Empowering Organizations with Cybersecurity and Resilience

Integrated Protection from Fleet to Infrastructure

Koen André Segers
Global Presales Lead Cybersecurity
Koen-Andre.Segers@dell.com

DELL Technologies

Security for the fleet and the infrastructure

Dell Trusted Workspace

Dell Trusted Infrastructure

PCs

Servers

Storage

Data Protection

World's most secure commercial PCs[1]

Hardware and software defenses for secure anywhere-work

Infrastructure designed with security in mind

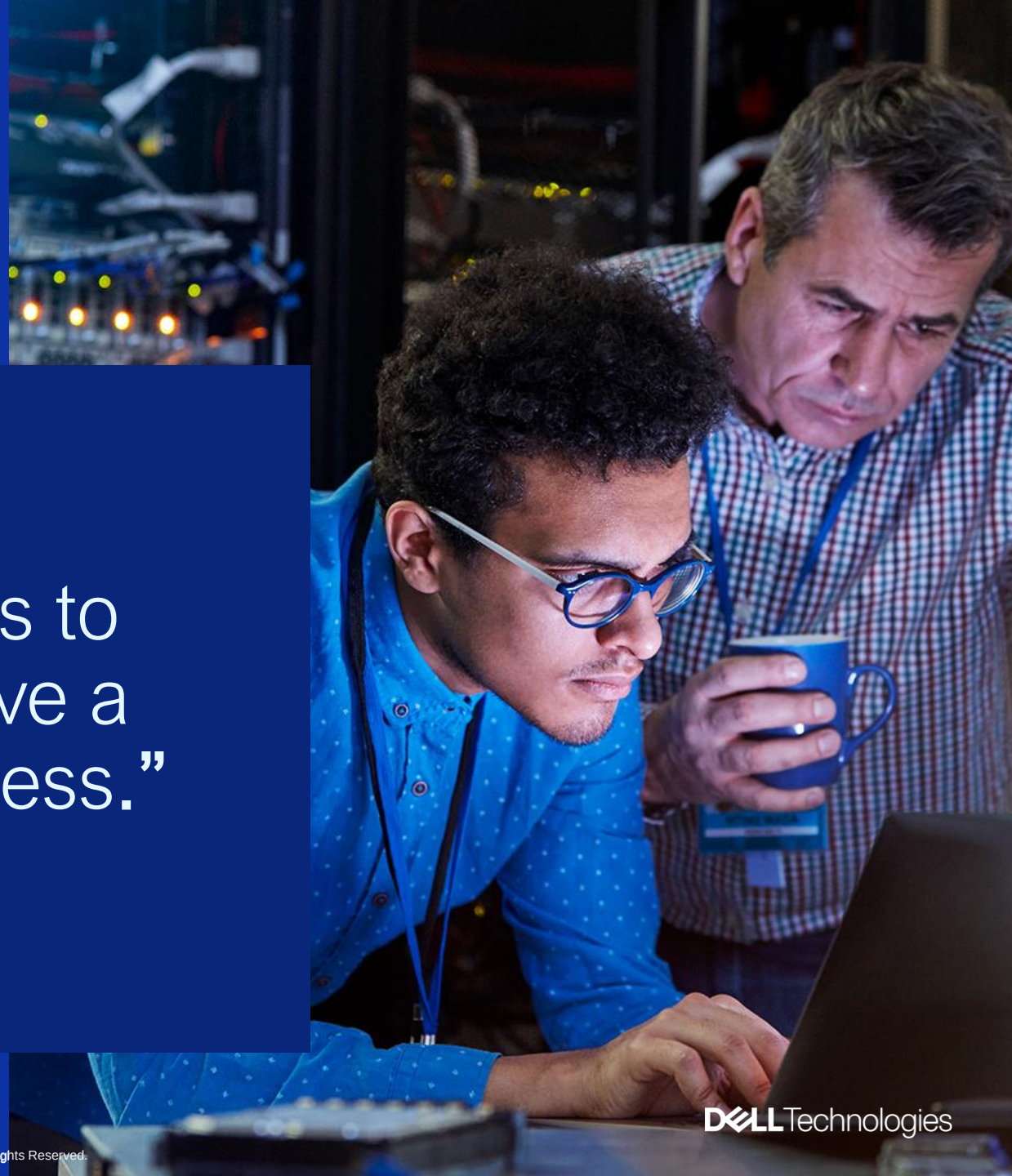
Robust security features built in including zero trust principles.

Services

Comprehensive expertise to prepare, detect, respond and recover

[1]*Based on Dell internal analysis, October 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features. Validated by Principled Technologies. A comparison of security features, April 2024.*

Prepare for the Worst-Case Scenario



> If a focused entity really wants to get into your system, they have a really high probability of success.”

Adm. Michael Rogers, former director of NSA and commander of U.S. Cyber Command

Mature security and resilience

To be successful, you need both

Security

Improve your security posture and reduce cyber risk by streamlining adoption, implementation and management of security tools and processes.

Reduce risk
Build trust
Reduce cost
Increase productivity
Reduce downtime
Fuel innovation

Resilience

Regularly assess business risk and resilience strategies, refining policies and procedures to reduce planned and unplanned downtime.

DELL Technologies

Threat funnel for cybersecurity & resilience

Minimize the vulnerabilities and entry points that can be exploited to compromise the environment.

Actively identify and address potential security incidents and malicious activities.

Restore the organization as quickly as possible while minimizing disruption.

Dell Trusted Workspace

Secure anywhere-work with hardware and software defenses built for today's cloud-based world

The world's most secure commercial AI PCs*

Software to improve the security of any fleet

Integrated Endpoint Security

CHALLENGE

IT-Security Gap

Emerging attack vectors can bypass traditional software-only security.

SOLUTION

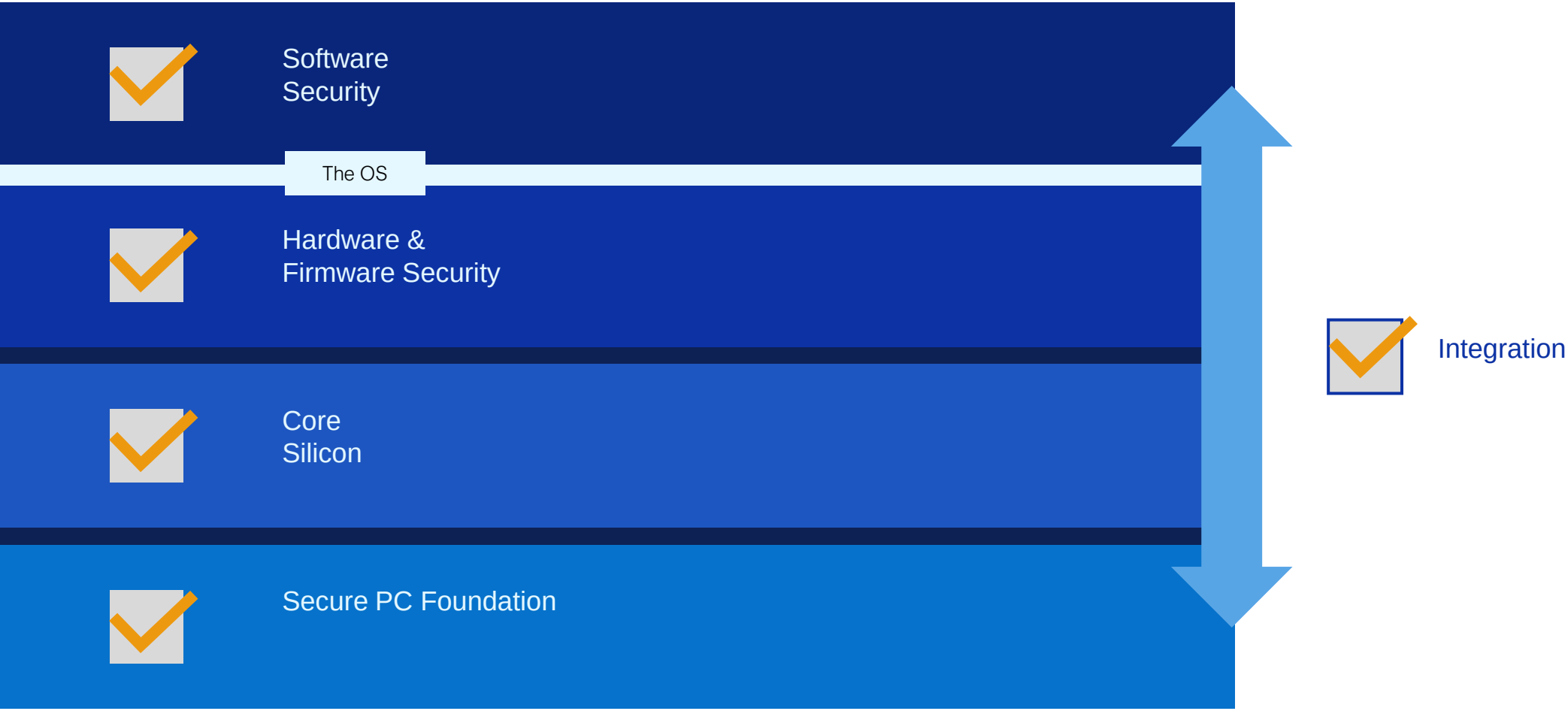
Hardware-Assisted Security

The PC manufacturer works directly with partners to develop integrations.

*Only Dell integrates with industry-leading software security**

What Modern Endpoint Security Looks Like

How Dell Can Help



An End-to-End Solution

Software Security

- CrowdStrike Flacon
- Absolute
- Microsoft Intune

The OS

Hardware & Firmware Security

- PC security leveraging Intel

Core Silicon

Secure PC Foundation

- Secure development lifecycle (SDL)
- Secure supply chain

Dell Trusted Device Application (telemetry)

Dell SafeBIOS
Indicators of Attack • BIOS Verification • Image Capture • CVE Detection

Dell Manageability Solutions
Dell Client Command • Dell Trusted Update Experience

Firmware verification | Below-the-OS silicon features | Intel Threat Detection Technology (TDT)

intel vPRO

DELL Technologies

Advanced Threat Protection

Ecosystem of best-of-breed partners to offer customers flexibility and choice through a broad portfolio of software solutions

Broad portfolio of third-party software

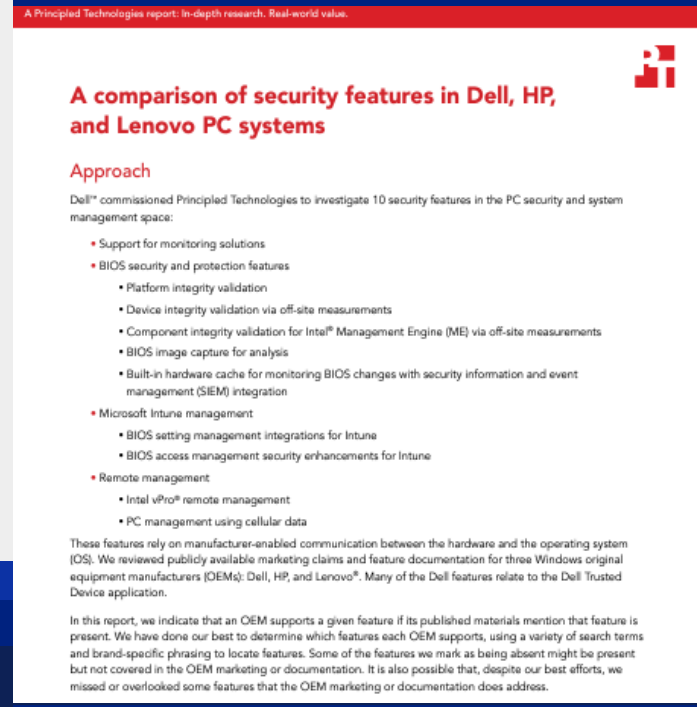
World’s Most Secure Commercial AI PCs*

Laptops

Desktops

Workstations

Principled Technologies found that Dell BIOS-level security wins vs. peers



A Principled Technologies report: In-depth research. Real-world value.

A comparison of security features in Dell, HP, and Lenovo PC systems

Approach

Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

- Support for monitoring solutions
- BIOS security and protection features
  - Platform integrity validation
  - Device integrity validation via off-site measurements
  - Component integrity validation for Intel® Management Engine (ME) via off-site measurements
  - BIOS image capture for analysis
  - Built-in hardware cache for monitoring BIOS changes with security information and event management (SIEM) integration
- Microsoft Intune management
  - BIOS setting management integrations for Intune
  - BIOS access management security enhancements for Intune
- Remote management
  - Intel vPro® remote management
  - PC management using cellular data

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs): Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device application.

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

Read the Study

DELL Technologies

intel vPRO

Hardware-Assisted Security

Dell | Intel | CrowdStrike

CROWDSTRIKE

In-memory exploit detection capabilities

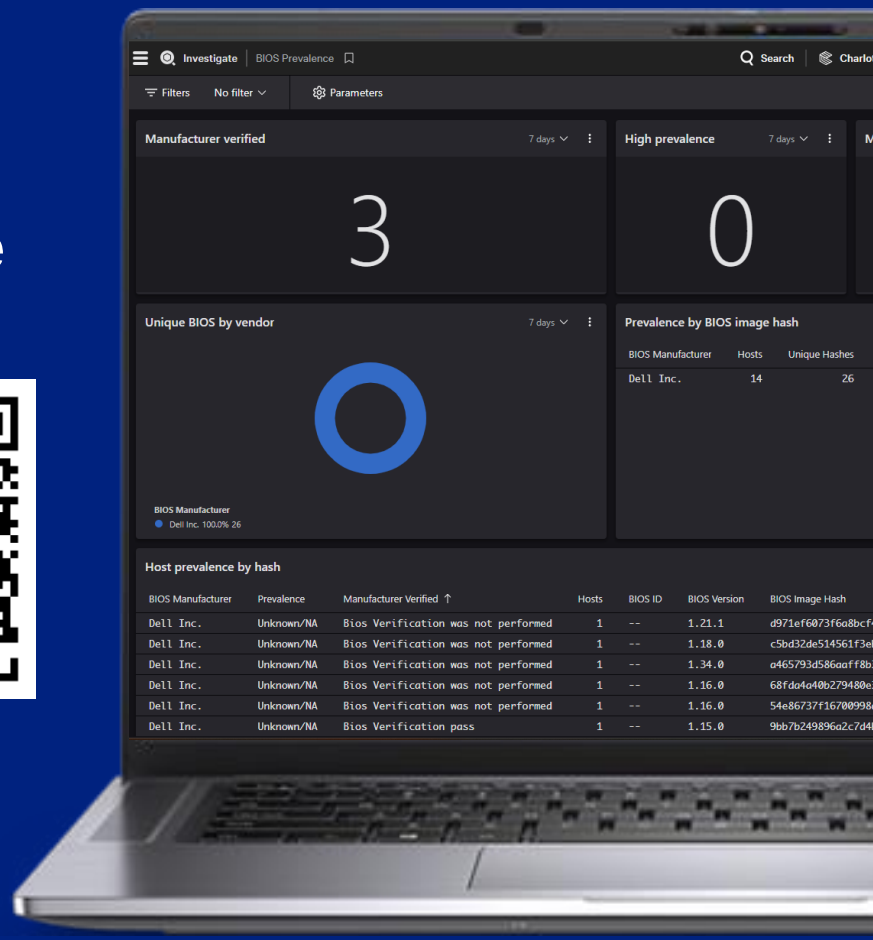
DELL Technologies

Secure devices and telemetry

intel.

More than a dozen Intel vPro optimizations

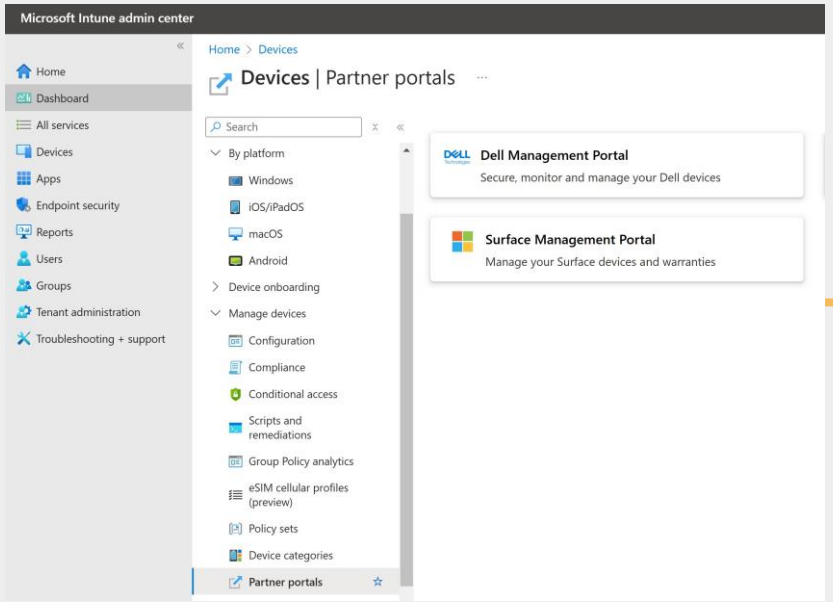
Demo the solution



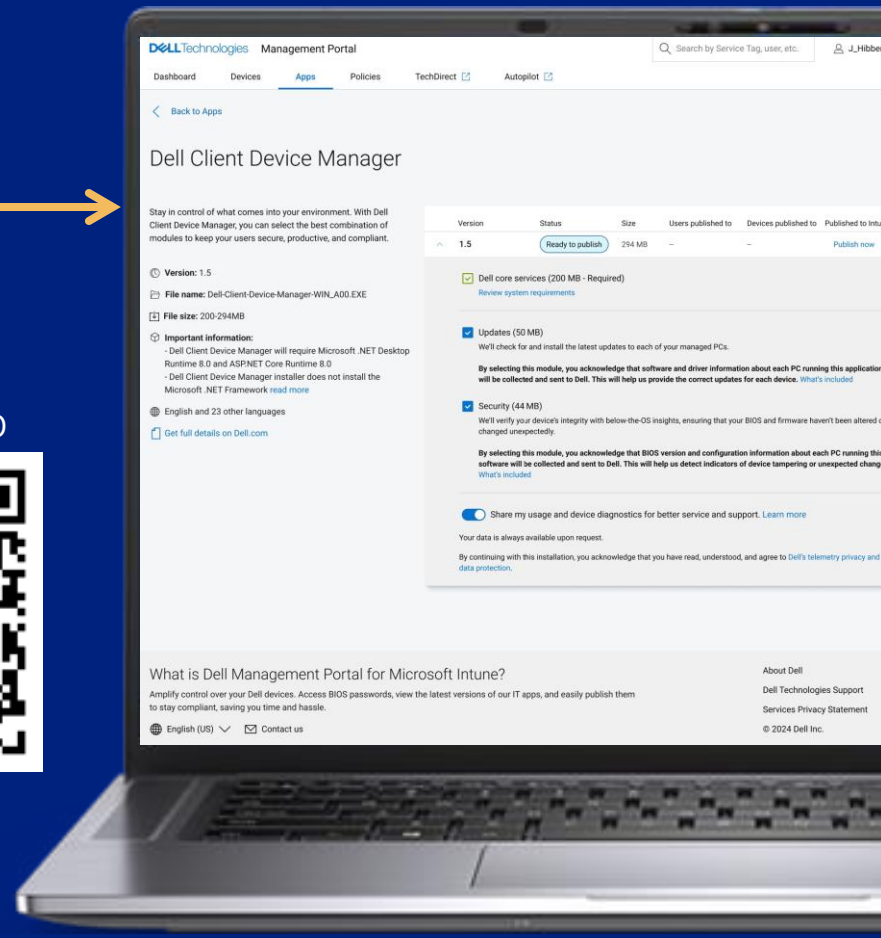
https://democenter.dell.com/interactive/ITD-0133

Endpoint Manageability

Dell | Intel | Microsoft Intune



Dell Trusted Device Demo



Most manageable commercial AI PCs*

Telemetry integrations streamline management

https://democenter.dell.com/interactive/ITD-0130

Security for the fleet and the infrastructure

Dell Trusted Workspace

Dell Trusted Infrastructure

PCs | Servers | Storage | Data Protection

World's most secure commercial PCs[1]

Hardware and software defenses for secure anywhere-work

Infrastructure designed with security in mind

Robust security features built in including zero trust principles.

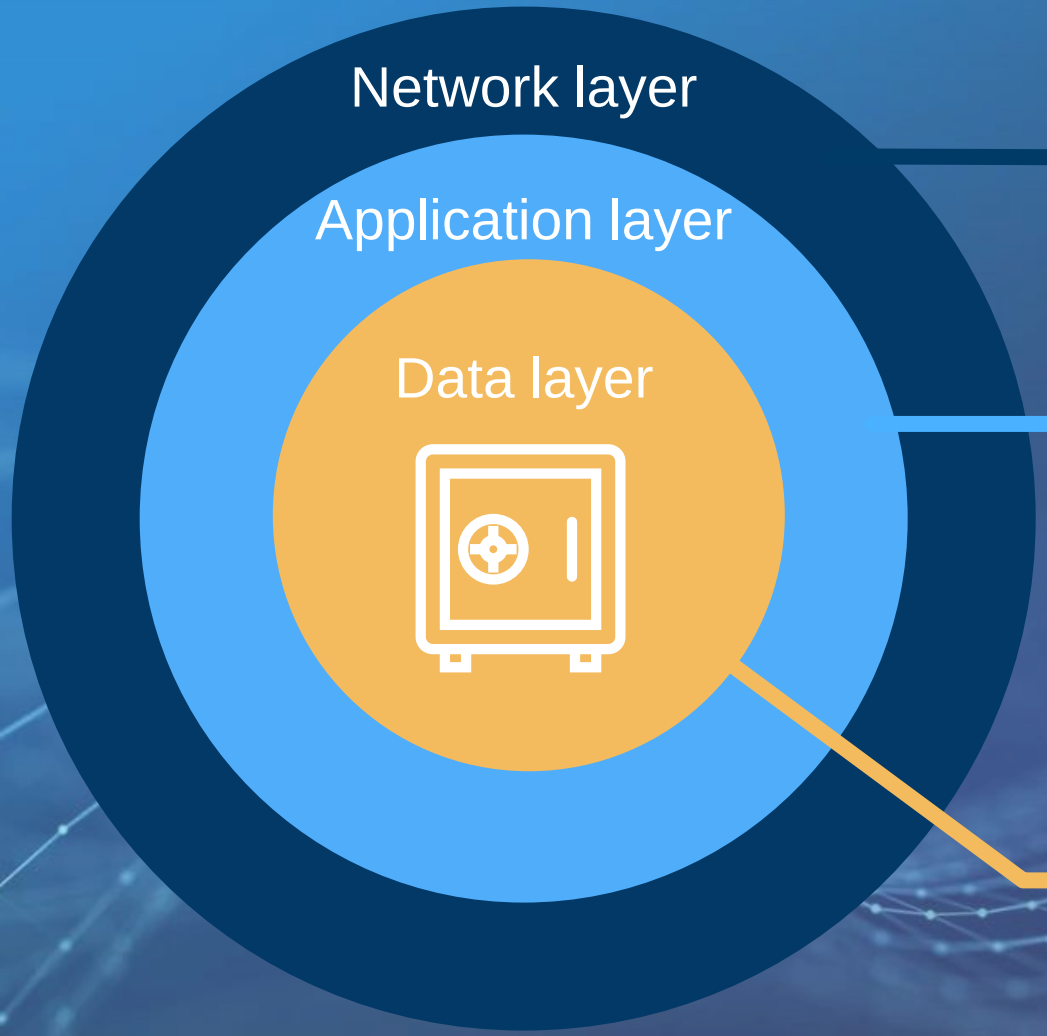
Services

Comprehensive expertise to prepare, detect, respond and recover

[1]*Based on Dell internal analysis, October 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features. Validated by Principled Technologies. A comparison of security features, April 2024.*

DELL Technologies

The Data Layer is the focus of many attacks

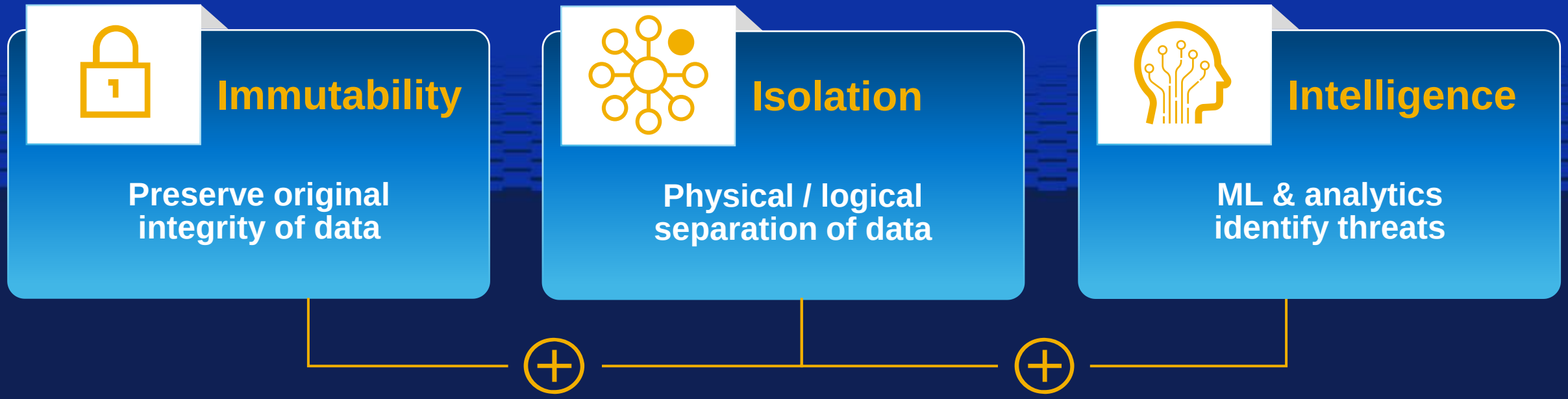


Multiple layers of security controls to protect your critical assets

Is your **data layer cyber resilient?**

DELL Technologies

Best Data Protection and Recovery Strategy



Secure Dell Storage solutions

Data isolation
Network separation with air-gapped vaults

Data immutability
Secure snapshots for granular recovery at scale

Intelligent detection
Monitors storage and data access for malicious activity to improve recovery

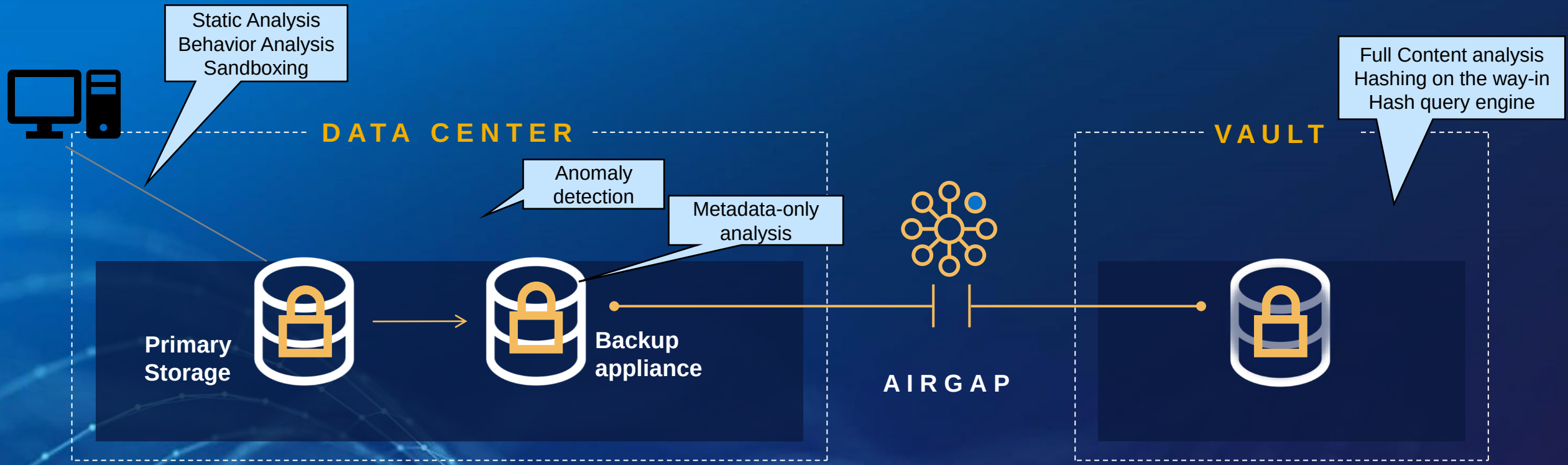
Federal certifications
STIG hardening, US DoD APL, IPv6 USGv6, Common Criteria, FIPS 140-2

Built in security
Hardware Root of Trust, secure boot, digitally signed firmware updates

Authentication and access
Role-based access control and multi-factor authentication

Data at rest encryption
Self-encrypting media and key management

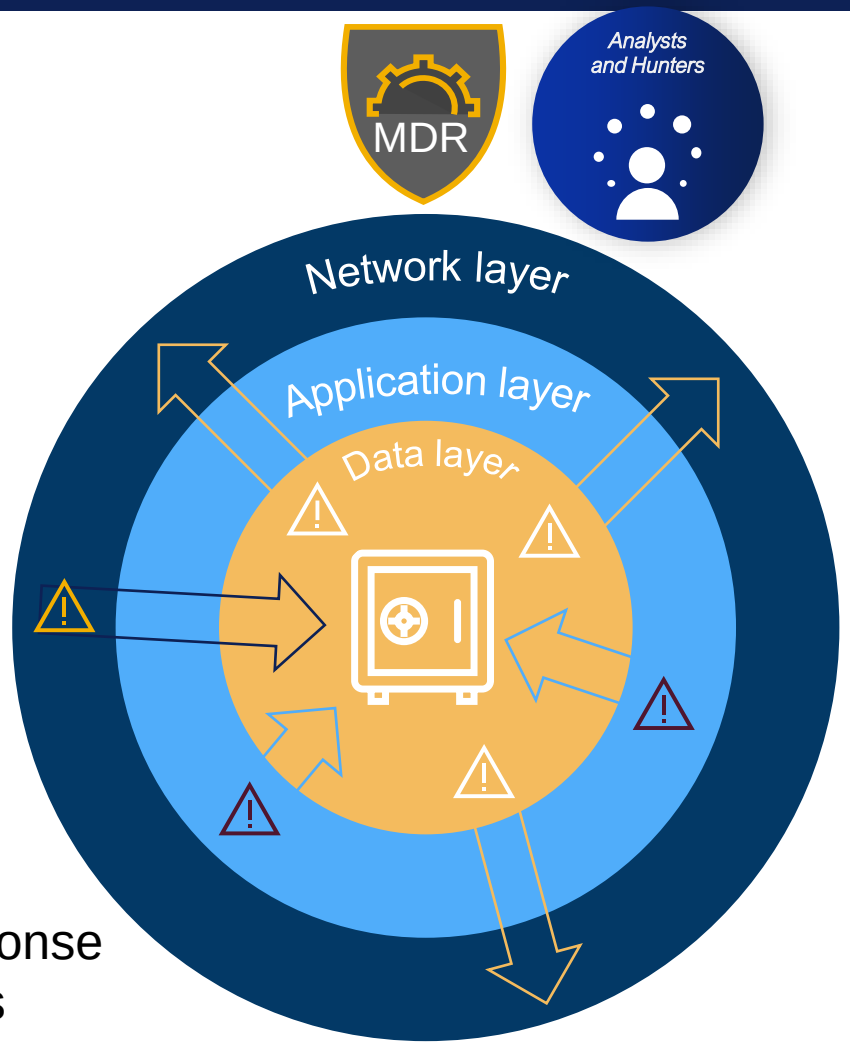
Intelligence. Detect Fast and with Confidence!



Immutability **Isolation** **Intelligence**

DELL Technologies

Multi-Layer Intelligence with incident correlation and API-based automation

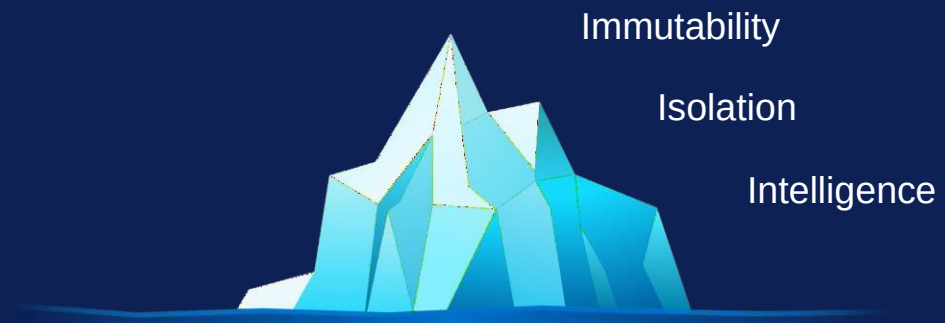


- 24/7 Global SOC
- Certified and Experienced Analysts
- Noise Reduction / Tuning
- Perform Complex Investigations
- Expertise to identify attack patterns
- Isolate or take actions on devices
- Threat Hunting
- Quarterly Reports

Two-way threat alerting and response between Security Operation tools

Defining Cyber Resilience

The perception is that this is enough…



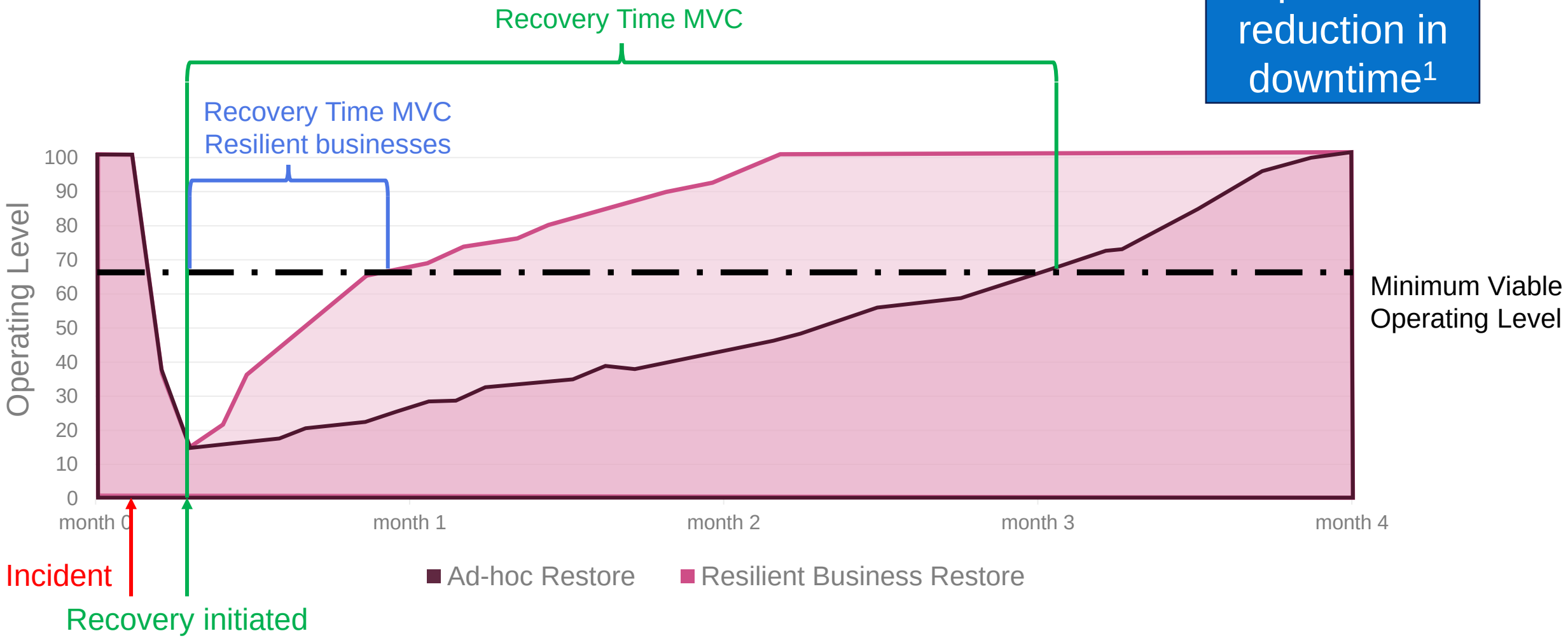
Multiple reports following real world events have indicated that *technology alone is simply not enough.*

Dell Technologies Cyber Resilience Capabilities:

Cyber Resilience as an Outcome

1) Forrester: The Total Economic Impact Of Dell PowerProtect Cyber Recovery

Up to 75% reduction in downtime[1]



https://www.pwc.co.uk/risk/assets/pdf/cyber-recovery-whitepaper-bridging-the-recovery-gap.pdf

Security for the fleet and the infrastructure

Dell Trusted Workspace

Dell Trusted Infrastructure

PCs | Servers | Storage | Data Protection

World's most secure commercial PCs[1]

Hardware and software defenses for secure anywhere-work

Infrastructure designed with security in mind

Robust security features built in including zero trust principles.

Services

Comprehensive expertise to prepare, detect, respond and recover

[1]*Based on Dell internal analysis, October 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features. Validated by Principled Technologies. A comparison of security features, April 2024.*

DELL Technologies

Why Dell for cybersecurity?

Largest security company you've never heard of

1. Size / experience
2. Embedded security
3. Partnerships
4. Integration
5. Service / support

Guardians of the gateway

Thank you

Let’s connect on the Dustin & Dell booth

DELL Technologies