



**Hewlett Packard  
Enterprise**

**HPE AI**

# **OPERATING SECURELY IN A HYBRID WORLD FY24 OUTLOOK**

---

Von Gardiner  
Director DoD Sales & Distinguished Technologist  
Hewlett Packard Enterprise

April 17, 2024

# Hybrid Strategy Coming to Life



Data | Sustainability | Security



# The Future is Hybrid ~ Told Ya!

HPE Discover 2018 Signaled The Next Stage Of The Company's Future Under Antonio Neri



HPE says that what sets **GreenLake Hybrid Cloud** apart from other managed services is that it is all automated and cloud-native so that organizations theoretically won't need to hire and train new staff to manage and oversee it.



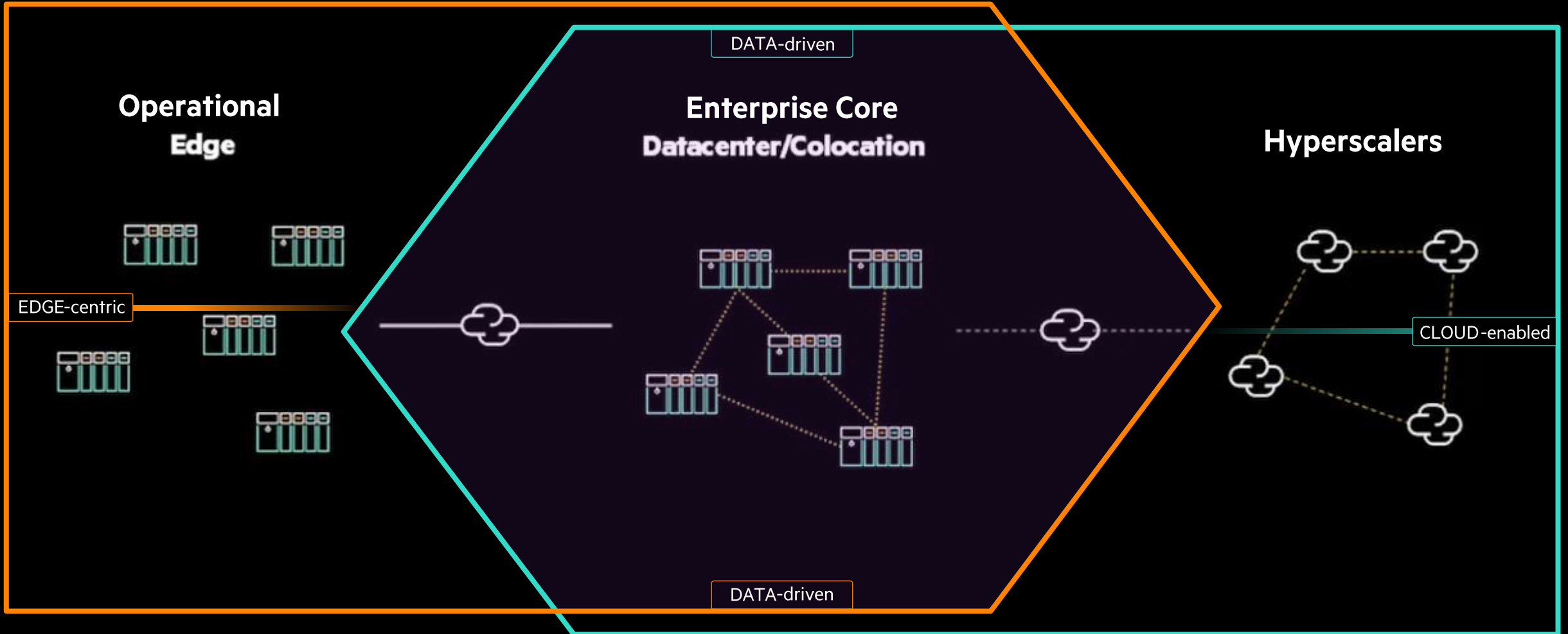
## Cloud in FY2024 Budget?

### Request to NIST for updated definitions and characteristics of “multi-cloud”

*Cloud Computing.*—The agreement encourages NIST to publish descriptions and definitions of the latest cloud characteristics, service models, deployment models, and multi-cloud. The agreement encourages NIST to include in its description of “multi-cloud” the characteristics of software technology that allow for data, application, and program portability. Additionally, the agreement encourages NIST to consider interoperability between multiple cloud computing software vendors and between public, private, and edge cloud environments.

# The Evolved Enterprise ~ Secure Hybrid Multi-cloud (as-a-Service)

Operations across the continuum from Edge to Core to Cloud Service Providers



*Physically insecure devices*

*Communication over untrustworthy networks*

# Today ~ ASCI White (Circa 2000-2001) In The Palm Of Your Hand... Literally



- 512 nodes totaling 8,192 processors (@ 375 MHz)
- Total of 6 terabytes (TB) of memory
- Total of 160 TB of disk storage
- Weighing 106 tons
- 3 MW of electricity for compute / 3 MW for cooling



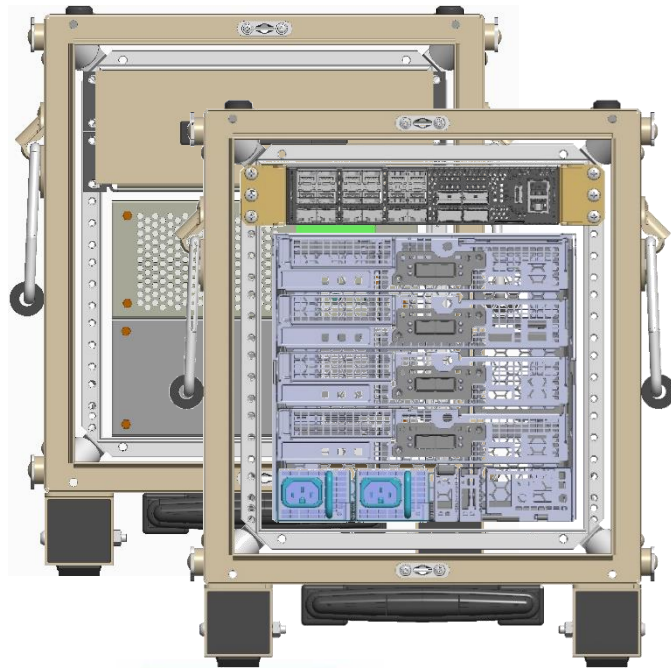
- Four 40 core CPUs (@ 2.3 GHz) & four T4/L4 GPUs
- Total of 6 terabytes (TB) of memory
- Total of 123 TB of NVMe storage (246TB in Dec 23)
- Weighing ~55lbs
- < 1.5KW of electricity



# DEPLOYABLE DISCONNECTED SECURE PRIVATE CLOUD PLATFORM

Edge DDIL Cloud Certified:

- AWS (Snowblade)
- Azure HCI
- Google Anthos
- Private Cloud
- IL2, IL4, IL6, IL7



TYPE	NAME	LOCATION	HOSTS	VMS	BARE METAL	STATUS
aws	GreenLake AWS Cloud US East	US East	0	3	0	OK
aws	GreenLake AWS Cloud US West	US West	0	3	0	OK
Microsoft Azure	GreenLake Azure Cloud	Global	0	1	0	OK
Google Cloud	GreenLake GCP	Global	0	4	0	OK
vmware	HPE GreenLake VMaaS Cloud	TorontoUPC	8	12	0	OK



Or Compute Ops Manager

Autonomous Cloud operations when disconnected from Hyperscaler/Gov Cloud/Core

# HPE EDGELINE SOLUTIONS (TO INCLUDE 5G/WIFI)

The HPE Edgeline EL8000t Chassis supports two Sapphire Rapids extremely powerful server nodes that can operate in 55C temperatures in a short depth 2U chassis. The EL8000 holds up to four servers.



TEMPEST Lids





# RUGGEDIZED EDGELINE EL8000 MIL-STD-810H CERTIFIED

## HPE Edgeline EL8000 in the Ultralife Rugged Case MIL-STD-810H Certification Tests

<b>MIL-STD-810H METHOD 514.8 - VIBRATION</b>	
<b>Procedure I: General Vibration</b>	
Category 8 – Propeller Aircraft (Conducted as Operational Test)	Passed ✓
Category 12 – Jet Aircraft (Conducted as Operational Test)	✓
Category 20 – Ground Vehicles (Used Category 4 Common Carrier Profile)	✓
Category 21 – Watercraft (Shipboard Random Vibration)	✓

<b>MIL-STD-810H Environmental Tests</b>	Measure	Passed
Method 500.6, Procedure I (Altitude Storage)	15,000 ft	✓
Method 500.6, Procedure II (Altitude Operation)	15,000 ft	✓
Method 501.7, Procedure I (High Temperature Storage)	+71C	✓
Method 501.7, Procedure II (High Temperature Operation)	+55C	✓
Method 501.7, Procedure II (High Temperature Tactical Standby)	+60C	✓
Method 502.7, Procedure I (Low Temperature Storage)	-40.5C	✓
Method 502.7, Procedure II (Low Temperature Operation)	-40C	✓
Method 507.6, Procedure II (Humidity Operation)	95% +/- 4%	✓



# Growing Evidence in the Private Sector for Hybrid Cloud

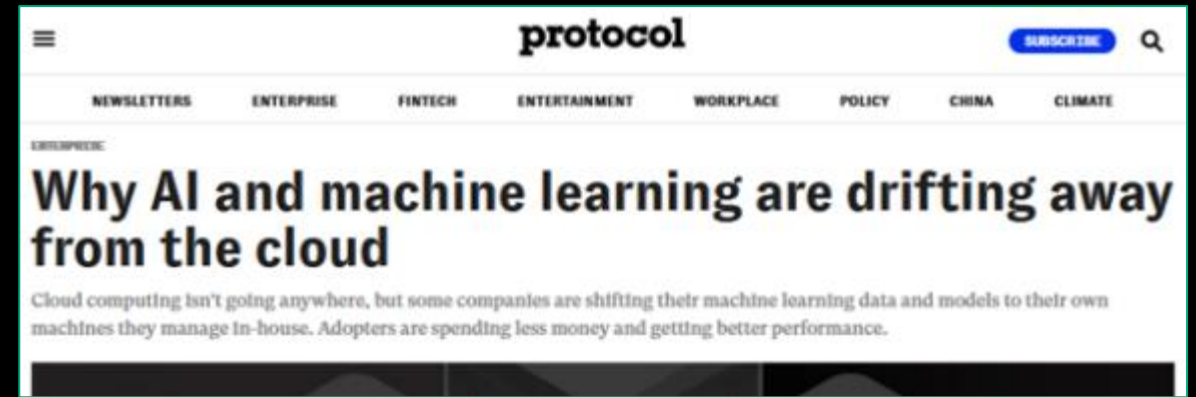


andreesen.  
horowitz It's time to build

Portfolio Team Focus Areas

## The Cost of Cloud, a Trillion Dollar Paradox

by Sarah Wang and Martin Casado

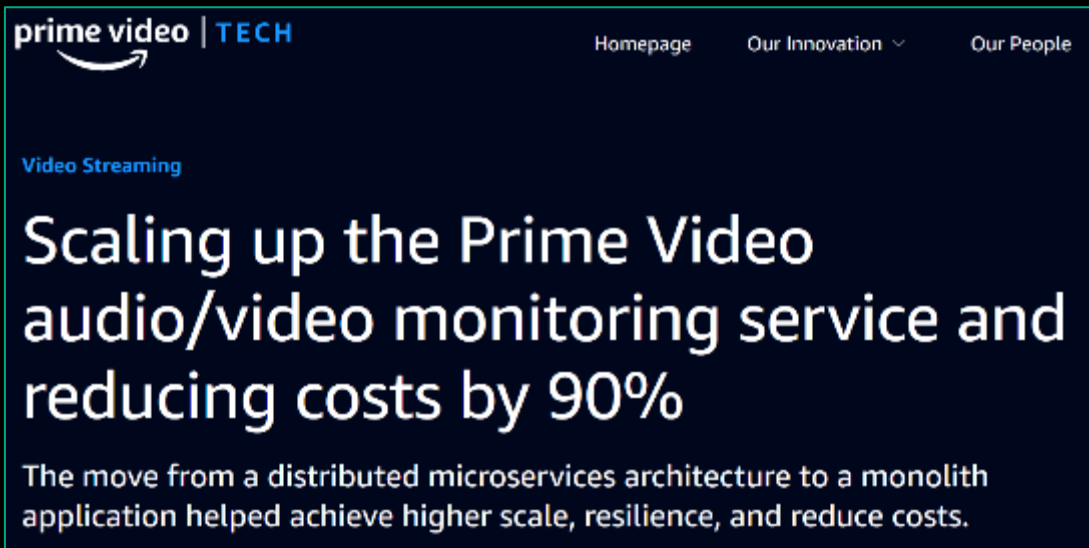


protocol

NEWSLETTERS ENTERPRISE FINTECH ENTERTAINMENT WORKPLACE POLICY CHINA CLIMATE

## Why AI and machine learning are drifting away from the cloud

Cloud computing isn't going anywhere, but some companies are shifting their machine learning data and models to their own machines they manage in-house. Adopters are spending less money and getting better performance.



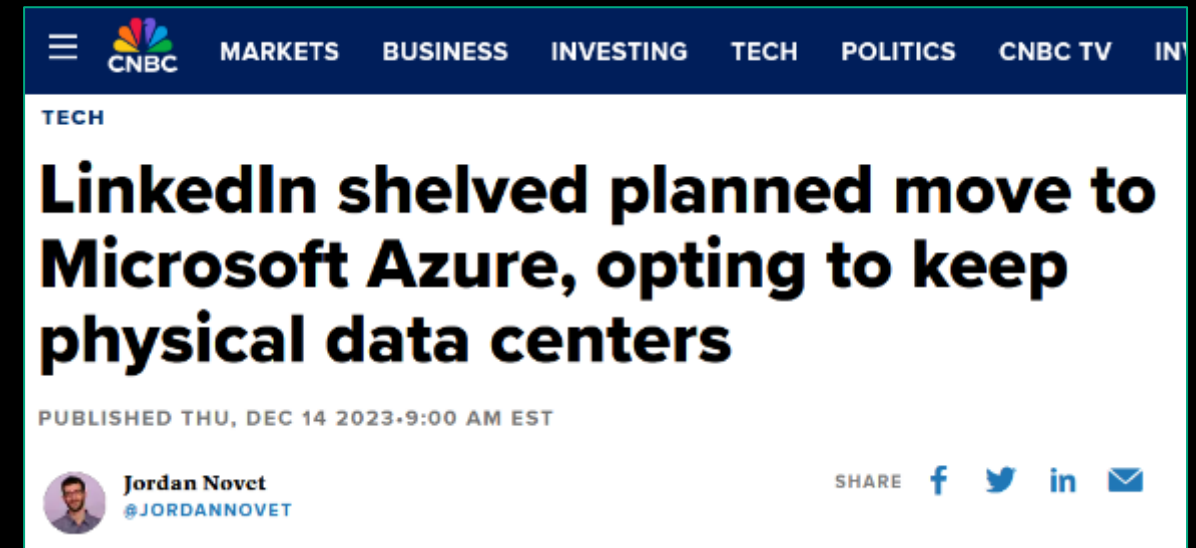
prime video | TECH

Homepage Our Innovation Our People

Video Streaming

## Scaling up the Prime Video audio/video monitoring service and reducing costs by 90%

The move from a distributed microservices architecture to a monolith application helped achieve higher scale, resilience, and reduce costs.



MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV

## LinkedIn shelved planned move to Microsoft Azure, opting to keep physical data centers

PUBLISHED THU, DEC 14 2023 9:00 AM EST

Jordan Novet @JORDANNOVET

SHARE f t in e

# Pentagon Spending Less Than Expected on JWCC



From [USAspending.gov](https://USAspending.gov) there were 30 JWCC Awards in Year 1:

Microsoft: \$22.8 Million

Oracle: \$9.3 Million

Amazon: \$7.8 Million

Google: \$3.9 Million

**TOTAL: \$43.8 Million**



# Is The Future of Federal Cloud Hybrid? It Has To Be...

Table 1: Agency-Reported Data Center Optimization Initiative (DCOI) Strategic Plan Fiscal Year (FY) 2022 the Number of Data Centers Reported as Closed in FY 2022, as of August 2022

Agency	Open at the start of FY22	DCOI FY22 closure goal	Closed as of August 2022	Additional planned FY22 closures	Additional planned FY23-FY25 closures
Department of Agriculture	2	0	0	0	
Department of Commerce	61	0	1	1	
Department of Defense	638	12	8	40	
Department of Education	0	0	0	0	
Department of Energy	96	2	1	2	
Department of Health and Human Services	88	0	0	2	
Department of Homeland Security	20	1	1	1	1
Department of Housing and Urban Development	2	0	0	0	0
Department of the Interior	50	1	1	0	0
Department of Justice	11	1	0	0	6
Department of Labor	6	1	0	1	0
Department of State	141	1	3	5	0
Department of Transportation	211	0	0	0	0
Department of the Treasury	103	0	0	0	0
Department of Veterans Affairs	274	3	5	0	0
Environmental Protection Agency	2	0	0	0	0
General Services Administration	4	0	0	0	
National Aeronautics and Space Administration	18	0	0	0	
National Science Foundation	1	0	0	0	
Nuclear Regulatory Commission	3	0	0	0	
Office of Personnel Management	2	0	0	0	
Small Business Administration	2	0	0	0	
Social Security Administration	11	0	0	6	
U.S. Agency for International Development	0	0	0	0	0
<b>Total</b>	<b>1746</b>	<b>22</b>	<b>20</b>	<b>58</b>	<b>44</b>

Agency	Open at the start of FY22	DCOI FY22 closure goal	Closed as of August 2022	Additional planned FY22 closures	Additional planned FY23-FY25 closures
Department of Agriculture	2	0	0	0	0
Department of Commerce	61	0	1	1	0
Department of Defense	638	12	8	40	31
Department of Education	0	0	0	0	0
Department of Energy	96	2	1	2	2

Department of Homeland Security	1	Yes
Department of Housing and Urban Development	0	Yes
Department of the Interior	0	Yes
Department of Justice	6	Yes
Department of Labor	0	Yes
Department of State	0	Yes
Department of Transportation	0	Yes
Department of the Treasury	0	Yes
Department of Veterans Affairs	0	Yes
Environmental Protection Agency	0	Yes

Small Business Administration	2	0	0	0	0
Social Security Administration	11	0	0	6	1
U.S. Agency for International Development	0	0	0	0	0
<b>Total</b>	<b>1746</b>	<b>22</b>	<b>20</b>	<b>58</b>	<b>44</b>

Still a few Data Centers in Federal Government...

Source: GAO analysis of agency data. | GAO-23-105946

# ARTIFICIAL INTELLIGENCE (AI)

---

*Hey, I need some of that! Just don't know what for yet..*



# What About AI in Federal?

## FY 2024 Budget

### Department of Homeland Security

#### Artificial Intelligence/Machine Learning

- **\$6M** program increase for Enterprise-Wide Maritime Domain Platform to provide an enterprise-wide applied artificial intelligence maritime domain capability in Management Directorate
- **\$279,875,000** for targeting operations. Within these funds, CBP is encouraged to review commercial, off-the-shelf artificial intelligence capabilities, visual analytics, and search platforms that might help improve the National Targeting Center's operations.
- **\$163.5M** is for integrated surveillance towers and autonomous surveillance towers, defined as integrated software and/or hardware systems that utilize sensors, onboard computing, and artificial intelligence to identify items of interest in CBP
- **\$12.6M** for artificial intelligence and machine learning capabilities under Non-Intrusive Inspection (NII) in CBP
- **\$14.4M** to procure advanced Computed Tomography scanners for deployment to mail and express consignment courier facilities and automation/machine learning to support targeting efforts under Non-Intrusive Inspection (NII) in CBP

#### Artificial Intelligence and Machine Learning

##### Defense-wide:

- **\$351.6M** for Chief Digital and Artificial Intelligence Officer (CDAO) – Demonstration/Validation (DEM/VAL) Activities
- **\$34.3M** for Chief Digital and Artificial Intelligence Officer (CDAO) – Military Intelligence Program
- **\$10M** program increase for artificial intelligence reinforcements in Defense-Wide
- **\$5M** program increase for artificial intelligence manufacturing in Defense-Wide
- **\$1M** program increase for artificial intelligence for explosive ordinance disposal decision support in Defense-Wide

# 2024 State CIO Top 10 Priorities

## Cybersecurity, digital services, AI top NASCIO's 2024 priorities

AI joins the National Association of State Chief Information Officers' annual priorities list for the first time in 2024.

### 1 CYBERSECURITY AND RISK MANAGEMENT

governance; budget and resource requirements; security frameworks; data protection; training and awareness; insider threats; third-party risk



### 1 DIGITAL GOVERNMENT / DIGITAL SERVICES

framework for digital services; state portals; improving and digitizing citizen experience; accessibility; identity management; digital assistants; privacy



### 3 ARTIFICIAL INTELLIGENCE / MACHINE LEARNING / ROBOTIC PROCESS AUTOMATION

adoption; delivery of state services; bots; digital assistants; citizen interaction; policy



### 4 LEGACY MODERNIZATION

enhancing, renovating, replacing, legacy platforms and applications; business process improvement



### 5 WORKFORCE

preparing for the future workforce and reimagining the government workforce; transformation of knowledge, skills and experience; more defined roles for IT asset management, business relationship management, and service integration



### 6 DATA MANAGEMENT / DATA ANALYTICS

data governance; data architecture; strategy; business intelligence; predictive analytics; big data; roles and responsibilities



### 7 BROADBAND / WIRELESS CONNECTIVITY

strengthening statewide connectivity; implementing rural broadband expansion; 5G deployment



### 8 IDENTITY AND ACCESS MANAGEMENT

supporting citizen digital services; workforce access; access control; authentication; credentialing; digital standards



### 9 CLOUD SERVICES

cloud strategy; selection of service and deployment models; scalable and elastic services; governance; service management; security; privacy; procurement

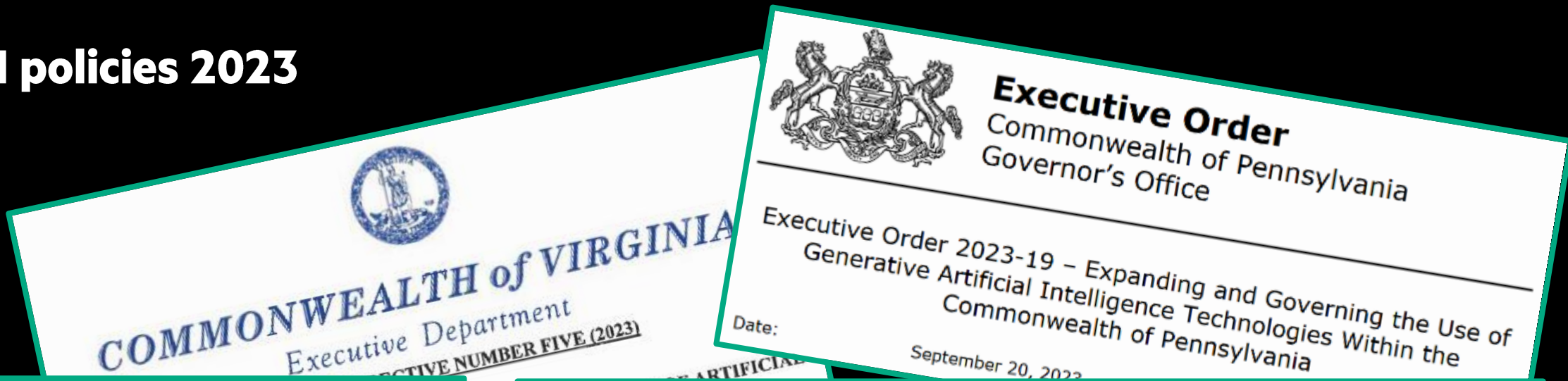


### 10 CIO AS BROKER / NEW OPERATING MODEL

building the new state CIO operating model in my state; state CIO as a trusted advisor and the ultimate business relationship manager; collaborating with agencies regarding strategy and operations; effectively managing industry partners



# State AI policies 2023



POLICY AND PROCEDURES  
MEMORANDUM  
8200.00

Effective Date  
31 July 2023

Approval Date  
25 July 2023

1.0 SUBJECT: Generative Artificial Intelligence Policy

2.0 DISTRIBUTION: Executive Branch Cabinet and Non-Cabinet A

EA-01-01-G  
State CIO Adopted: August 8, 2023  
TSB Approved: N/A  
Sunset Review: August 8, 2026

Replaces:  
N/A

EXECUTIVE DEPARTMENT  
STATE OF CALIFORNIA

EXECUTIVE ORDER N-12-23

AND RESPONSIBLE  
TELLIGENCE

**WHEREAS** the State of California is a global leader in innovation, research, development, human capital, and entrepreneurship; and

**WHEREAS** Generative Artificial Intelligence ("GenAI") represents a significant leap forward in technology, by generating novel text, images, and other content, which will transform the way that the State and the world conduct business and serve the public; and





# SECURE HYBRID MULTI-CLOUD OPERATIONS

---

*If it was easy, you'd already be doing it!*



# SIX KEY CHALLENGES TO REALIZING SECURE HYBRID MULTI-CLOUD OPS

---

- Platform/infrastructure security & location
- Security, Authentication & Attestation across environments (SPIFFE & SPIRE)
- Application Rationalization
  - **Re-host/Re-platform/Re-architect/Re-write/Retain/Retire**
- Data availability between environments (Data Fabric)
- Workload Orchestration, Automation and Management (Ansible, Puppet, Chef, etc.)
- Multi-path analysis / dynamic QoS / guaranteed delivery / network resilience (SD-WAN) / Automated PACE Plans

# TODAY'S MOST COMMON SECURITY THREATS

## Security Today



- Denial of Service (DOS):**  
Make crucial changes to the target's firmware that interfere with its ability to perform key functions.
- Distributed Denial of Service (DDoS):**  
Overwhelm the target with bogus requests for information or assistance from multiple sources, tying up resources and hindering its ability to respond to legitimate users.
- Data Theft or Information Theft:**  
Malware or compromised code copied directly into the target's firmware renders it completely useless. Sometimes called "bricking" a server, i.e., rendering it as useful as a brick.
- Permanent Denial of Service (PDoS):**  
Bricked or permanently disabled servers.
- Ransomware:**  
Hostile software that invades a PC or server and locks it permanently, preventing legitimate users from accessing any content unless a ransom payment is made.

**Security requirements for cloud environments...do you have a say or not?**

# NIST-BASED HOLISTIC APPROACH TO CYBERSECURITY HAS THREE POINTS OF FOCUS



## Prevent/Protect



## Detect



## Recover

- Silicon Root of Trust
- CNSA (formerly NSA Suite B)
- Two Factor Authentication CAC
- Prevent Firmware Attacks from OS
- Secure Erase of NAND Data
- Common Criteria & FIPS 140-2 Level1
- UEFI Secure Boot
- TPM 2.0
- NIST 800-147b BIOS
- PCI-DSS Compliance
- Secure Supply Chain

- Firmware Runtime Validation
- Chassis Intrusion Detection on Most Servers
- Rack Cabinet Door Detector
- Verified Boot Integrity Check
- Trusted eXecution Technology
- SIEM Tool Support
- Audit Logs
- Measured Boot

- Secure Auto Recovery
- Recover Operating Systems
- Data Collection for Forensic Evaluation
- HPE PointNext recovery services

Build it In

Stop it Now

Recover it Fast



***You can't recover if you don't even know you've been attacked!***

# ZERO TRUST, CYBERSECURITY AND SUPPLY CHAIN RISK MANAGEMENT

***EITHER THEY'RE IMPORTANT, OR THEY'RE NOT!***

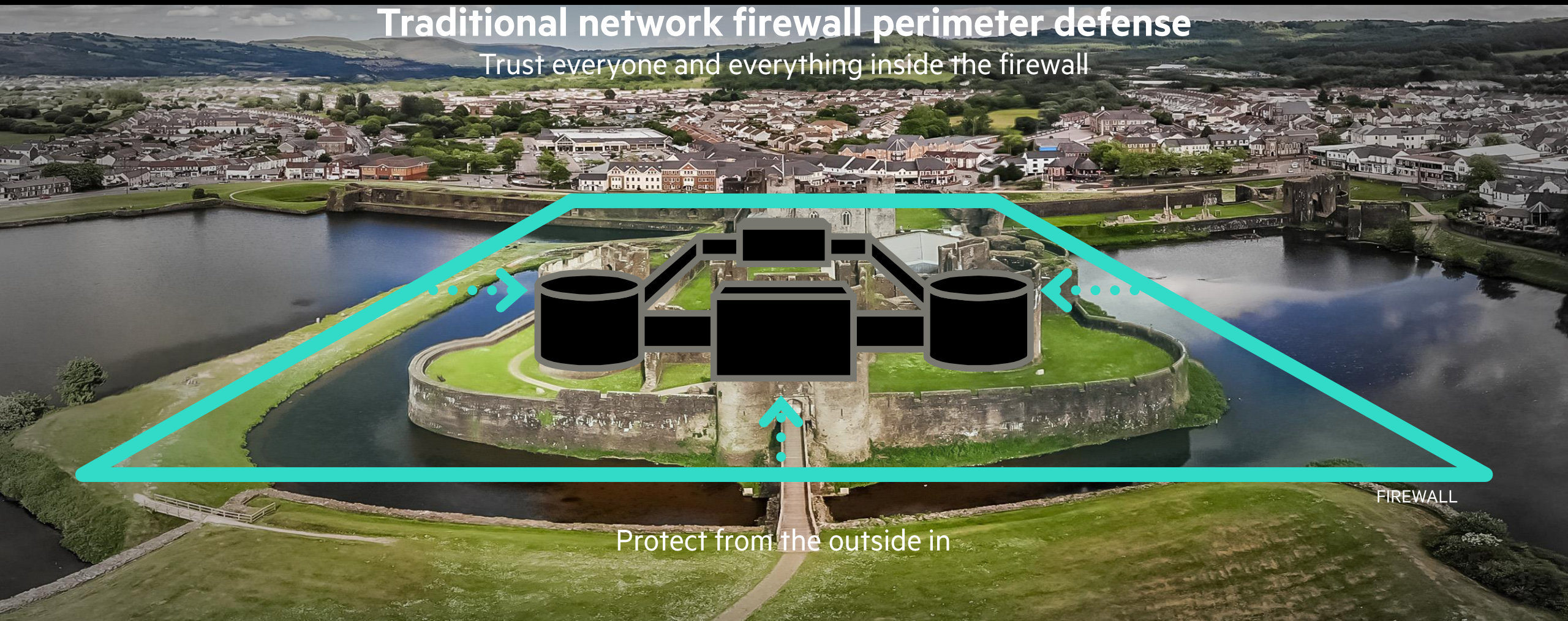
---

Because security is a **must** regardless of where your workloads run or your data resides.



# WHERE DID ZERO TRUST COME FROM AND WHAT DOES IT MEAN?

Traditional network firewall perimeter defense  
Trust everyone and everything inside the firewall



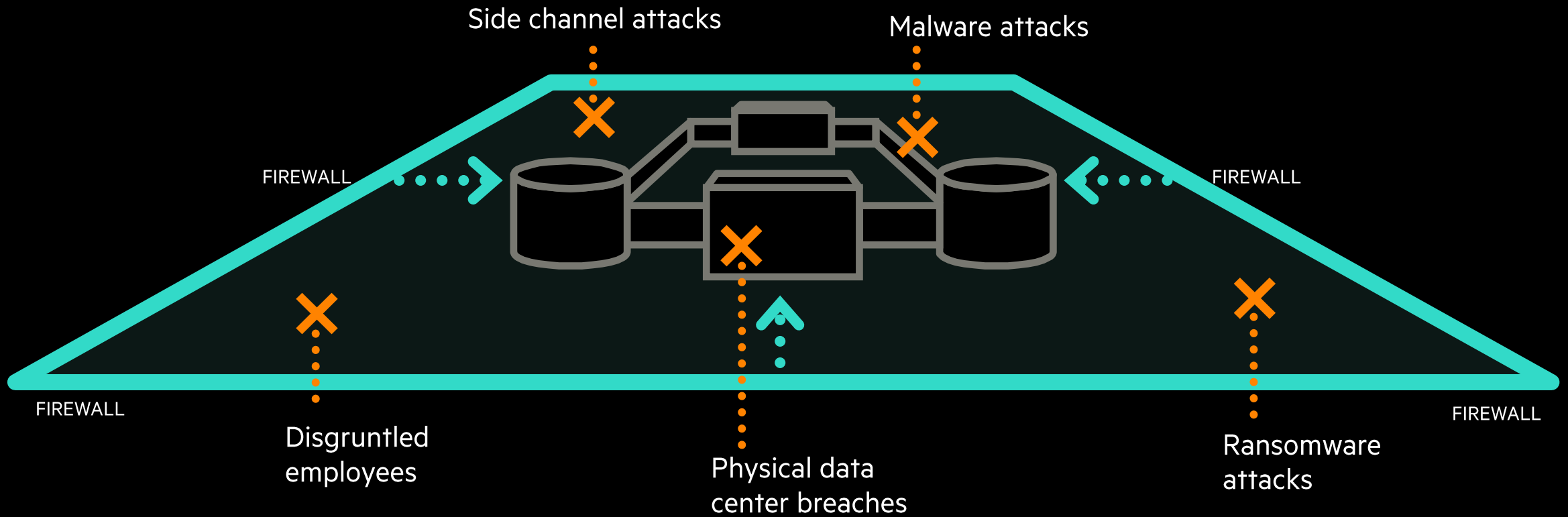
FIREWALL

Protect from the outside in



# WHAT DOES ZERO TRUST MEAN?

## Traditional network firewall perimeter defense



# WHAT DOES ZERO TRUST MEAN?

## Zero Trust Security

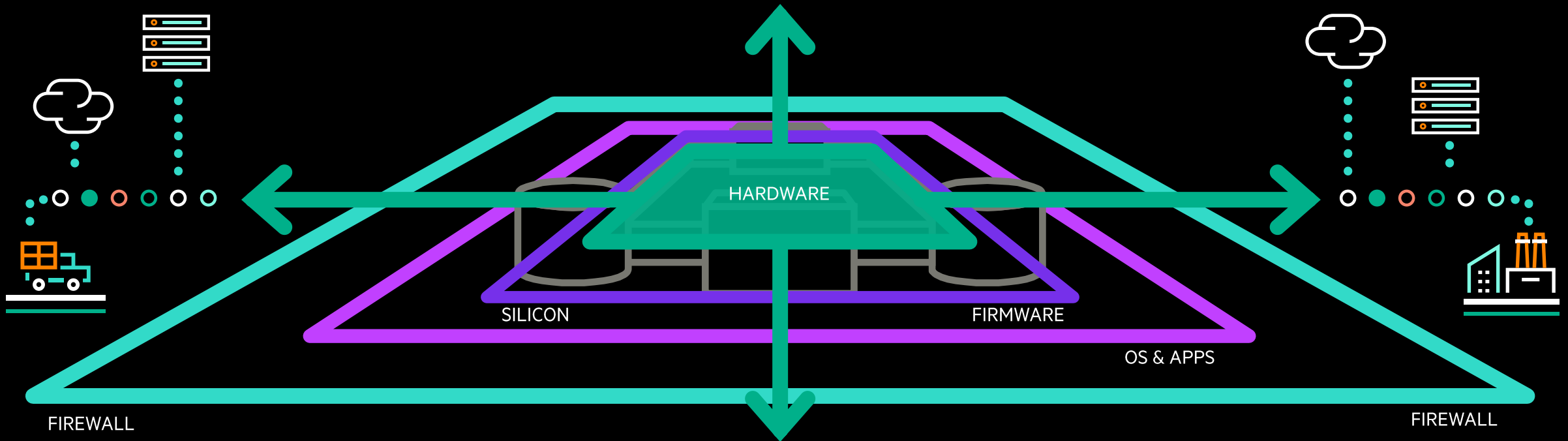
Never trusting, continuously verifying

Protect from the inside out

Identity aware, data-driven, workload relevant

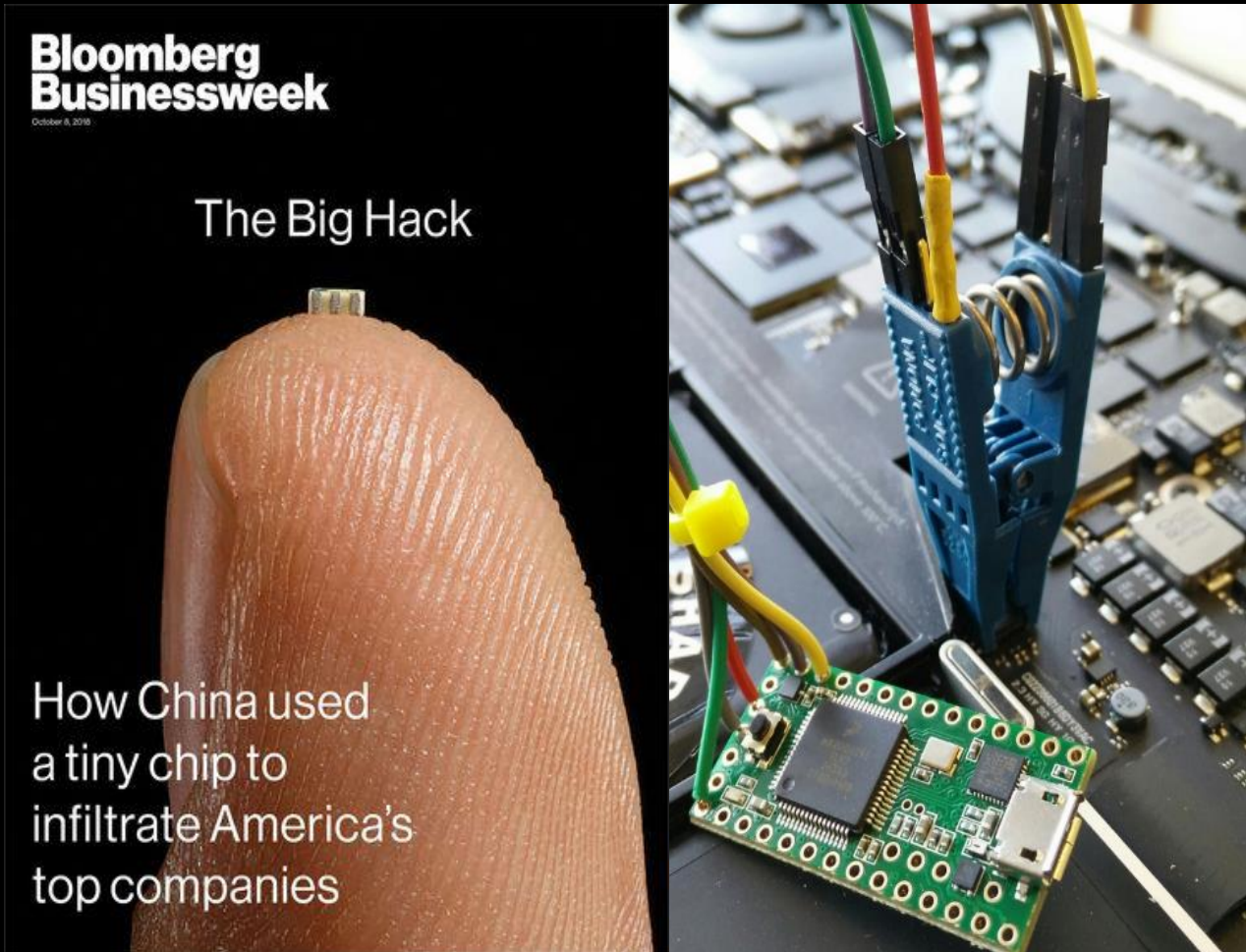
Many edges, data centers and clouds

Many edges, data centers and clouds





# NEW ATTACK VECTORS APPEAR WEEKLY



Cisco Security Advisory

### Cisco Secure Boot Hardware Tampering

**High**

<b>Advisory ID:</b>	cisco-sa-20190513-secureboot	CVE-2019-0753
<b>First Published:</b>	2019 May 13 17:30 GMT	CWE-284
<b>Last Updated:</b>	2019 May 14 20:41 GMT	
<b>Version 1.2:</b>	<a href="#">Interim</a>	
<b>Workarounds:</b>	No workarounds available	
<b>Cisco Bug IDs:</b>	<a href="#">CSCvn77141</a>	
	<a href="#">CSCvn77142</a>	
	<a href="#">CSCvn77143</a>	

CISCO Secure Boot Anchor Trust hardware FPGAs remotely bypassed, all FPGAs in all the CISCO devices in the field need to be reprogramed. \$22B/year of revenue in switches & routers affected.

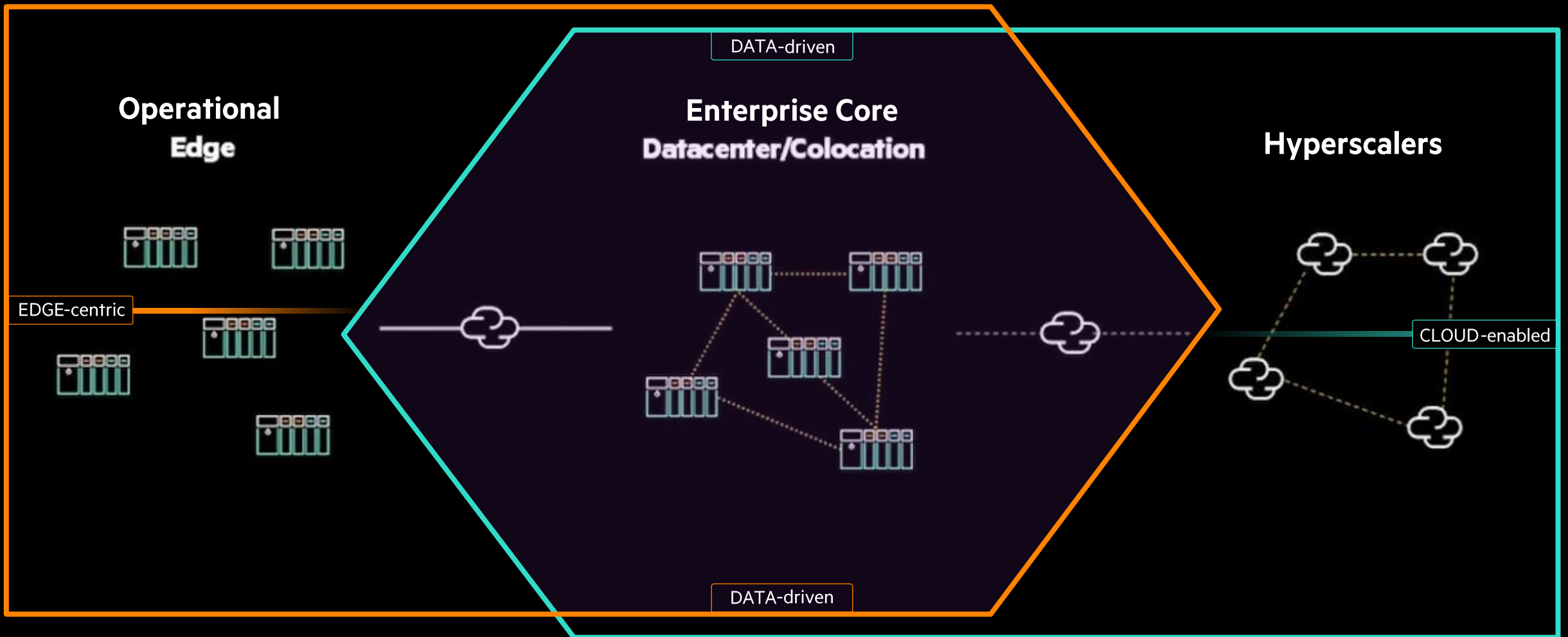
# TRUSTED SUPPLY CHAIN ~ COUNTRY OF ORIGIN “USA”

- Parts inspected, loaded and assembled in the US, by vetted US Citizens, creating a country-of-origin: *USA manufacturing*
- Four HPE-exclusive security features can be enabled to ensure the secure condition upon customer receipt:
  - **High Security Mode:** locks down the host and requires specific authentication to boot
  - **Server Configuration Lock:** takes cryptographic measurements of all the firmware, hardware components and options to create encrypted log, compared at first boot
  - **UEFI Secure Boot:** connects the HPE Silicon Root of Trust to the OS (if loaded by HPE)
  - **Trusted Delivery:** Servers can be shipped via monitored vehicles with two vetted drivers



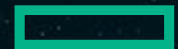
# The Evolved Enterprise ~ Secure Hybrid Multi-cloud (as-a-Service)

Operations across the continuum from Edge to Core to Cloud Service Providers



*Physically insecure devices*

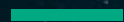
*Communication over untrustworthy networks*



**Hewlett Packard  
Enterprise**

**HPE AI**

**THANK YOU**



[Von.Gardiner@hpe.com](mailto:Von.Gardiner@hpe.com)

