Dell Technologies inspiration —

Secure by Design - The data centers of the future in the AI Era

Poul Kjeldgaard – Field CTO

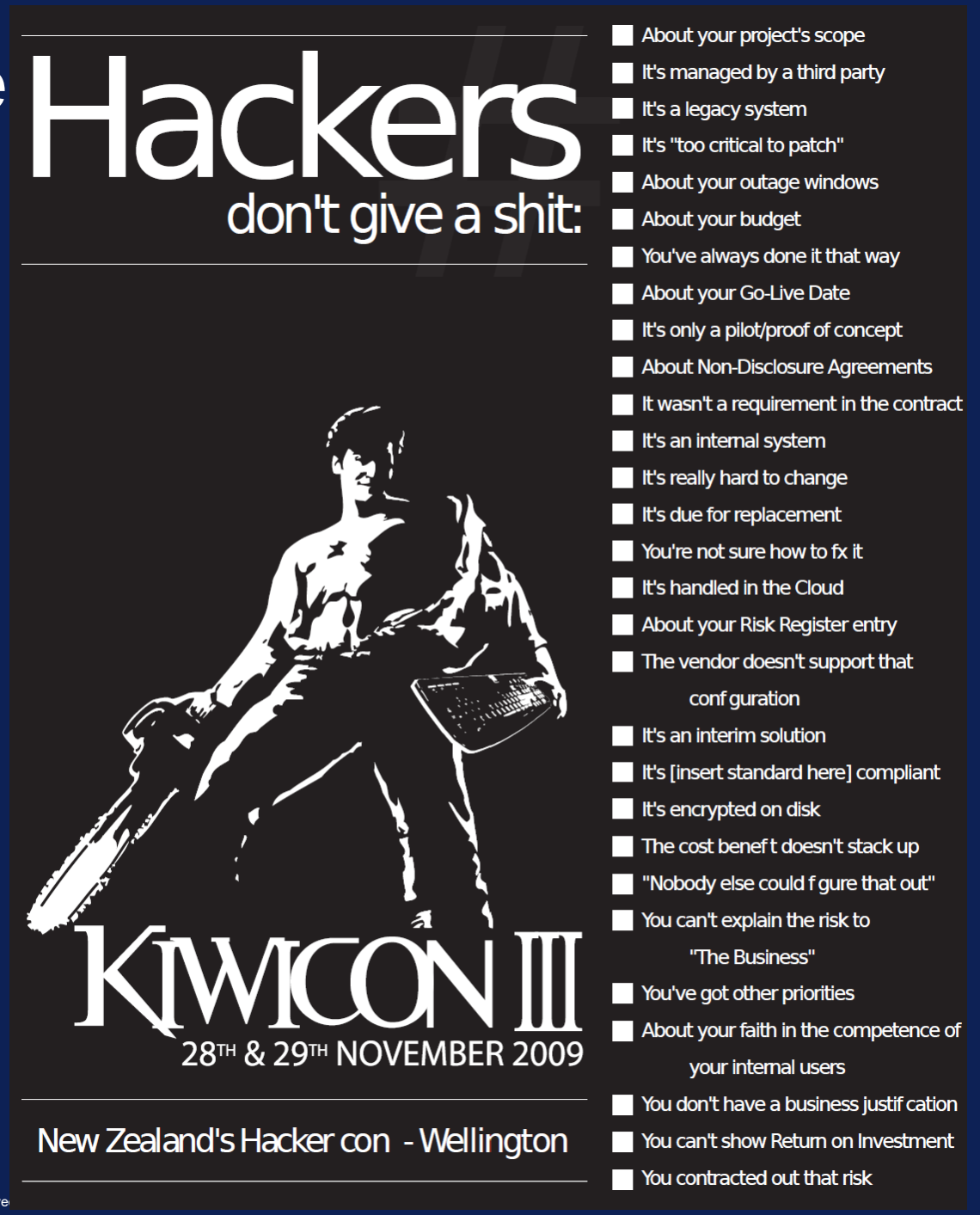
DELL Technologies

AMD

It is about what we put in our Datace 2026 Update in an AI era context.

- After the big project – to create or renovate the DC
- Then physical Security is applied
- DC are certified to certain standard and processes are create and people are educated.

- Then IT is onboarded and with that comes challenges – independent if you are an owner, a hoster, a Cloud, a customer etc.

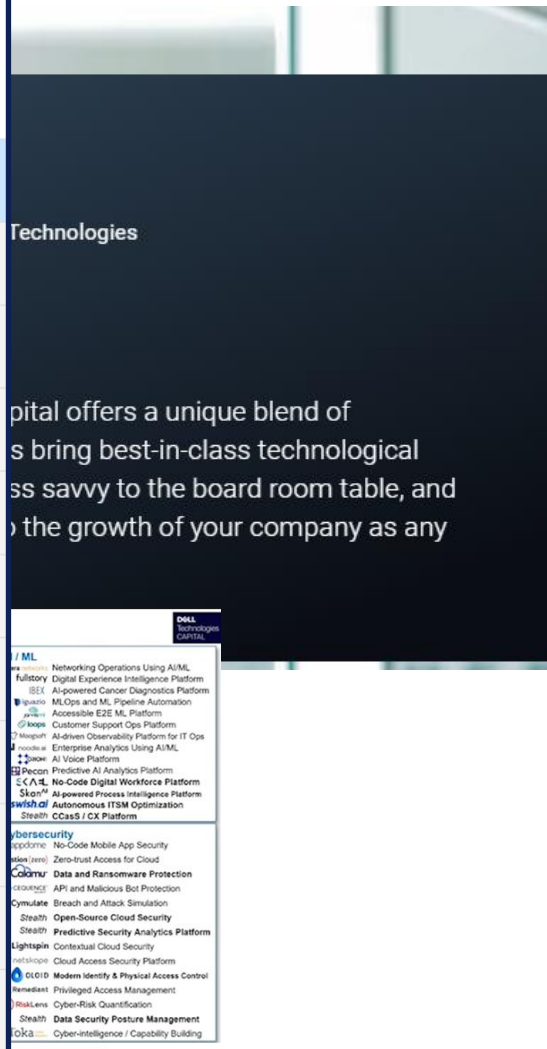


Access to innovation - Dell Technologies Capital

HARRITY TEAM SERVICES CHARITY PROGRESS ANALYTICS SOFTWARE TOOLS NEWS & INSIGHTS CAREERS

Stay informed with the Patent 300® list – a trusted ranking of leading patent holders. This essential resource, from Harrity Patent Analytics, highlights trends, statistics, and the innovators shaping the future. See footnotes for updates to corporate tree changes in 2026 list.

RANK	ORGANIZATION	COUNTRY	2025 US PATENTS	YOY CHANGE
1	SAMSUNG ELECTRONICS CO., LTD.		7519	▲ 12%
2	TAIWAN SEMICONDUCTOR MFG. CO. LTD.		4232	▲ 6%
3	QUALCOMM		3856	▲ 10%
4	HUAWEI TECHNOLOGIES CO., LTD.		3480	▲ 6%
5	CANON K.K.		2987	▲ 13%
6	SAMSUNG DISPLAY CO., LTD.		2924	▲ 11%
7	TOYOTA JIDOSHA K.K.		2907	▲ 19%
8	APPLE INC.		2856	▼ -8%
9	INTERNATIONAL BUSINESS MACHINES CORPORATION		2467	▼ -11%
10	DELL TECHNOLOGIES		2445	▲ 38%
11	BOE TECHNOLOGY GROUP CO., LTD.		2375	▲ 19%



MDA DELL Technologies

Reference: Dell Technology – Zero Trust for DoD

Dell Technologies Achieves US Department of Defense Validation for Zero Trust Solution – **02.April 2025**

DELL Technologies

Project Fort Zero

Detachable Edge deployment model: 5G-connected, Zero Trust-protected, mobile operation vehicle

5G, Zero Trust use case: transmits over a 2.5 mile radius and protects up to 50 square miles

Powered by the Zero Trust Center of Excellence: Dell is leading the Zero Trust ecosystem with more than 30 partners

Dell Center of Excellence will address 3 deployment models

On Premises

Cloud

Detachable Edge

Validated Zero Trust: the government will certify the solution for advanced maturity against the U.S. Department of Defense Zero Trust reference architecture

The fully configured **Project Fort Zero** solution will lower the barrier to Zero Trust adoption, reducing the estimated time for advanced Zero Trust adoption through a private cloud.*

*DoD Zero Trust Capability Execution Roadmap (COA 1), Portfolio Management Office, January 6, 2023, https://dodcio.defense.gov/Portals/0/Documents/Library/ZTCapabilityExecutionRoadmap.pdf

COA 2

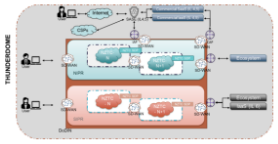
Commercial Cloud

- Relies on commercial provider(s) to develop ZT compliant cloud environments using Greenfield approach
- Achieves DoD ZT quicker than COA-1
- Mandate would be to achieve DoD ZT "Target" level, at a minimum
- Provides standardized tools and capabilities to support ZT execution

COA 3

Private Cloud

- Government Owned/Operated high-performance Native ZT Cloud (NZTC) using Greenfield approach
- Achieves DoD ZT quicker than COA-1
- Achieves immediate DoD ZT "Advanced" level by design, which needs to be independently validated



oject Fort Zero's on premises, sovereign zero trust private cloud infrastructure.

ell Technologies Achieves US Department of Defense alidation for Zero Trust Solution | Dell USA

DELL Technologies

The malicious script is designed to steal npm, GitHub, AWS and GCP tokens, and also installs TruffleHog. This open source tool can detect as many as 800 different types of secrets, including API keys, access tokens, database passwords and encryption keys. This

CYBERWARFARE

Iranian Cyber Group Handala Targets US Troops in Bahrain

US service members received WhatsApp messages claiming they would be targeted with drones and missiles.

By Ionut Arghire | April 29, 2026 (6:35 AM ET)

The Iran-linked threat actor Handala this week targeted US troops in Bahrain in an influence campaign carried out on WhatsApp.

TRENDING

1 OpenSSH Flaw Allowin
Access Lurked for 15 Y
2 Incomplete Windows P
Zero-Click Attacks
3 Medtronic Hack Confir
ShinyHunters Threaten
4 Firefox Vulnerability Al
Fingerprinting
5 Easily Exploitable 'Pack
Vulnerability Leads to R
6 Robinhood Vulnerabilit
Phishing Attacks
7 No Patch for New Phar
Escalation Technique in
8 Energy and Water Mar
Hacked

Daily Briefing Newsle

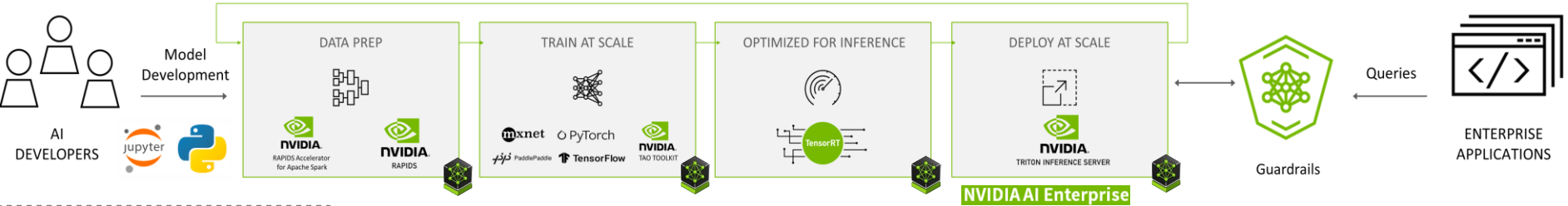
TRENDING

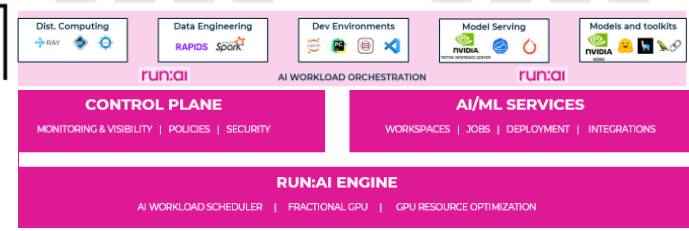
1 OpenSSH Flaw Allowing Full Root Shell Access Lurked for 15 Years
2 Incomplete Windows Patch Opens Door to Zero-Click Attacks
3 Medtronic Hack Confirmed After ShinyHunters Threatens Data Leak
4 Firefox Vulnerability Allows Tor User Fingerprinting
5 Energy and Water Management Firm Itron Hacked
6 Easily Exploitable 'Pack2TheRoot' Linux Vulnerability Leads to Root Access
7 Robinhood Vulnerability Exploited for Phishing Attacks
8 Recent Microsoft Defender Vulnerability Exploited as Zero-Day

DELL Technologies

GenAI Validated Design

Medical Imaging | Speech AI (Riva) | Customer Service | Recommenders | Physics ML | Communications (NeMo) | Video Analytics | Logistics | Conversational AI | Robotics (Isaac) | Autonomous Vehicles | Cybersecurity (Morpheus)

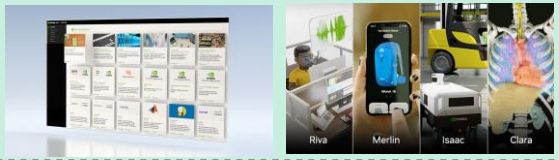




Open AI Models

LLaMA by Meta

NVIDIA Pretrained Models



AI/ML Platform Tools

NVIDIA MERLIN | NVIDIA TRITON INFERENCE SERVER | NVIDIA NEMO

AI/ML OPS

run:ai

PowerEdge R660

Kubernetes Control Plane | Management nodes

NVIDIA Base Command Manager

Kubernetes control plane

master | master | master

Infrastructure Management

Kubernetes workers

pod | pod | pod | pod | pod | pod

NVIDIA NIM | NVIDIA GPU OPERATOR | NVIDIA NETWORK OPERATOR

containerd

Red Hat Enterprise Linux | ubuntu

Dell AI Factory

Storage

Dell PowerScale F600 - File

Dell ECS EX500 - Object

Networking

PowerSwitch S5232-ON or S5248-ON

Inferencing

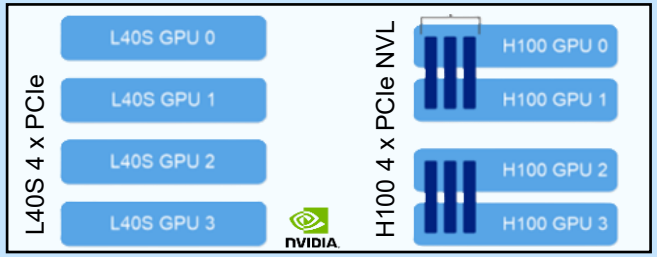
NVIDIA QM8790/QM9790 InfiniBand

Training

Compute

PowerEdge R760xa with L40 w/25 GbE

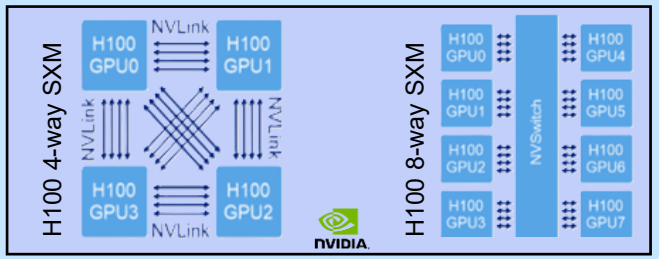
PowerEdge R760xa with H100 NVL w/100 GbE



Inferencing

PowerEdge XE8640

PowerEdge XE9680



Training

A different approach might be needed?

AMD DELL Technologies

Dell Private Cloud

Hypervisor Freedom

Dell AIOPs
SaaS

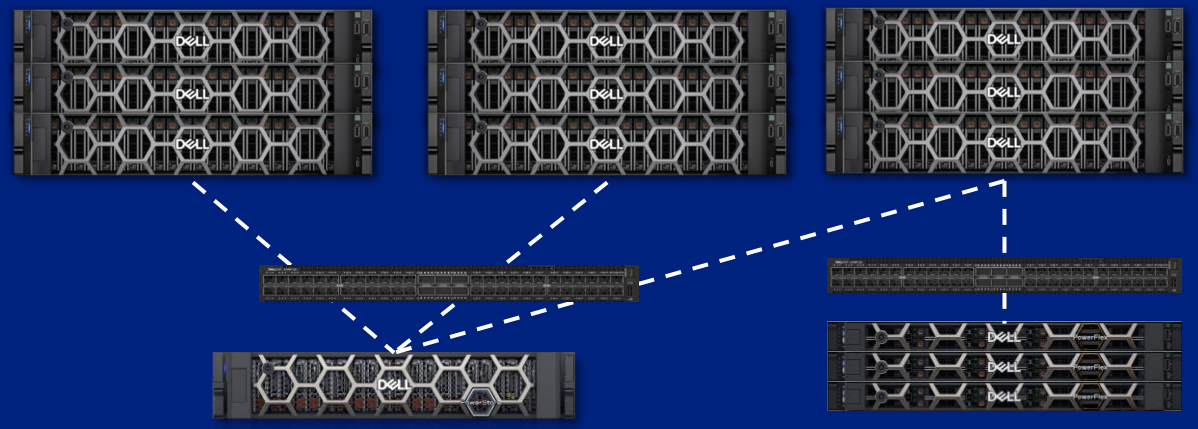
Dell Automation Platform
SaaS or On-Premises
Portal | Onboarding | Asset Mgmt | Catalog | Blueprints | Orchestrator
Multi-System/Cluster | Users & Access Mgmt | Connectivity | Entitlements

Dell Private Cloud

Dell Private Cloud
On-Premises

Day 1 & 2 automation
Known good state
Full Stack Upgrades
Cloud OS & Storage integration
Assurance
Solution support

Dell Private Cloud SW		DPC Extension + Dell Private Cloud SW
Cloud OS	*Use your Own License*	VMware vSphere® / Red Hat OpenShift / AHV
Dell PowerEdge	*New or Existing*	
Networking	*Bring your own*	
Dell Storage	*New or Existing*	



Dell NativeEdge
On-Premises

Dell AI Solutions
On-Premises

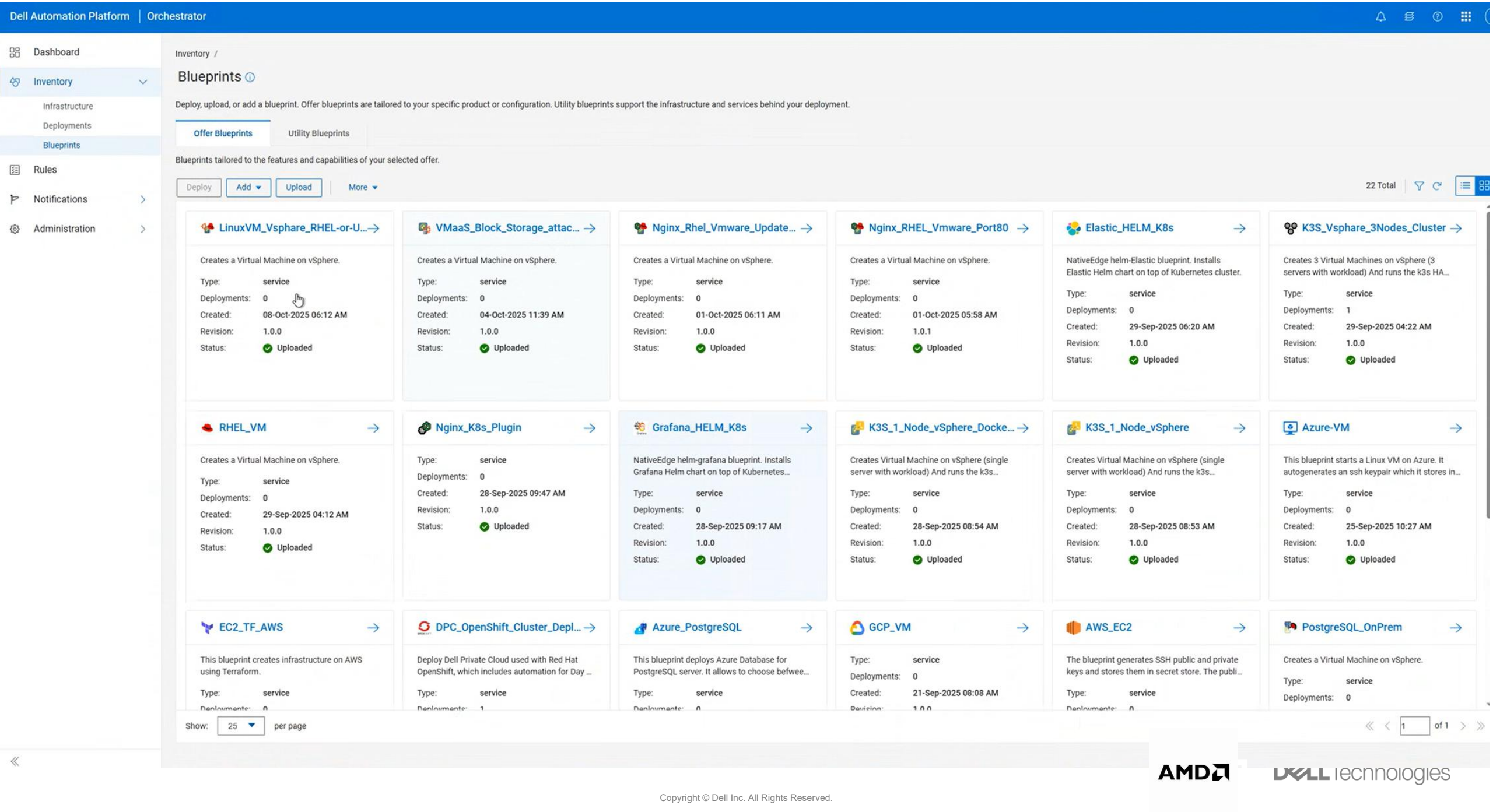
Dell Automation Studio
On-Premises

Operationally consistent Flexibility, Choice, and Control Investment Protection

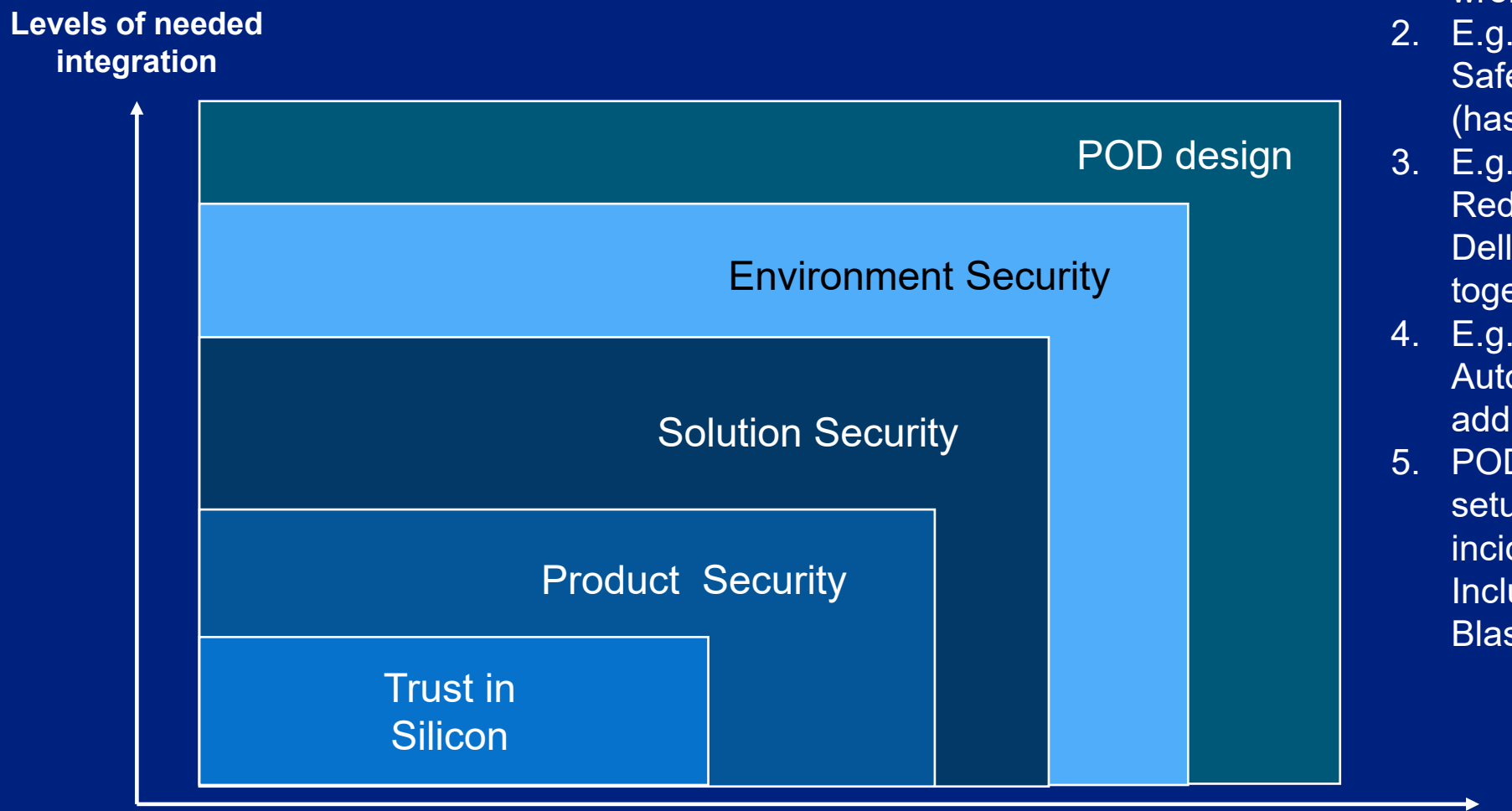
Secure by design

Secure Supply Chain – Hardware & Software

AMD DELL Technologies



Secure by Design – layered defense



1. Crypto graphical footprint of Chips = no wrong chips anywhere
2. E.g. a Server security Features like Safe bios process, Safe driver process (hash'ed driver packages) etc.
3. E.g. Dell Validated design for Red Hat – Red Hat security features on top of Dell's product security – all validated together
4. E.g. Dell Private Cloud with Dell Automation Platform – on top of no. 3. additional certifications
5. POD design. With the correct network setup, PODs can be protected from incidents e.g., from other PODs. Including reducing Attack Surface and Blast Radius

Operationally consistent
Flexibility, Choice, and Control
Investment Protection

Secure by design

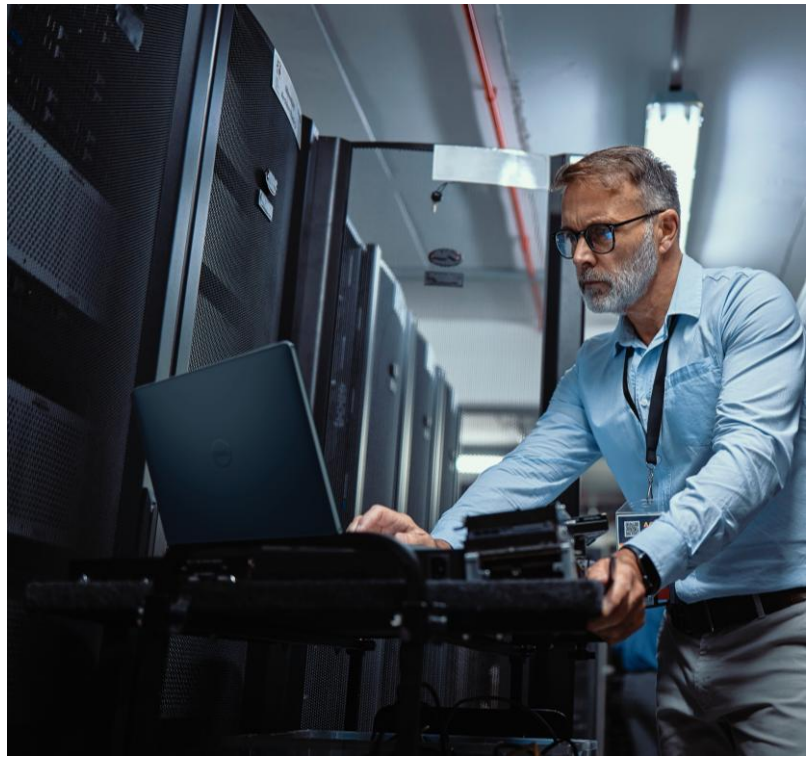
Secure Supply Chain – Hardware & Software

AMD DELL Technologies

Strengthen security

Legacy servers weren't built for today's threat landscape. Modernize your stack with embedded cyber resiliency to build zero-trust architecture.

- **Enable zero trust by design:** PowerEdge servers combine silicon-based root of trust (RoT), secure boot, and a Cyber Resilient Architecture to help enforce least-privilege access and maintain a continuous chain of trust.
- **Reduce risk from the hardware up:** PowerEdge servers validate firmware integrity at every boot or A/C cycle with a silicon-based RoT.
- **Extend trust through the full boot process:** iDRAC integrates with AMD Platform Secure Boot (PSB) to validate BIOS and OS bootloader integrity.[1]
- **Protect data in use without performance tradeoffs:** AMD Secure Memory Encryption and Secure Encrypted Virtualization – Encrypted State protect virtualized environments while maintaining performance.[2]
- **Ensure component authenticity**: iDRAC uses the Security Protocol and Data Model (SPDM) to validate hardware and I/O cards, helping create a dependable, secure environment.[3]



1. https://infohub.delltechnologies.com/en-us/p/securing-the-digital-frontier-inside-dell-and-amd-s-zero-trust-approach/
2. https://infohub.delltechnologies.com/en-us/p/enable-security-features-w-o-impact-to-oltp-performance-for-dell-poweredge-servers-with-amd-epyc-processors/
3. https://www.dell.com/support/manuals/en-us/idrac9-lifecycle-controller-v7.x-series/idrac9_scg_tta/security-protocol-and-data-model?guid=guid-861a0182-acd4-4811-930c-837235d8b475&lang=en-us

AMD DELL Technologies

Zero-trust by design in Dell Private Cloud with Dell Automation Platform

Identity	Verified for every user, endpoint, and service
Device	Hardware-rooted attestation and registration
Network	Enforced encryption, micro-segmentation, and mutually authenticated service flows
Application workload	Blueprint-level identity and integrity controls
Data	Secured, encrypted, and policy-governed data
Visibility and analytics	Continuous monitoring across identity, configuration, and deployment events
Automation and orchestration	Policy-driven enforcement that is tightly embedded into operations

Dell Automation Platform is built in accordance with **National Institute of Standards and Technology (NIST)** Zero Trust Architecture (SP 800-207) and **incorporates all seven pillars of modern zero trust:**

Zero trust is not an add-on in Dell Automation Platform, but rather it is the **foundation upon which automation, blueprinting, and lifecycle management are constructed.**

AMD DELL Technologies

Zero-trust by design in Dell Private Cloud with Dell Automation Platform

Audit logging and forensics

Dell Automation Platform implements security logging in compliance with the **Office of Management and Budget (OMB) Memorandum M-21-31**.
This includes:

- Structured audit logs
- Complete traceability of user actions and system events
- Blueprint lifecycle logging
- API usage and integration monitoring
- Support for Security Information and Event Management (SIEM) ingestion

This ensures an auditable and forensically sound operational environment.

Native compliance alignment

Dell Automation Platform simplifies organizational security certifications by providing integrated alignment with:

- ISO 27001 controls (ISO 27001 certified)
- SOC 2 principles (SOC 2 Type 1 attested)
- NIST Zero Trust (SP 800-207) (compliant)
- Secure configuration baselines (CIS/STIG) (compliant)
- VPAT 508 accessibility (VPAT 508 attested)
- USGv6 compliance (USGv6 certified)

This helps reduce the audit burden and accelerates compliance adoption across mission-critical infrastructure.

AMD DELL Technologies

Overcome security barriers of enterprise-scale AI

Recently research shows that 87% of security leaders say AI is significantly increasing the number of threats that require attention[1].

Secure your supply chain

Minimize risks of integrating public models, data and repositories.

Secure your operations

Protect training and data management operations with continuous development and integration.

Secure your run time

Ensure safe AI execution with security visibility and resilience across the stack.

AMD DELL Technologies

AI Factory

Data resilient framework to protect AI / Data at scale

DELL Technologies

DATA

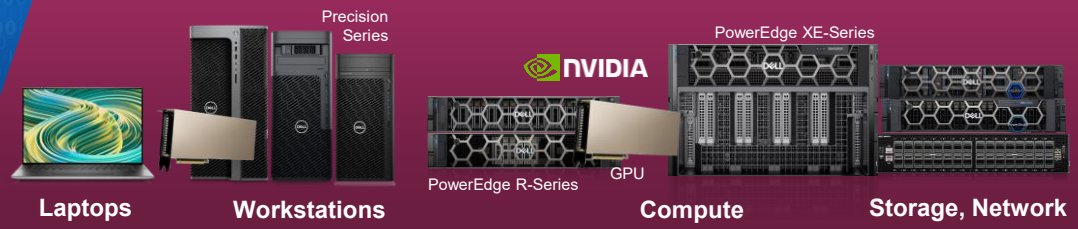
SERVICES

Strategy | Data | Platform | Use Case | Operate & Scale

AI SOFTWARE

APPS | MODELS | SOLUTIONS | FRAMEWORKS & TOOLS

INFRASTRUCTURE



Laptops | Workstations | Compute | Storage, Network

USE CASES

- Digital & Support Assistants
- Content & Code Generation
- Data creation
- Natural Language Search

Security & Resiliency Services

- Resiliency Program Management
- Data Privacy and Security
- Application Continuity Automation
- Layered Defense

AMD DELL Technologies

AI Factory

Data resilient framework to protect AI / Da

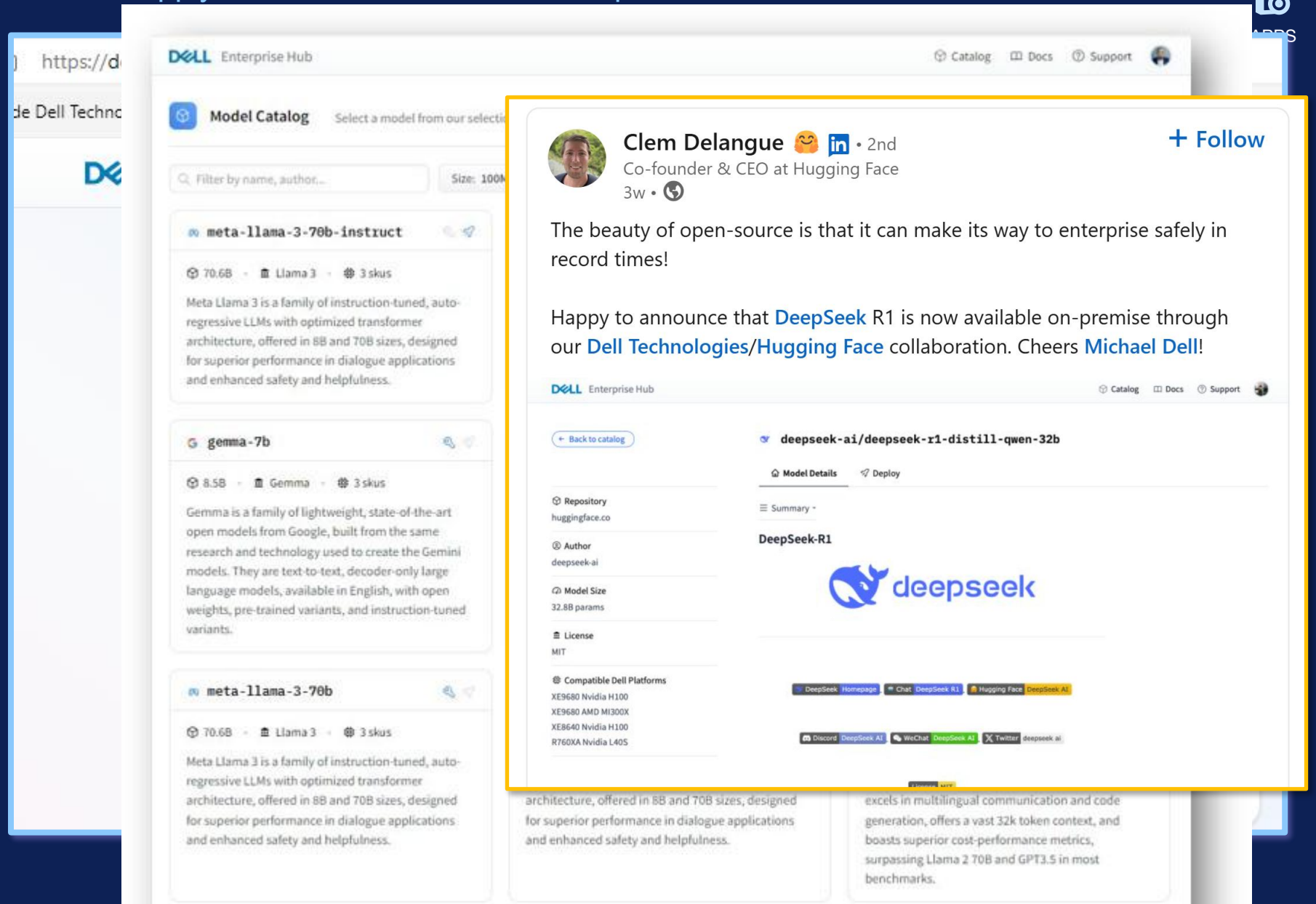
200+ Dell AI Factory new releases

4,000+ New Customers

AMD DELL Technologies

Making AI Secure (& easy): Dell Enterprise Hub on Hugging Face

Secure supply chain for AI models and components.



MODELS SOLUTIONS FRAMEWORKS & TOOLS

- ✓ **Authenticated portal** on Hugging Face for Dell customers
- ✓ **Optimized open-source models** for Dell infrastructure
- ✓ **Custom, dedicated containers**, scripts and technical documents
- ✓ **All included software dependencies** and platform specific optimizations
- ✓ **Accelerate time-to-value** with on-premises deployment
- ✓ **Accelerator service** for rapid prototyping

AMD DELL Technologies

Summary

The executive summary – attacks cannot be prevented by acquiring another FireWall

Secure by consume

Sovereign
Share nothing

No Mixed responsibilities
Full Oversight – easy managed by AI

Think beyond the FireWall

Start AI with Security

Shadow AI might be more dangerous than Shadow IT

DELL Technologies

AMD

Thank you

DELL Technologies

AMD