

DATA CENTERS DENMARK

Conference & Exhibition

29-30 April 2026

Dell Technologies inspiration — Secure by Design - The data centers of the future in the AI Era

Poul Kjeldgaard – Field CTO

It is about what we put in our Datacenter 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 created 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.

Hackers don't give a shit:



KIWICON III
28TH & 29TH NOVEMBER 2009

New Zealand's Hacker con - Wellington

- About your project's scope
- It's managed by a third party
- It's a legacy system
- It's "too critical to patch"
- About your outage windows
- About your budget
- You've always done it that way
- About your Go-Live Date
- It's only a pilot/proof of concept
- About Non-Disclosure Agreements
- It wasn't a requirement in the contract
- It's an internal system
- It's really hard to change
- It's due for replacement
- You're not sure how to fix it
- It's handled in the Cloud
- About your Risk Register entry
- The vendor doesn't support that configuration
- It's an interim solution
- It's [insert standard here] compliant
- It's encrypted on disk
- The cost benefit doesn't stack up
- "Nobody else could figure that out"
- You can't explain the risk to "The Business"
- You've got other priorities
- About your faith in the competence of your internal users
- You don't have a business justification
- You can't show Return on Investment
- You contracted out that risk

Access to innovation - Dell Technologies Capital



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%

Technologies

Capital offers a unique blend of... bring best-in-class technological... s savvy to the board room table, and... the growth of your company as any

Reference: Dell Technologies – Zero Trust for DoD

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



Project Fort Zero

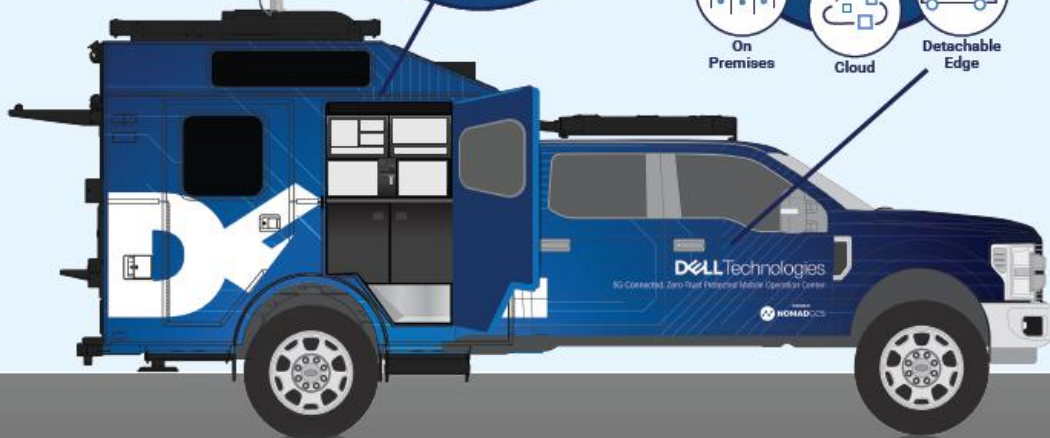
Detachable Edge deployment model: 5G-connected, Zero Trust-protected, mobile operation vehicle

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.*

COA 2

Commercial Cloud

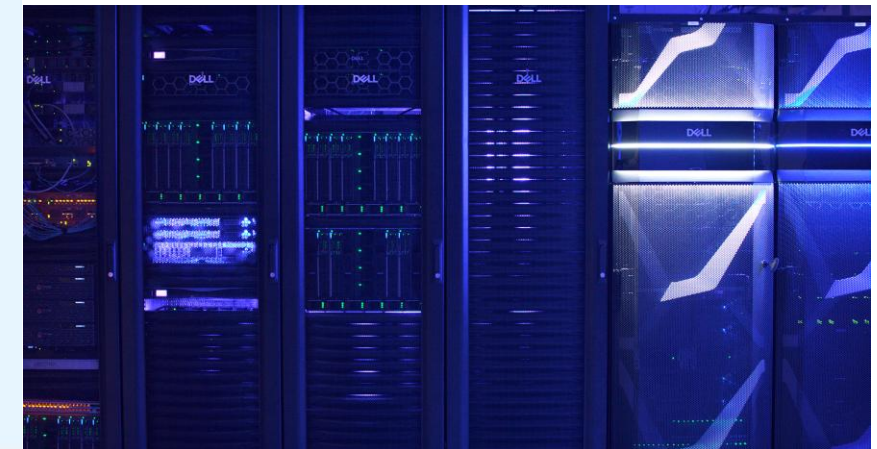
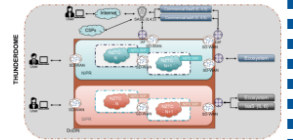
- Relies on commercial provider(s) to develop ZT compliant cloud environments using Greenfield approach
- Achieves DoD ZT quicker than COA-1
- Mandate would be to achieve DoD ZT "Target" level, at a minimum
- Provides standardized tools and capabilities to support ZT execution



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



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

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.

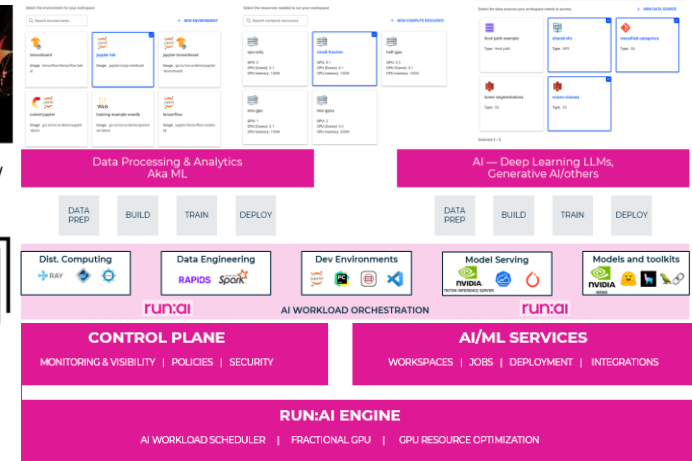
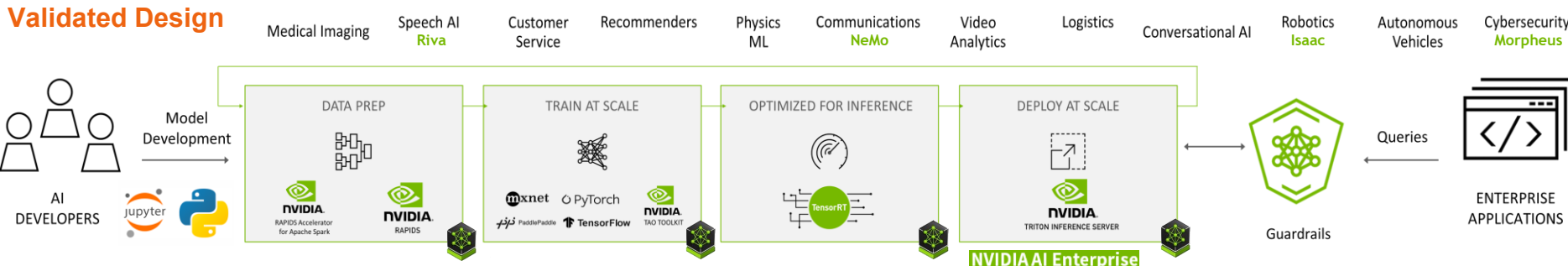
TRENDING

- 1 OpenSSH Flaw 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 Easily Exploitable 'Pack2TheRoot' Linux Vulnerability Leads to Root Access
- 6 Robinhood Vulnerability Exploited for Phishing Attacks
- 7 No Patch for New Phishing Escalation Technique in WhatsApp
- 8 Energy and Water Management Firm Itron Hacked

Daily Briefing News

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



Open AI Models

NVIDIA Pretrained Models

NVIDIA AI Enterprise

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

Infrastructure Management

Kubernetes workers

NVIDIA NIM, GPU OPERATOR, 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

L40S 4 x PCIe

H100 4 x PCIe NVL

Inferencing

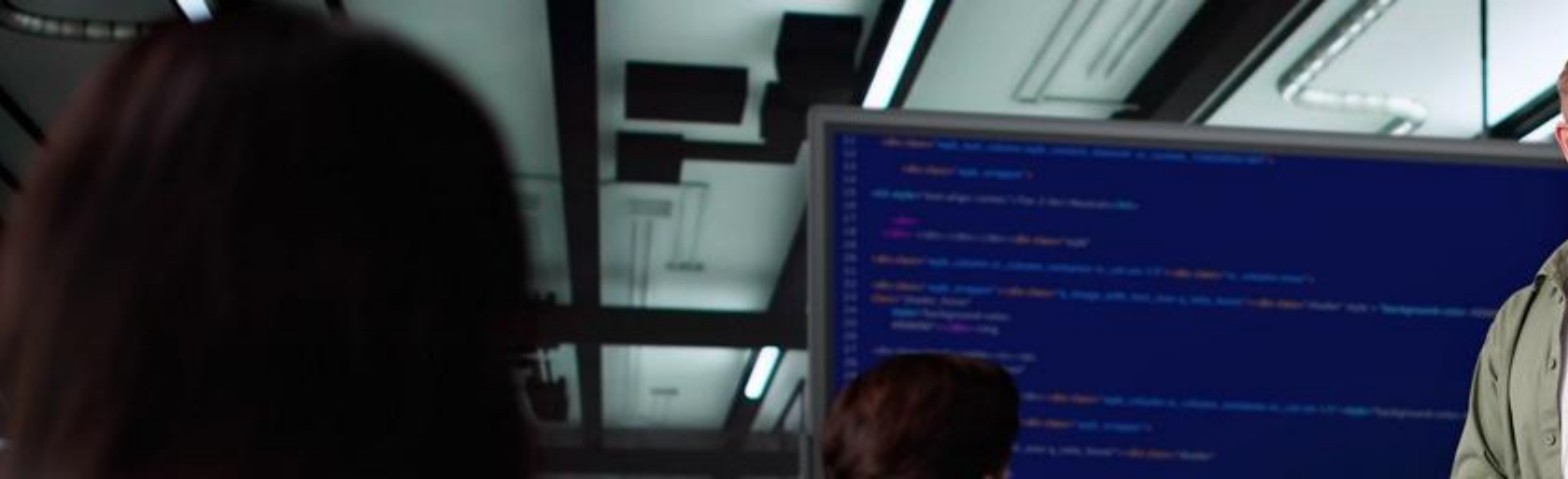
PowerEdge XE8640

PowerEdge XE9680

H100 4-way SXM

H100 8-way SXM

Training



A different approach
might be needed?

Dell Private Cloud

Hypervisor Freedom

Dell Automation Platform

SaaS or On-Premises

Portal | Onboarding | Asset Mgmt | Catalog | Blueprints | Orchestrator
Multi-System/Cluster | Users & Access Mgmt | Connectivity | Entitlements

Dell AIOPs
SaaS



Dell Private Cloud

Dell Private Cloud On-Premises

Dell Private Cloud SW

DPC Extension

Dell Private Cloud SW

Cloud OS



DPC Extension

Dell Private Cloud SW

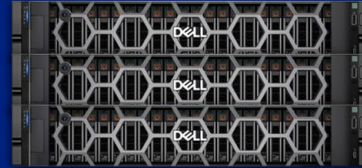


DPC Extension

Dell Private Cloud SW



Dell PowerEdge



Networking



Dell Storage



Dell NativeEdge
On-Premises



Dell AI Solutions
On-Premises



Dell Automation Studio
On-Premises



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

Use your Own License

New or Existing

Bring your own

New or Existing

Operationally consistent
Flexibility, Choice, and Control
Investment Protection

Secure by design

Secure Supply Chain –
Hardware & Software



- Dashboard
- Inventory**
 - Infrastructure
 - Deployments
 - Blueprints**
- Rules
- Notifications
- Administration

Inventory /

Blueprints ⓘ

Deploy, upload, or add a blueprint. Offer blueprints are tailored to your specific product or configuration. Utility blueprints support the infrastructure and services behind your deployment.

Offer Blueprints Utility Blueprints

Blueprints tailored to the features and capabilities of your selected offer.

Deploy Add ▾ Upload More ▾

22 Total 🔍 🔄 ☰

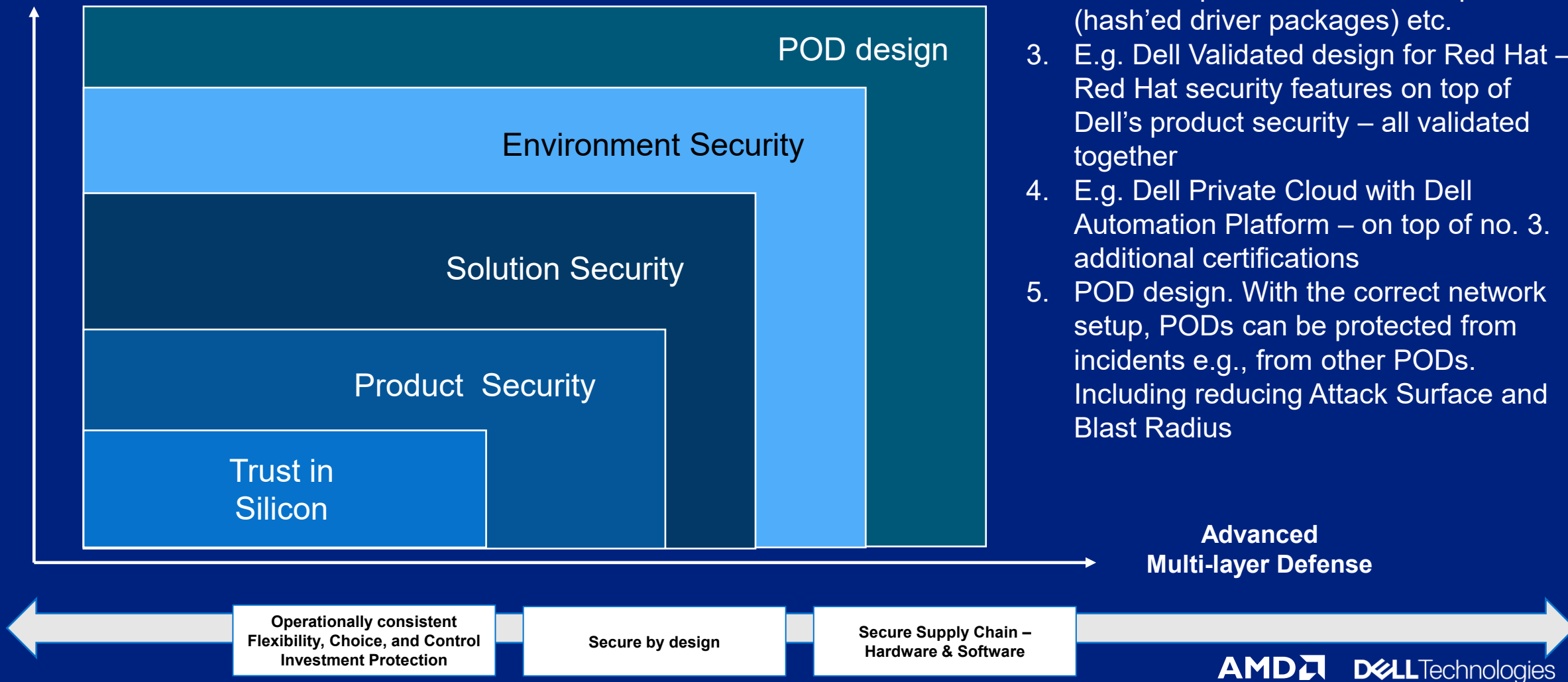
<p>LinuxVM_Vsphere_RHEL-or-U... →</p> <p>Creates a Virtual Machine on vSphere.</p> <p>Type: service</p> <p>Deployments: 0</p> <p>Created: 08-Oct-2025 06:12 AM</p> <p>Revision: 1.0.0</p> <p>Status: Uploaded</p>	<p>VaaS_Block_Storage_attac... →</p> <p>Creates a Virtual Machine on vSphere.</p> <p>Type: service</p> <p>Deployments: 0</p> <p>Created: 04-Oct-2025 11:39 AM</p> <p>Revision: 1.0.0</p> <p>Status: Uploaded</p>	<p>Nginx_Rhel_Vmware_Update... →</p> <p>Creates a Virtual Machine on vSphere.</p> <p>Type: service</p> <p>Deployments: 0</p> <p>Created: 01-Oct-2025 06:11 AM</p> <p>Revision: 1.0.0</p> <p>Status: Uploaded</p>	<p>Nginx_RHEL_Vmware_Port80 →</p> <p>Creates a Virtual Machine on vSphere.</p> <p>Type: service</p> <p>Deployments: 0</p> <p>Created: 01-Oct-2025 05:58 AM</p> <p>Revision: 1.0.1</p> <p>Status: Uploaded</p>	<p>Elastic_HELM_K8s →</p> <p>NativeEdge helm-Elastic blueprint. Installs Elastic Helm chart on top of Kubernetes cluster.</p> <p>Type: service</p> <p>Deployments: 0</p> <p>Created: 29-Sep-2025 06:20 AM</p> <p>Revision: 1.0.0</p> <p>Status: Uploaded</p>	<p>K3S_Vsphere_3Nodes_Cluster →</p> <p>Creates 3 Virtual Machines on vSphere (3 servers with workload) And runs the k3s HA...</p> <p>Type: service</p> <p>Deployments: 1</p> <p>Created: 29-Sep-2025 04:22 AM</p> <p>Revision: 1.0.0</p> <p>Status: Uploaded</p>
<p>RHEL_VM →</p> <p>Creates a Virtual Machine on vSphere.</p> <p>Type: service</p> <p>Deployments: 0</p> <p>Created: 29-Sep-2025 04:12 AM</p> <p>Revision: 1.0.0</p> <p>Status: Uploaded</p>	<p>Nginx_K8s_Plugin →</p> <p>Type: service</p> <p>Deployments: 0</p> <p>Created: 28-Sep-2025 09:47 AM</p> <p>Revision: 1.0.0</p> <p>Status: Uploaded</p>	<p>Grafana_HELM_K8s →</p> <p>NativeEdge helm-grafana blueprint. Installs Grafana Helm chart on top of Kubernetes...</p> <p>Type: service</p> <p>Deployments: 0</p> <p>Created: 28-Sep-2025 09:17 AM</p> <p>Revision: 1.0.0</p> <p>Status: Uploaded</p>	<p>K3S_1_Node_vSphere_Docke... →</p> <p>Creates Virtual Machine on vSphere (single server with workload) And runs the k3s...</p> <p>Type: service</p> <p>Deployments: 0</p> <p>Created: 28-Sep-2025 08:54 AM</p> <p>Revision: 1.0.0</p> <p>Status: Uploaded</p>	<p>K3S_1_Node_vSphere →</p> <p>Creates Virtual Machine on vSphere (single server with workload) And runs the k3s...</p> <p>Type: service</p> <p>Deployments: 0</p> <p>Created: 28-Sep-2025 08:53 AM</p> <p>Revision: 1.0.0</p> <p>Status: Uploaded</p>	<p>Azure-VM →</p> <p>This blueprint starts a Linux VM on Azure. It autogenerates an ssh keypair which it stores in...</p> <p>Type: service</p> <p>Deployments: 0</p> <p>Created: 25-Sep-2025 10:27 AM</p> <p>Revision: 1.0.0</p> <p>Status: Uploaded</p>
<p>EC2_TF_AWS →</p> <p>This blueprint creates infrastructure on AWS using Terraform.</p> <p>Type: service</p> <p>Deployments: 0</p>	<p>DPC_OpenShift_Cluster_Depl... →</p> <p>Deploy Dell Private Cloud used with Red Hat OpenShift, which includes automation for Day ...</p> <p>Type: service</p> <p>Deployments: 1</p>	<p>Azure_PostgreSQL →</p> <p>This blueprint deploys Azure Database for PostgreSQL server. It allows to choose betwee...</p> <p>Type: service</p> <p>Deployments: 0</p>	<p>GCP_VM →</p> <p>Type: service</p> <p>Deployments: 0</p> <p>Created: 21-Sep-2025 08:08 AM</p> <p>Revision: 1.0.0</p>	<p>AWS_EC2 →</p> <p>The blueprint generates SSH public and private keys and stores them in secret store. The publi...</p> <p>Type: service</p> <p>Deployments: 0</p>	<p>PostgreSQL_OnPrem →</p> <p>Creates a Virtual Machine on vSphere.</p> <p>Type: service</p> <p>Deployments: 0</p>

Show: 25 per page

1 of 1

Secure by Design – layered defense

Levels of needed integration



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

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

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.**



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.



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 attention¹.



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.

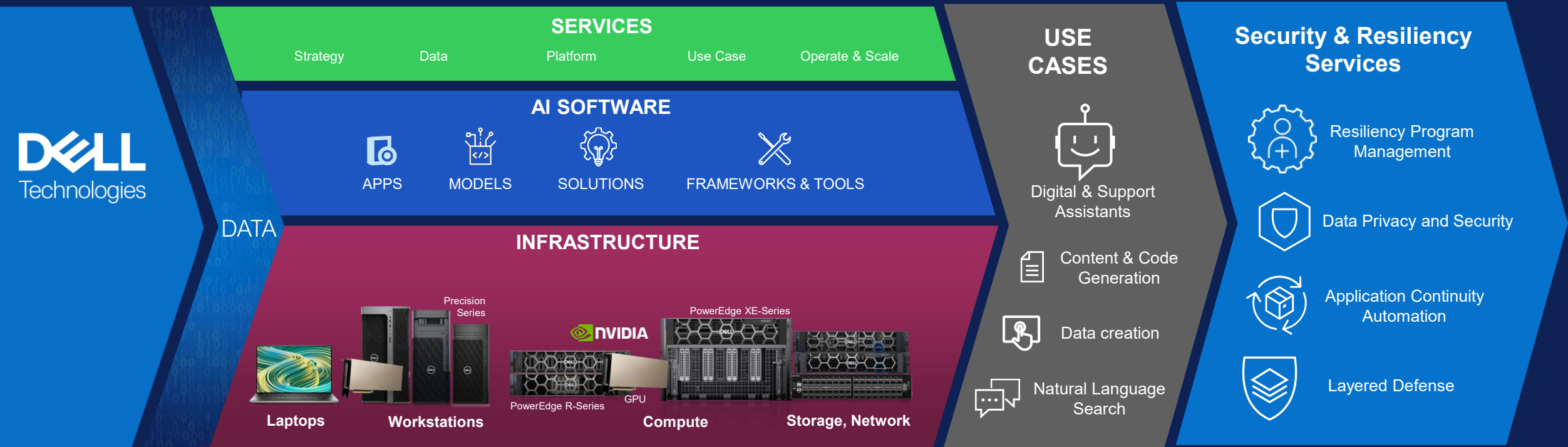


Secure your run time

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

AI Factory

Data resilient framework to protect AI / Data at scale



AI Factory

Data resilient framework to protect AI / Data



OWASP | **TOP 10** LLM APPLICATIONS & GENERATIVE AI

OWASP Top 10 for LLM Applications 2025

Version 2025
November 18, 2024

OWASP PDF v4.2.0a 20241114-202703

200+ Dell AI Factory new releases

4,000+ New Customers

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

Secure supply chain for AI models and components.



https://d...
de Dell Techno



Dell Enterprise Hub

Catalog Docs Support

Model Catalog Select a model from our selection

Filter by name, author... Size: 100B

meta-llama-3-70b-instruct

70.6B · Llama 3 · 3 skus

Meta Llama 3 is a family of instruction-tuned, auto-regressive LLMs with optimized transformer architecture, offered in 8B and 70B sizes, designed for superior performance in dialogue applications and enhanced safety and helpfulness.

gemma-7b

8.5B · Gemma · 3 skus

Gemma is a family of lightweight, state-of-the-art open models from Google, built from the same research and technology used to create the Gemini models. They are text-to-text, decoder-only large language models, available in English, with open weights, pre-trained variants, and instruction-tuned variants.

meta-llama-3-70b

70.6B · Llama 3 · 3 skus

Meta Llama 3 is a family of instruction-tuned, auto-regressive LLMs with optimized transformer architecture, offered in 8B and 70B sizes, designed for superior performance in dialogue applications and enhanced safety and helpfulness.



Clem Delangue · 2nd
Co-founder & CEO at Hugging Face
3w ·

+ Follow

The beauty of open-source is that it can make its way to enterprise safely in record times!

Happy to announce that **DeepSeek R1** is now available on-premise through our **Dell Technologies/Hugging Face** collaboration. Cheers **Michael Dell!**

Dell Enterprise Hub

Catalog Docs Support

← Back to catalog

deepseek-ai/deepseek-r1-distill-qwen-32b

Model Details Deploy

Summary

DeepSeek-R1



Repository
huggingface.co

Author
deepseek-ai

Model Size
32.8B params

License
MIT

Compatible Dell Platforms
XE9680 Nvidia H100
XE9680 AMD MI300X
XE8640 Nvidia H100
R760XA Nvidia L40S

DeepSeek Homepage Chat DeepSeek R1 Hugging Face DeepSeek AI

Discord DeepSeek AI WeChat DeepSeek AI Twitter deepseek.ai

architecture, offered in 8B and 70B sizes, designed for superior performance in dialogue applications and enhanced safety and helpfulness.

excels in multilingual communication and code generation, offers a vast 32k token context, and boasts superior cost-performance metrics, surpassing Llama 2 70B and GPT3.5 in most benchmarks.

✓ 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



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

Thank you