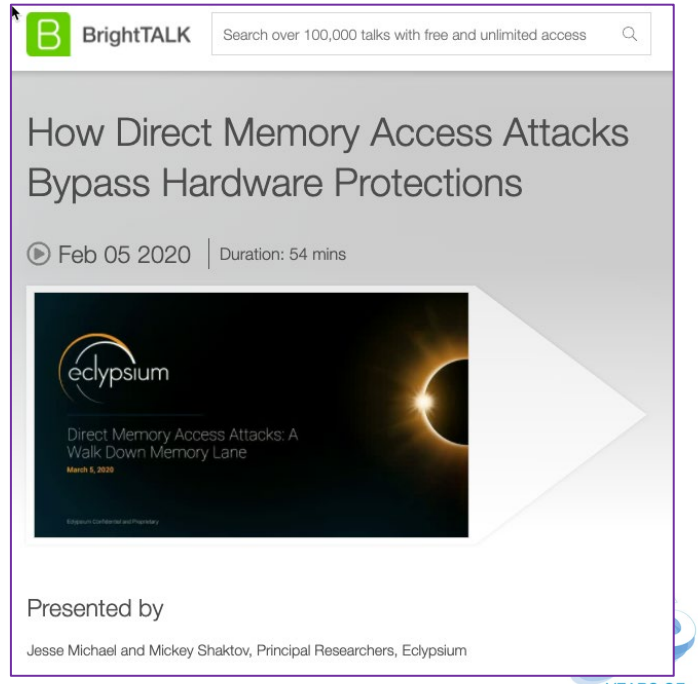
DMA firmware guidance

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





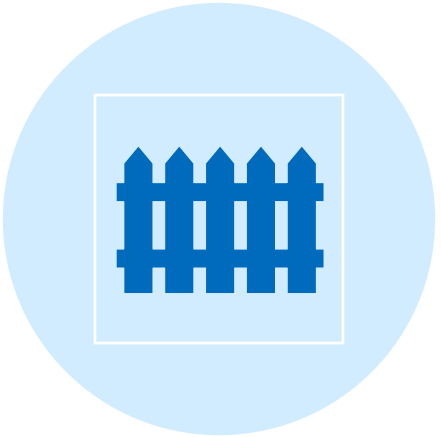




How OakGate helps Firmware-level Behavior and Test

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

FIRMWARE DOWNLOAD CAPABILITY TO VALIDATE THE FIRMWARE DOWNLOAD PROCESS

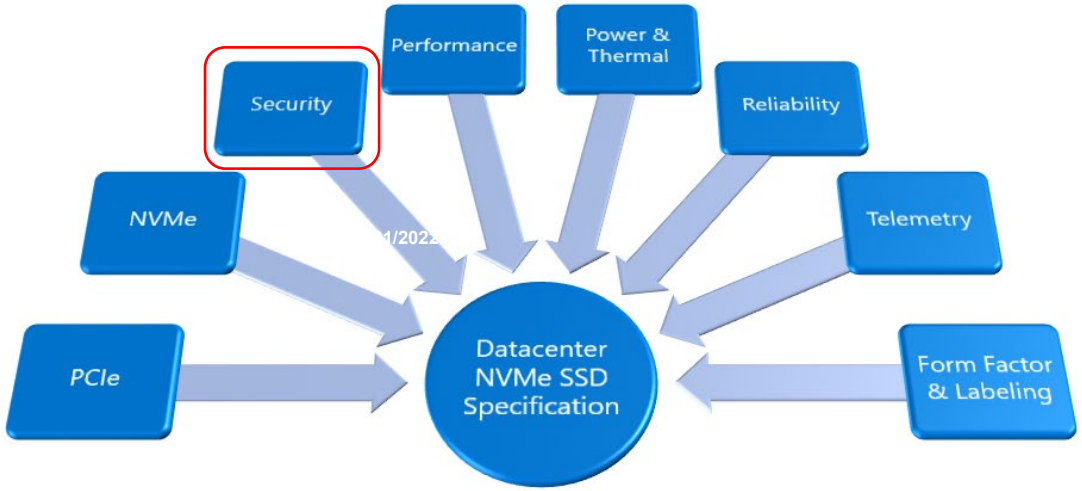


MEMORY FENCING TECHNOLOGY TO IDENTIFY WHEN/IF THE SSD HAS VIOLATED THE MEMORY MAPPING

What's New? OCP – Open Compute Project

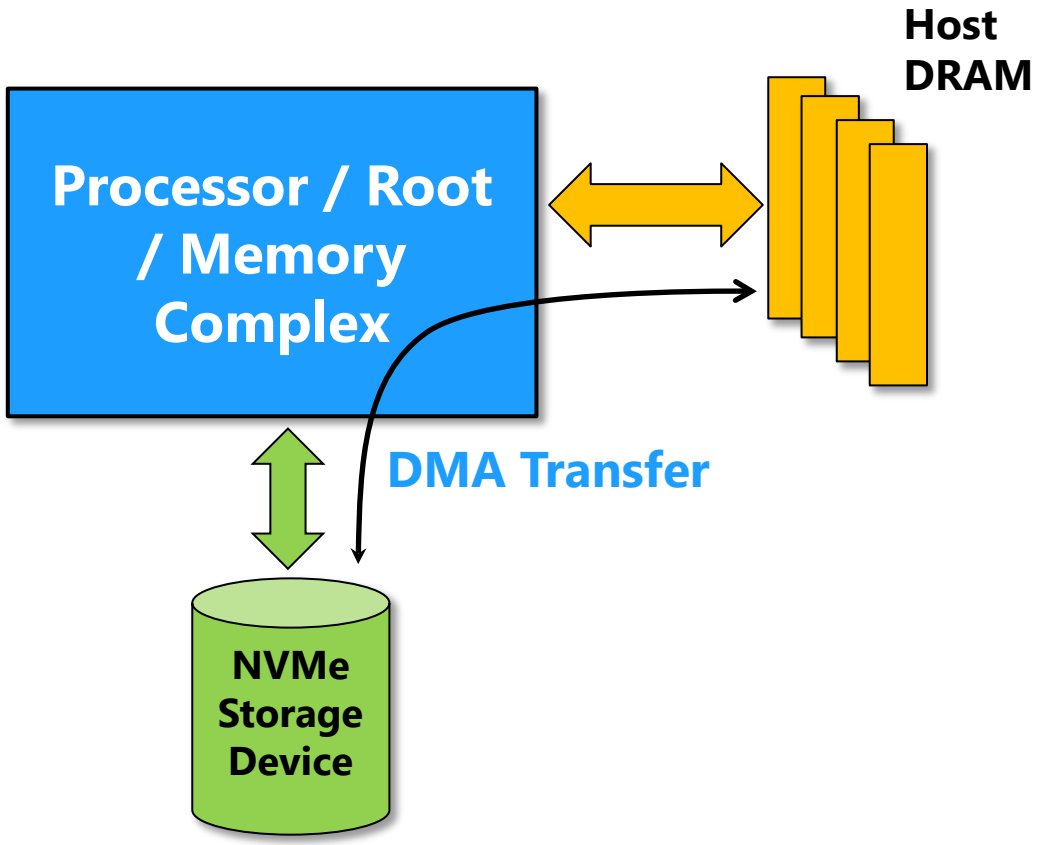
- ✓ Validation against the Datacenter NVMe SSD Specification ensures the target device complies with the wide array of common requirements across multiple datacenter customers
  - ✓ Common & deterministic SSD functionality in-system
  - ✓ Numerous datacenter opportunities from one leveraged SSD design

OPEN Compute Project



OakGate Memory Fencing Solution

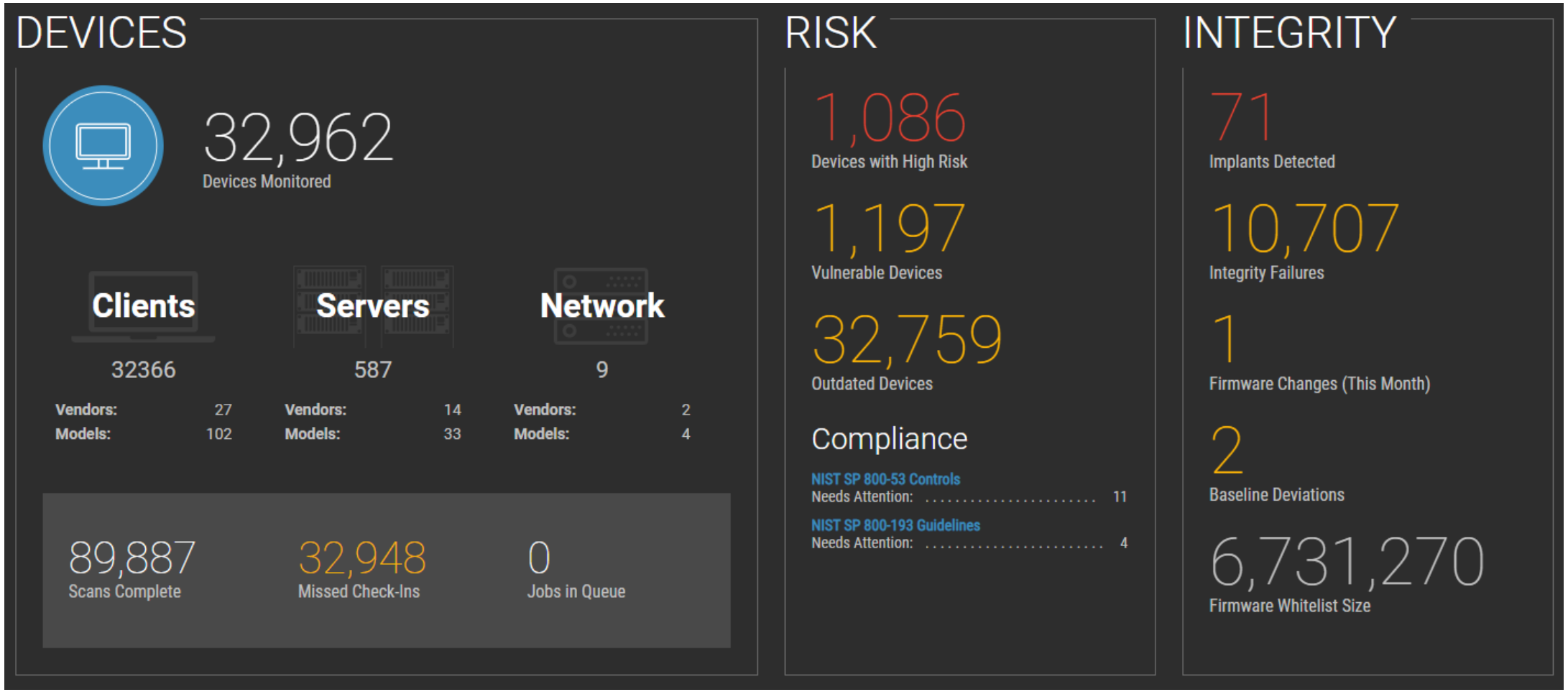
- The Teledyne LeCroy OakGate Test Appliance detects functional errors that occur when a device with a Direct Memory Access (DMA) engine accesses memory space outside of the area specified by the device driver
- With OakGate's IO Exerciser users can create simulated workloads that simulate the lifetime 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

Flash Memory Summit

Using the Eclypsium Platform for firmware security

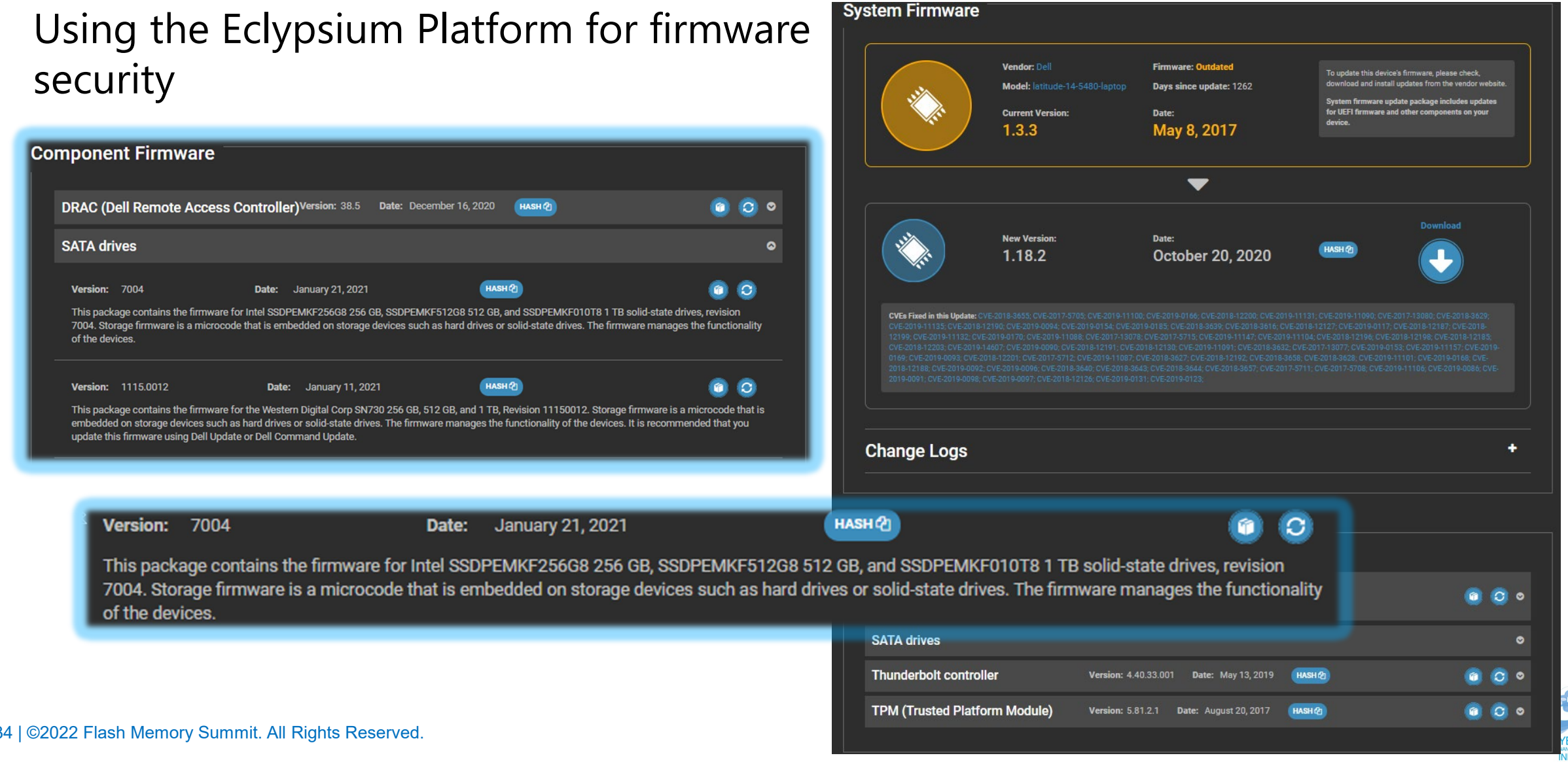


35 YEARS OF NAND FLASH MEMORY INNOVATION

Eclypsium Creates an SBOM That Includes Firmware

Flash Memory Summit

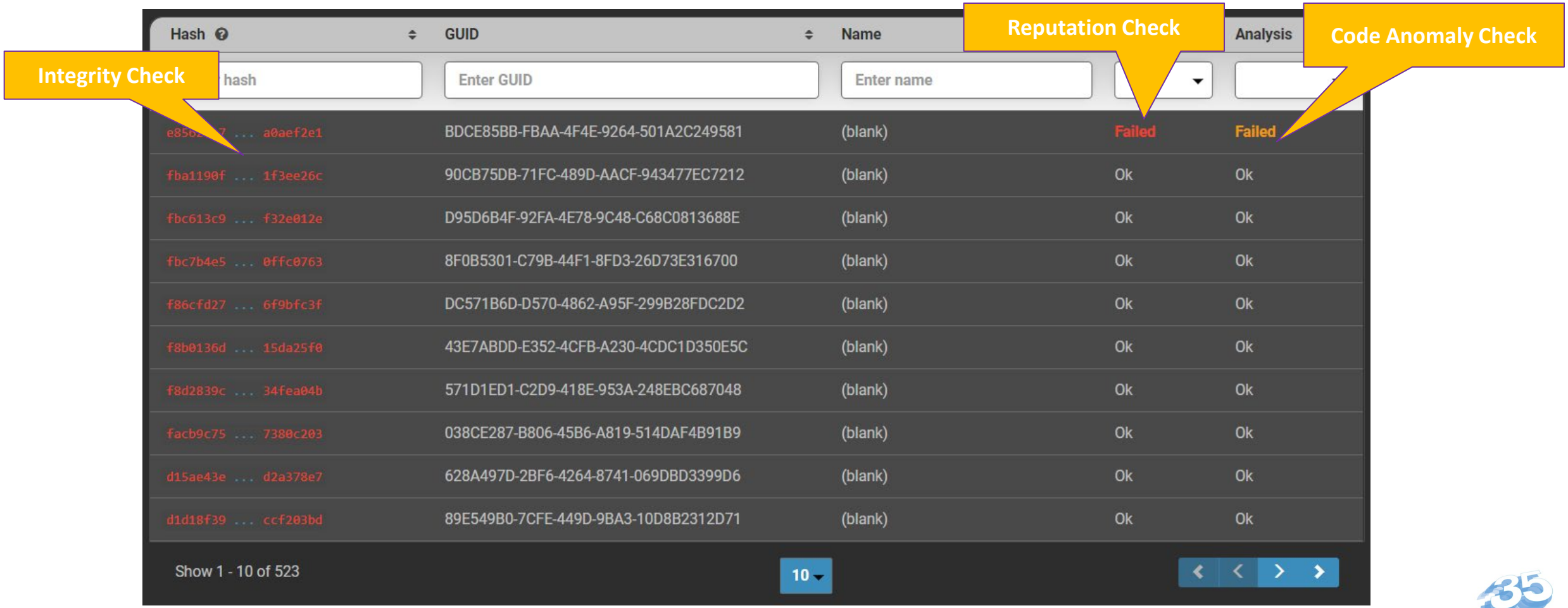
Using the Eclypsium Platform for firmware security



Eclypsium Creates an SBOM That Includes Firmware

Flash Memory Summit

Using the Eclypsium Platform for firmware security



35 YEARS OF NAND FLASH MEMORY INNOVATION

In Summary:

Flash Memory Summit

- 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

35 YEARS OF NAND FLASH MEMORY INNOVATION

Questions

Contact Teledyne LeCroy

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 T28 Analyzer

Summit T3-8 Analyzer

Summit Z416 Exerciser
Gen 4 up to x16

Summit Z58 5.0 Exerciser/Analyzer
Gen 5 up to x8

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

Summit T3-16 Exerciser
with Test Platform

Email Sales: protocolsales@teledynelecroy.com

Phone Support: 1-800-553-2769

www.teledynelecroy.com

