dtuc.

Prevent Threats with Dell Commercial PCs

Dell Technologies User Community

DELL Technologies

Meet our speakers!

Tom Bentz

Product Marketing Endpoint
Security
Client Solutions Group
Dell Technologies

Indranil Chatterjee

Product Manager
Security and Manageability
Dell Technologies

Ryan Johnson

Product Manager
Cloud Client & Software
Solutions
Dell Technologies

THE MODERN WORKPLACE

What’s keeping IT and Security up at night?

Detection of BIOS and firmware-level events

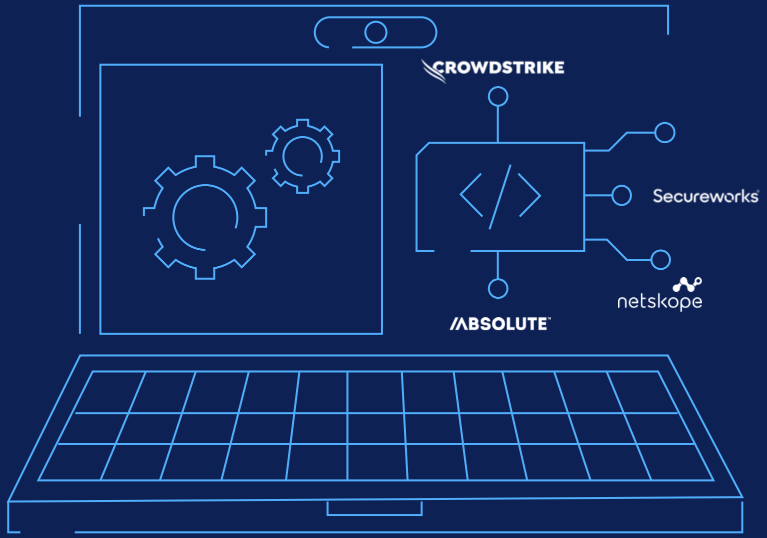
High-risk configurations

Secure Connectivity

Prevent device-level threats and mitigate user error risk with Dell

Secure anywhere-work with Dell Trusted Workspace

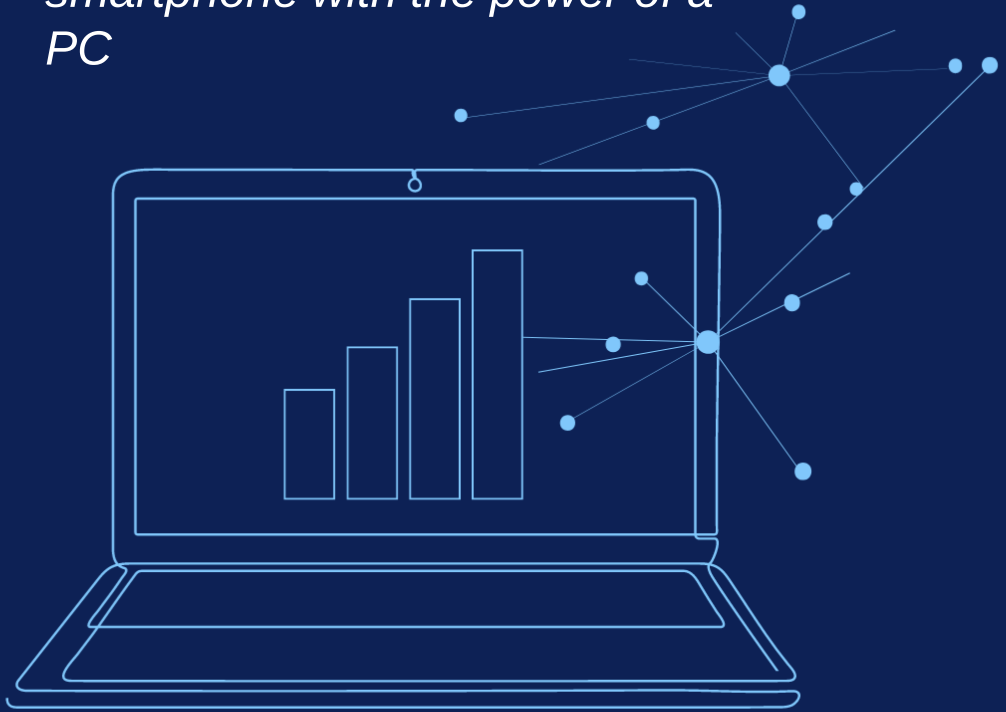
Hardware and software defenses



Solution Spotlight:
Dell-unique CVE Detection*

Dell Connected PCs with secure mobile broadband

The convenient connection of a smartphone with the power of a PC



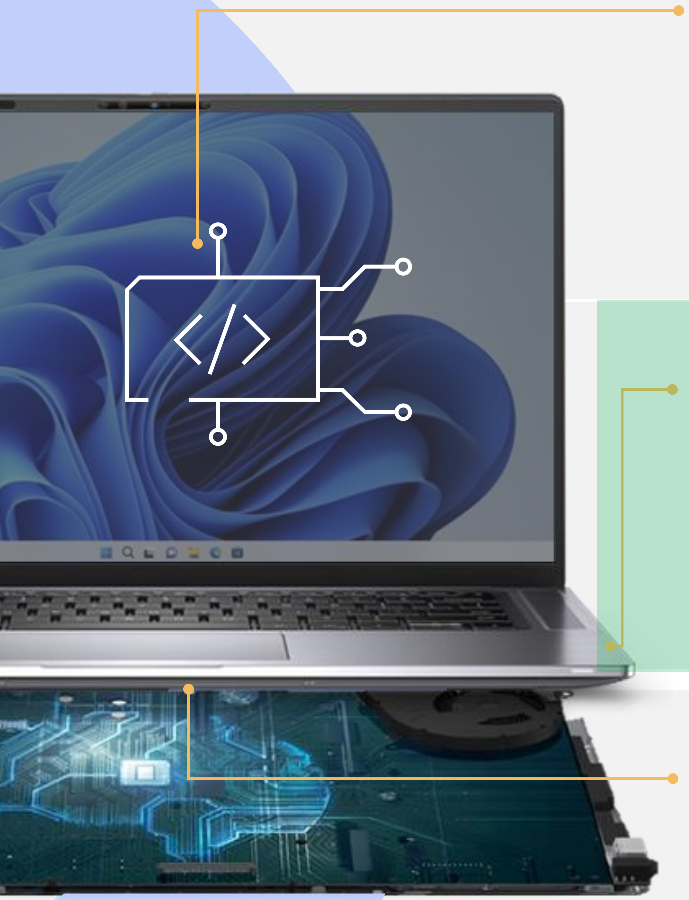
*Based on Dell internal analysis, April 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features.

Dell Trusted Workspace

Tom Bentz
Indranil Chatterjee

DELL Technologies

Dell Trusted Workspace



Built-on Software Security

Strengthen the security of any fleet with advanced protection via an ecosystem of best-of-breed partners curated by Dell.

SafeGuard and Response • SafeData

Built-in Hardware & Firmware Security

Prevent and detect foundational attacks with deep defenses at the BIOS/firmware and hardware levels.

SafeBIOS • SafeID

Built-with Supply Chain Security

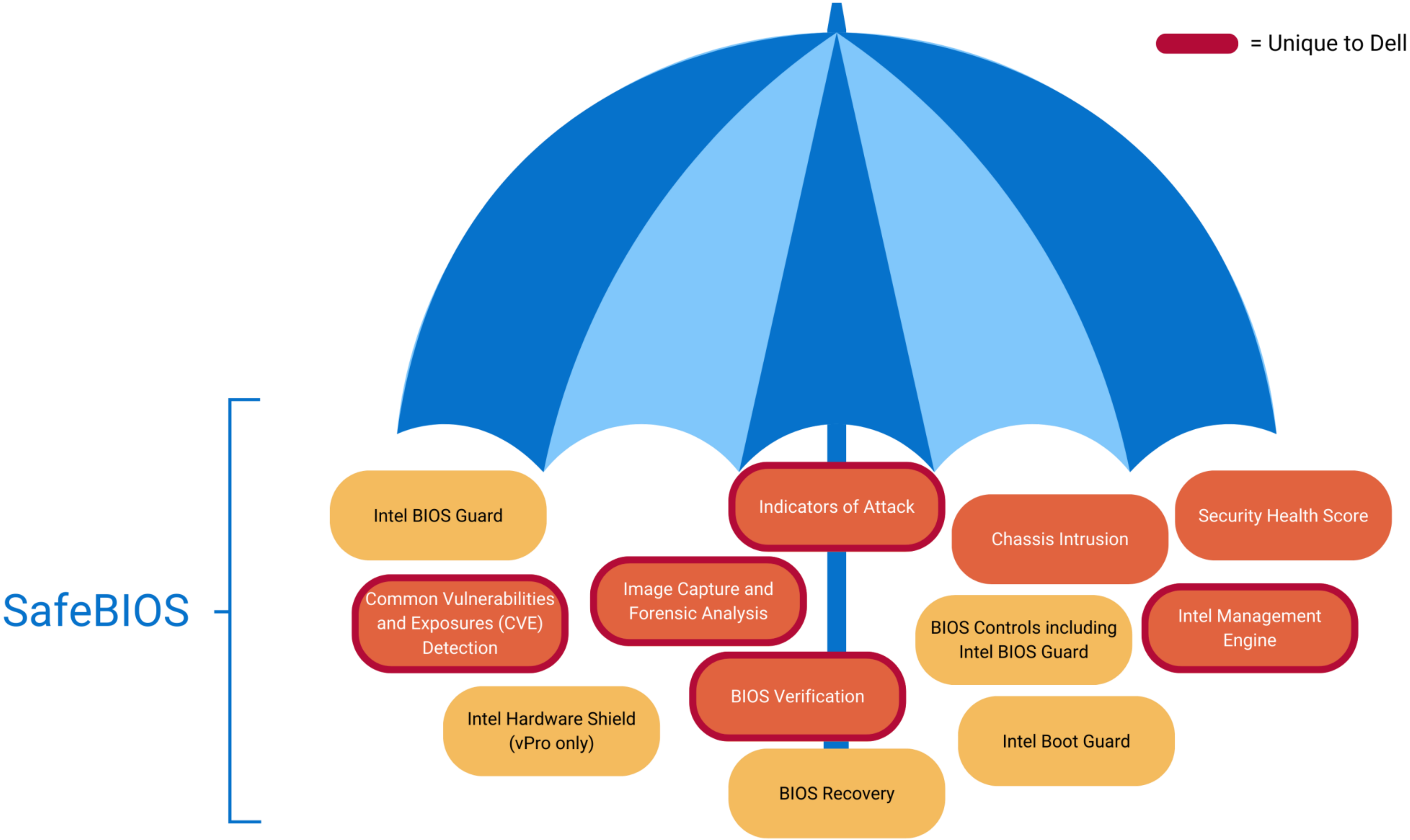
Trust hardware is tamper-free on delivery with optional paid add-ons for extra supply chain assurance.

SafeSupply Chain

Dell Built-in Security

Dell Trusted Device Application

(DTD App)



D&LLTechnologies

Dell Trusted Device App

Secured Component Verification

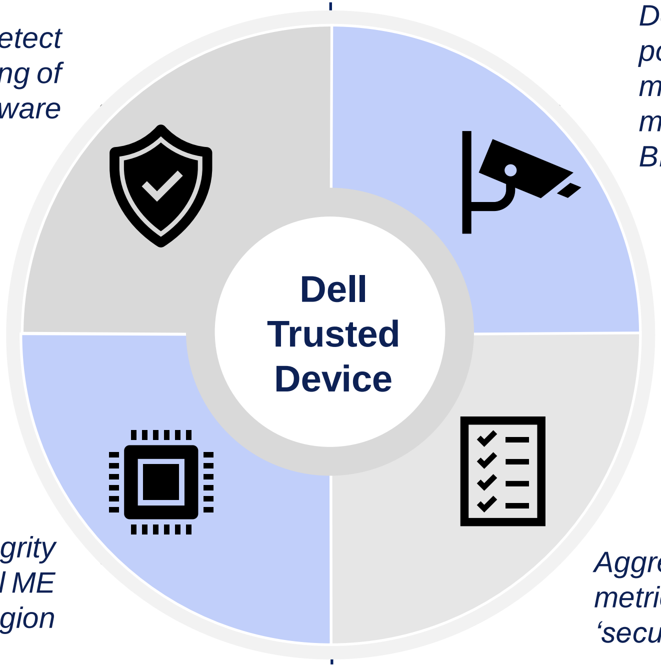
- Supply-chain assurance offering that enables verification of the integrity of the components inside a Dell computer, driven by Trusted Device

BIOS Verification

- Compare cryptographic measurements of BIOS image with off-host golden measurements

Indicators of Attack

- Monitor changes to BIOS attributes and alert when potentially malicious modifications are detected
- Examples include disabling SecureBoot, removing an admin password, etc.



Detect tampering of BIOS firmware

Detect potentially malicious modifications to BIOS attributes

Verify integrity of Intel ME region

Aggregate various metrics into one ‘security score’

Intel ME Verification

- Compare ME firmware found on the platform with previously measured hashes (stored off-host)

Security Score

- Looks for presence of antivirus software and encryption software along with BV, MEV, IoA to calculate a security score
- Compliments other Secure Scores (Microsoft, McAfee, etc.) which grade OS Settings and antivirus configuration

Common Vulnerabilities & Exposure

- Identifies if Dell-supplied software components (BIOS, firmware, drivers, applications, utilities) have a security liability, and provide customers with the necessary actions to remediate them.

Why CVE Detection is important

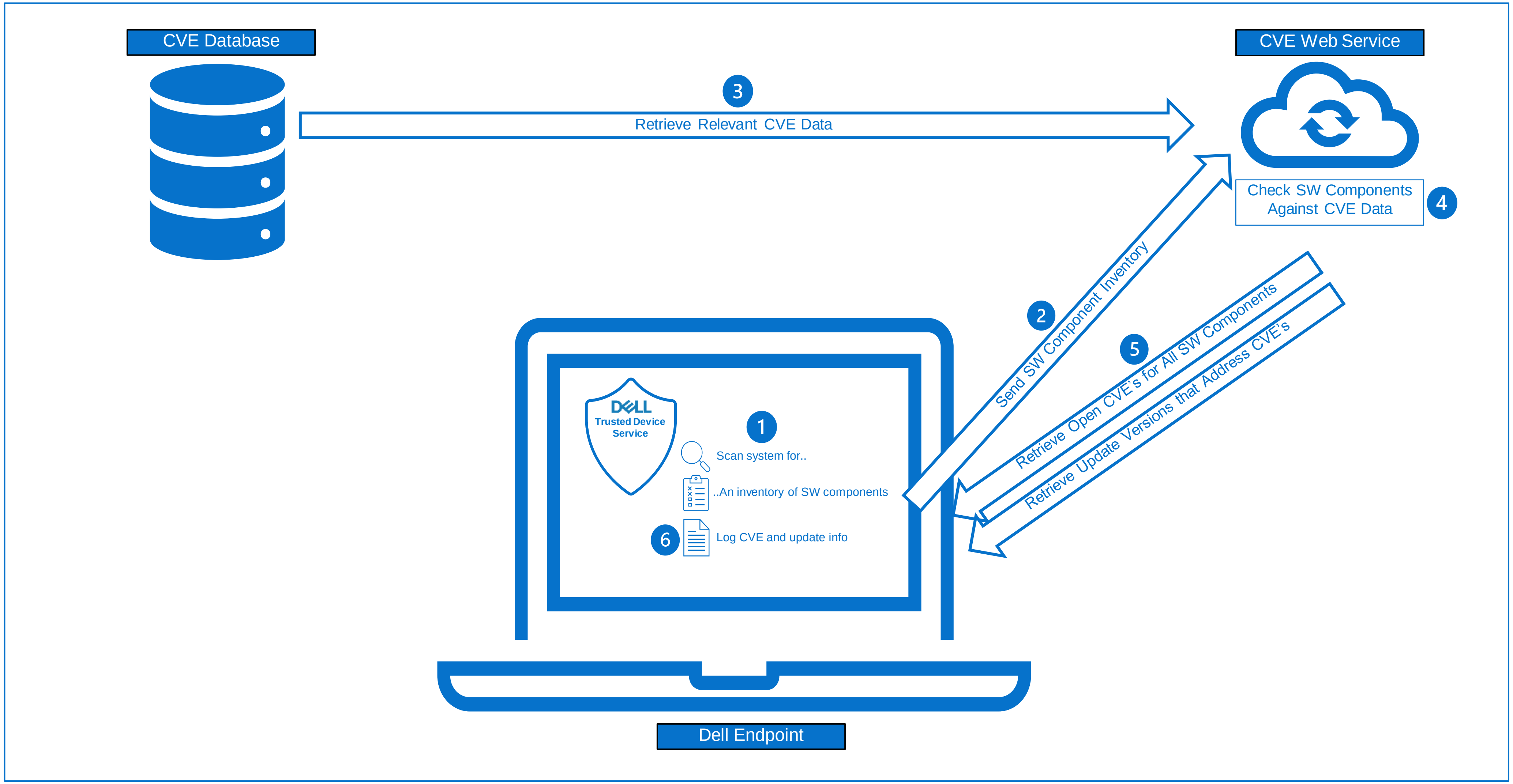
- CVE = Common Vulnerabilities & Exposures
  - A vulnerability is a weakness
  - An exposure is a mistake
- Publicly disclosed computer security flaws, each with a unique ID
- Maintained in the U.S. National Vulnerability Database

CVE Detection for BIOS

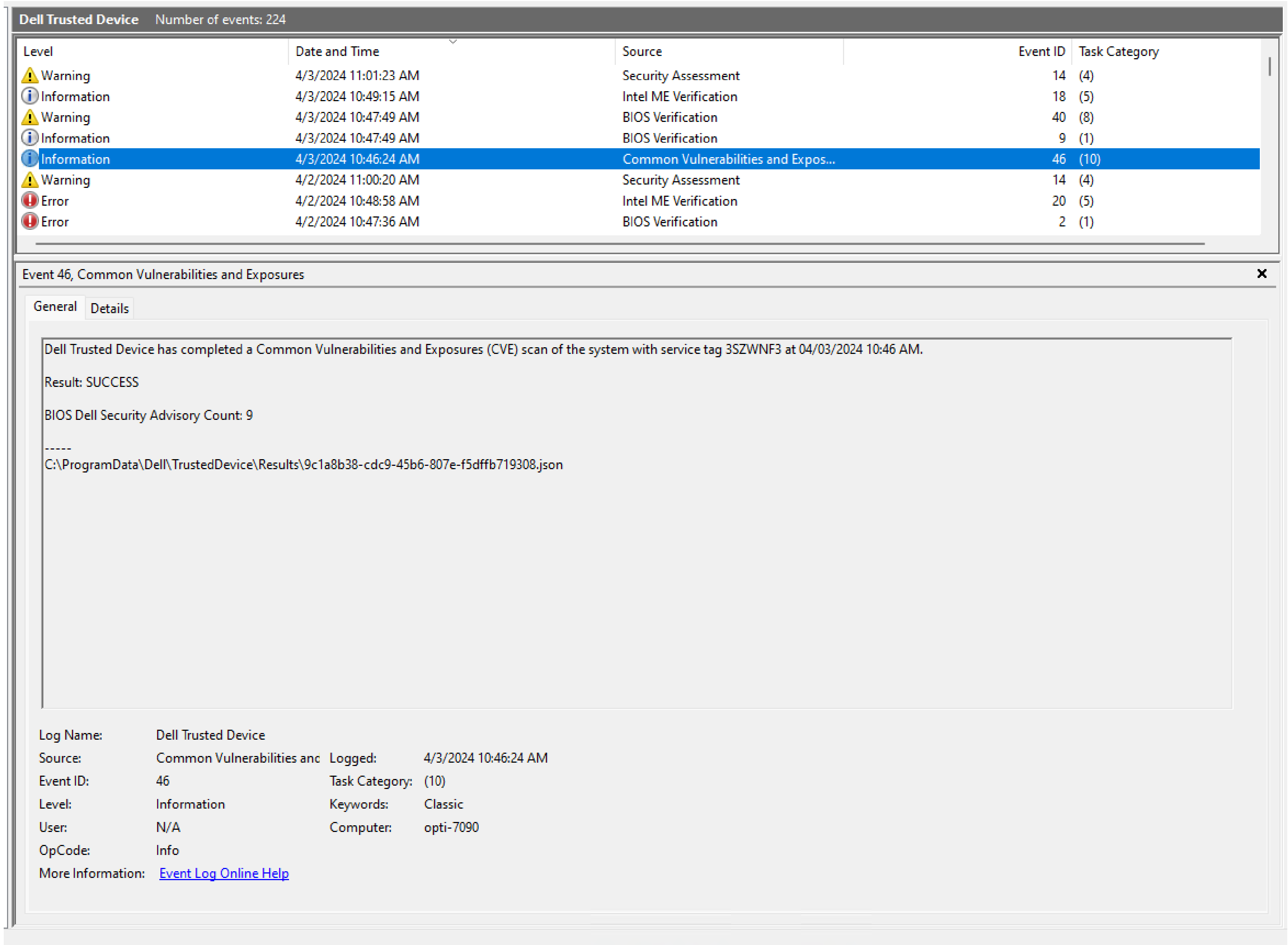
- Unique built-in security check* that scans for and alerts on known BIOS flaws
- Available now - DTD v6.3
- Quick detection of security exposures
- Keeps BIOS in compliance across the fleet

*Based on Dell internal analysis, April 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features.

How CVE Detection Works


CVE Database
CVE Web Service
3
Retrieve Relevant CVE Data
Check SW Components Against CVE Data
4
2
Send SW Component Inventory
5
Retrieve Open CVE's for All SW Components
Retrieve Update Versions that Address CVE's
DELL
Trusted Device Service
1
Scan system for..
..An inventory of SW components
6
Log CVE and update info
Dell Endpoint

Results show in Windows Event Log



Dell Trusted Device Number of events: 224

Level	Date and Time	Source	Event ID	Task Category
⚠ Warning	4/3/2024 11:01:23 AM	Security Assessment	14	(4)
ⓘ Information	4/3/2024 10:49:15 AM	Intel ME Verification	18	(5)
⚠ Warning	4/3/2024 10:47:49 AM	BIOS Verification	40	(8)
ⓘ Information	4/3/2024 10:47:49 AM	BIOS Verification	9	(1)
ⓘ Information	4/3/2024 10:46:24 AM	Common Vulnerabilities and Expos...	46	(10)
⚠ Warning	4/2/2024 11:00:20 AM	Security Assessment	14	(4)
❗ Error	4/2/2024 10:48:58 AM	Intel ME Verification	20	(5)
❗ Error	4/2/2024 10:47:36 AM	BIOS Verification	2	(1)

Event 46, Common Vulnerabilities and Exposures

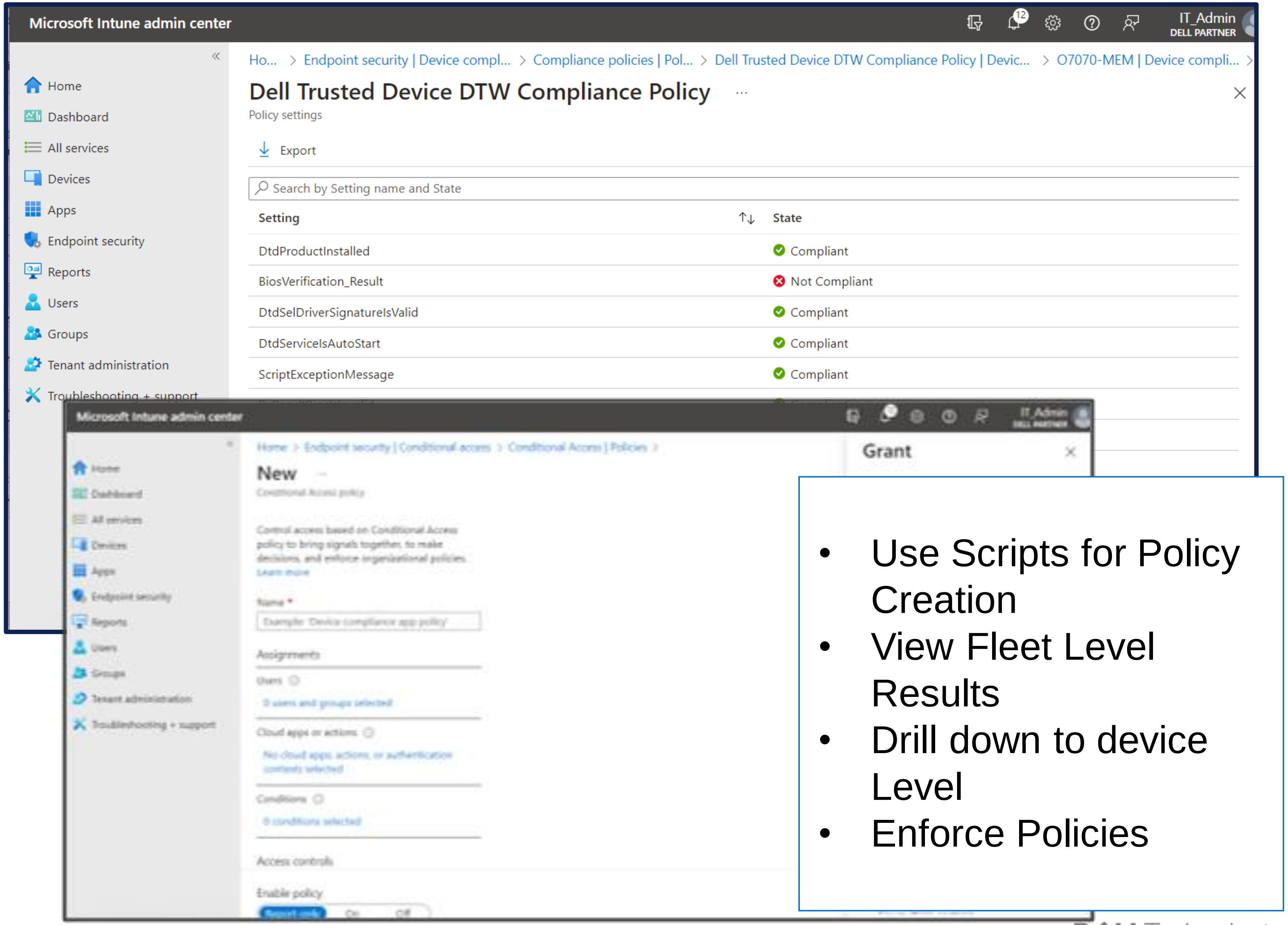
```
Dell Trusted Device has completed a Common Vulnerabilities and Exposures (CVE) scan of the system with service tag 3SZWNF3 at 04/03/2024 10:46 AM.

Result: SUCCESS

BIOS Dell Security Advisory Count: 9

-----
C:\ProgramData\Dell\TrustedDevice\Results\9c1a8b38-cdc9-45b6-807e-f5dffb719308.json
```

Log Name:	Dell Trusted Device		
Source:	Common Vulnerabilities anc	Logged:	4/3/2024 10:46:24 AM
Event ID:	46	Task Category:	(10)
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	opti-7090
OpCode:	Info		
More Information:	Event Log Online Help		

Remediate a flaw with DTD App and Intune

Create and enforce compliance policies

Learn more about our Intune integration in the Dell Demo Center



Ho... > Endpoint security | Device compl... > Compliance policies | Pol... > Dell Trusted Device DTW Compliance Policy | Devic... > O7070-MEM | Device compli... >

Dell Trusted Device DTW Compliance Policy

Policy settings

Export

Search by Setting name and State

Setting	State
DtdProductInstalled	✓ Compliant
BiosVerification_Result	✗ Not Compliant
DtdSelDriverSignatureIsValid	✓ Compliant
DtdServiceIsAutoStart	✓ Compliant
ScriptExceptionMessage	✓ Compliant

Home > Endpoint security | Conditional access > Conditional Access | Policies >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users

0 users and groups selected

Cloud apps or actions

No cloud apps, actions, or authentication contexts selected

Conditions

0 conditions selected

Access controls

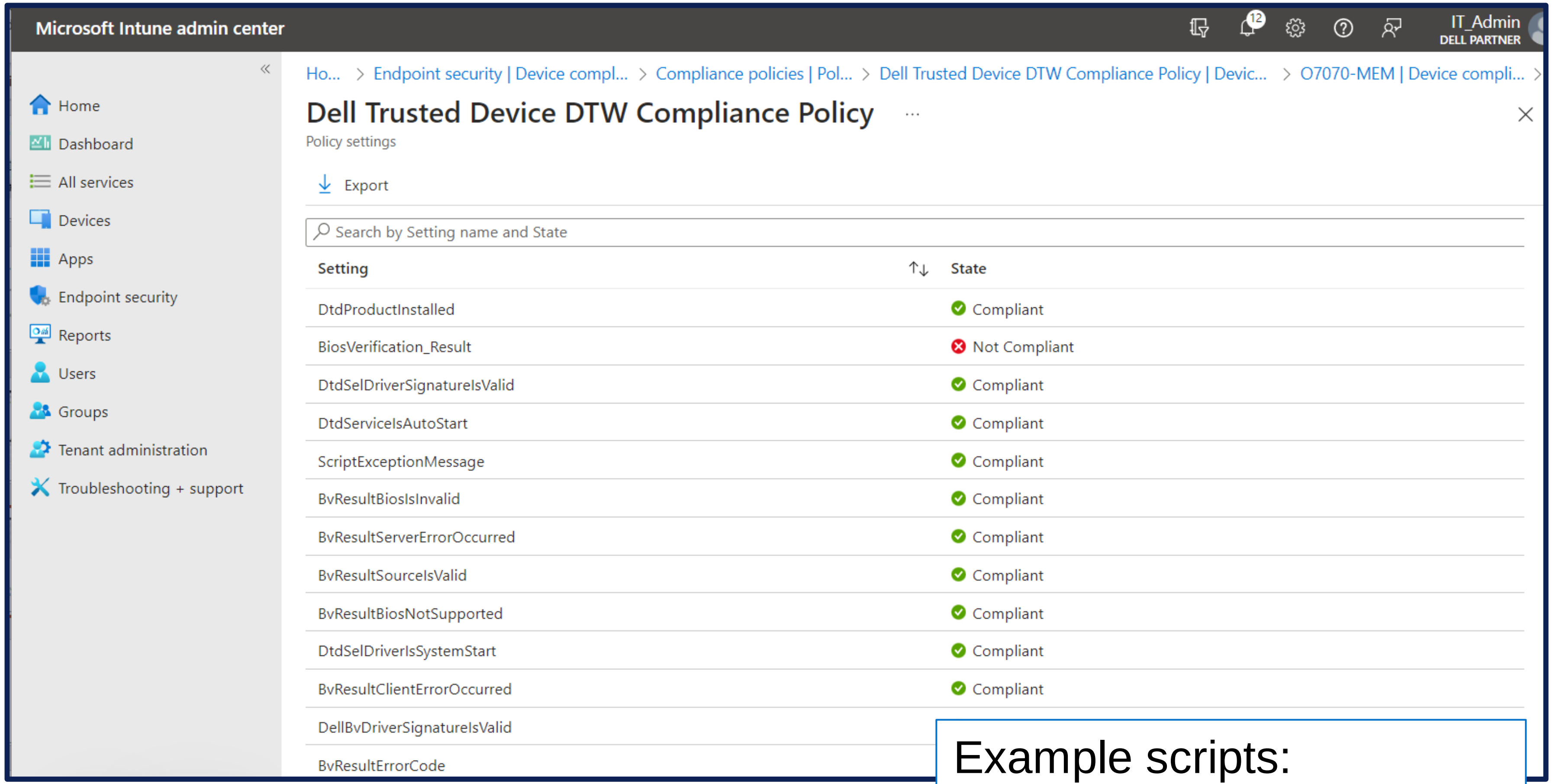
Enable policy

Report-only On Off

Grant

- Use Scripts for Policy Creation
- View Fleet Level Results
- Drill down to device Level
- Enforce Policies

Compliance Policy Creation


Microsoft Intune admin center
IT_Admin
DELL PARTNER
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Ho... > Endpoint security | Device compl... > Compliance policies | Pol... > Dell Trusted Device DTW Compliance Policy | Devic... > O7070-MEM | Device compli... >
Export
Search by Setting name and State

Dell Trusted Device DTW Compliance Policy

Policy settings

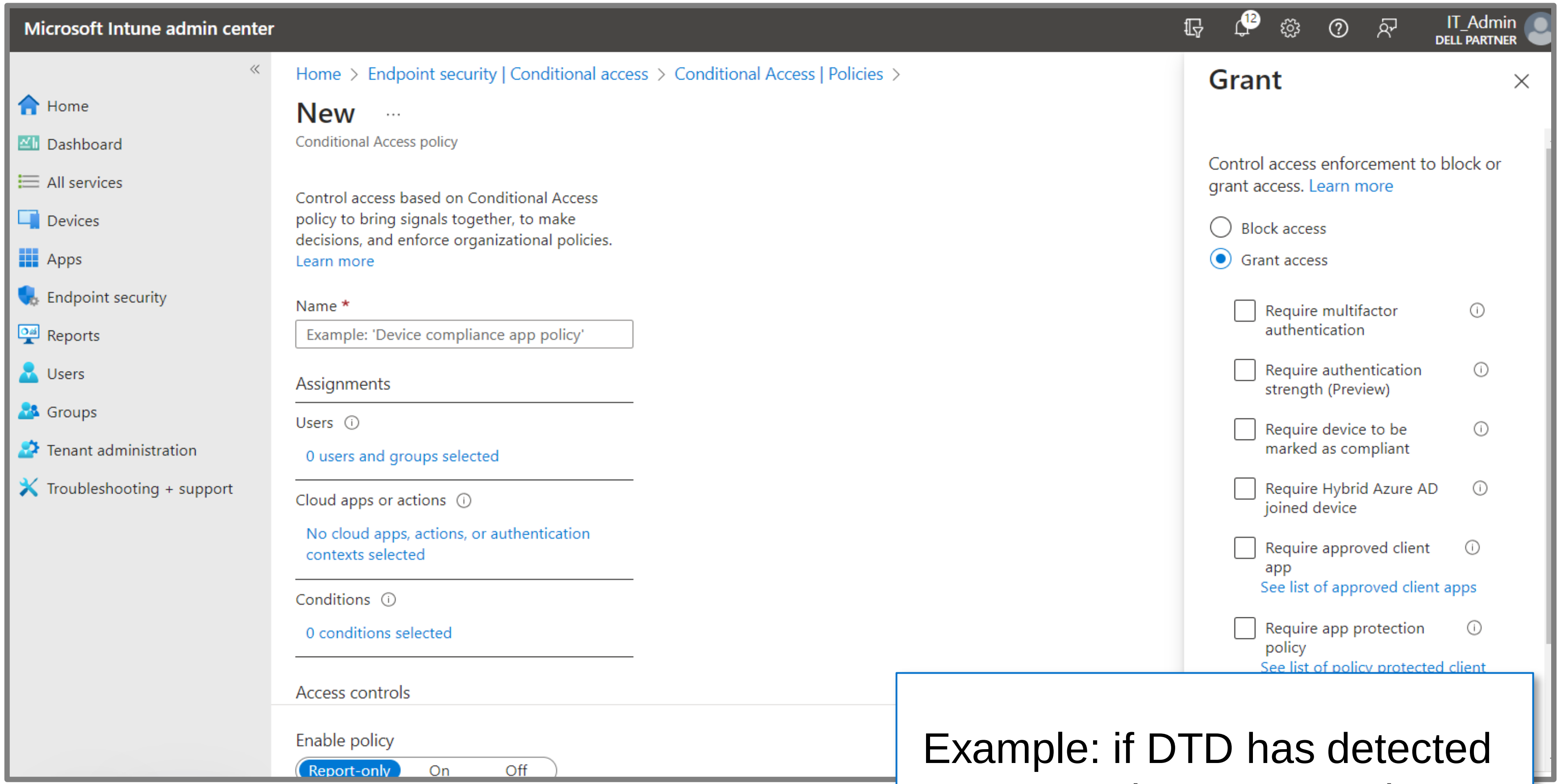
Setting	State
DtdProductInstalled	✓ Compliant
BiosVerification_Result	✗ Not Compliant
DtdSelDriverSignatureIsValid	✓ Compliant
DtdServiceIsAutoStart	✓ Compliant
ScriptExceptionMessage	✓ Compliant
BvResultBiosIsInvalid	✓ Compliant
BvResultServerErrorOccurred	✓ Compliant
BvResultSourceIsValid	✓ Compliant
BvResultBiosNotSupported	✓ Compliant
DtdSelDriverIsSystemStart	✓ Compliant
BvResultClientErrorOccurred	✓ Compliant
DellBvDriverSignatureIsValid	
BvResultErrorCode	

Example scripts:

- Is the device's verification in compliance?
- Has the product been successfully installed?
- Is the driver signature valid?

Learn more about our Intune integration in the Dell Demo Center

Compliance Policy Enforcement



Microsoft Intune admin center

IT_Admin
DELL PARTNER

Home > Endpoint security | Conditional access > Conditional Access | Policies >

New ...
Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *
Example: 'Device compliance app policy'

Assignments

Users ⓘ
0 users and groups selected

Cloud apps or actions ⓘ
No cloud apps, actions, or authentication contexts selected

Conditions ⓘ
0 conditions selected

Access controls

Enable policy
Report-only | On | Off

Grant

Control access enforcement to block or grant access. Learn more

○ Block access
● Grant access

□ Require multifactor authentication ⓘ
□ Require authentication strength (Preview) ⓘ
□ Require device to be marked as compliant ⓘ
□ Require Hybrid Azure AD joined device ⓘ
□ Require approved client app ⓘ
See list of approved client apps
□ Require app protection policy ⓘ
See list of policy protected client

Example: if DTD has detected a tampered BIOS on a given endpoint, admin can restrict that endpoint's ability to access privileged assets.

Learn more about our Intune integration in the Dell Demo Center

Explore Dell Trusted Devices

Latitude

OptiPlex

Precision

How to benefit from Dell-unique CVE Detection* today

- Included on all Dell commercial PCs – no extra cost
- Install the DTD App to maximize CVE Detection and other SafeBIOS protections

*Based on Dell internal analysis, April 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features.

Connected PCs

Ryan Johnson

Mobile Broadband is essential in today’s world

Connected PCs are laptops with mobile broadband that work like smartphones to enable access to the internet when a secure Wi-Fi connection is not available

Connected PCs offer:

Better user experience

Improved productivity

Enhanced security

DELL Technologies

Benefits of Mobile Broadband on Dell Connected PCs

SIMPLE

Better user experience

More flexible work schedules

Instant connectivity

SEAMLESS

Improved productivity

Faster internet & reliable bandwidth

Better support for mobile or hybrid workers

SECURE

Enhanced security

Mobile broadband is more secure

No need for unsecure public Wi-Fi

Users have a few traditional options to stay connected

Public Wi-Fi

- Hassle to find Wi-Fi name & password
- Unreliable speed and bandwidth
- Security risk

Tethering or Personal Hotspot

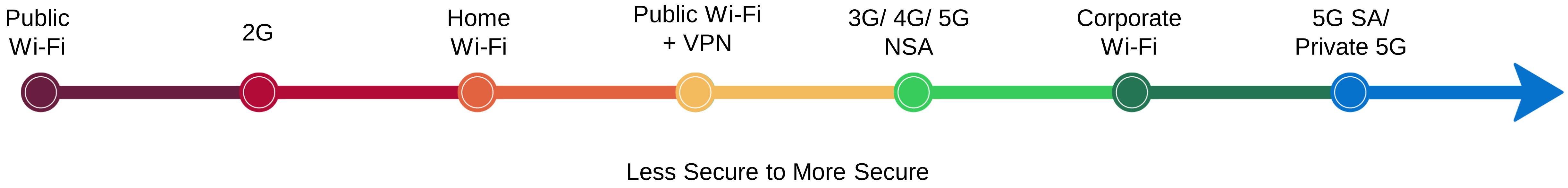
- Personal data usage/limits
- Availability & user error
- Phone battery drainage

Portable Hotspot “Puck”

- Additional external device

Phone

- Small screen limitations
- Lose PC productivity



Security benefits of Connected PCs

“5G provides a **more reliable connection** over a greater distance and **demonstrates more resilience** against physical obstacles and radio interference than Wi-Fi.”

“5G networks demonstrated security benefits over … technologies like **Wi-Fi tethering** since they allow the wireless device to eliminate any reliance on the Wi-Fi protocol, and thus **reduce the wireless attack surface significantly**.”

“**A standalone 5G network is more resilient against many security risks and attacks than a typical Wi-Fi network**. Most … attacks that were found to still be possible against a 5G network had higher costs and required additional effort and skill.”

Explore Dell Connected PCs

- The industry's most secure commercial PCs*
- Carrier promotions available

Latitude

9000 Series – **9450 2-in-1**, 9440 2-in-1

7000 Series – **7350**, **7450**, **7650**, 7340, 7440, 7640

5000 Series – **5350**, **5450**, **5550**, 5340, 5430, 5440

3000 Series – **3550**, 3440, 3540, 3140

Rugged

7000 Series – **7030**, **7230**, **7330**

5000 Series – **5430**

Precision

7000 Series – **7680**, **7780**

3000 Series – **3490**, **3590**, **3591**, 3480, 3580, 3581

Chromebook

3000 Series - 3110

5000 Series - 5430

Learn More

Blog: Get to CVEs Before They Compromise Your PC

What is the Dell Trusted Device App?

Overview

Key Benefits

View DTD Insights within Top IT Environments

Solution Brief: DTD Application

Client Solutions Dell Trusted Device: BIOS Security

A deep dive into the foundational, BIOS-level security of Dell Trusted Devices, the industry's most secure commercial PCs*

White Paper: Dell Trusted Device

The Always-Connected PC in the New World of Work

White Paper: The Always Connected PC in the New World of Work

Dell Connected PCs: Empowering and Learning

Disasters and Disruptions

Blog: Connected PCs Empowering Future Work and Learning

Questions?

DELL Technologies