

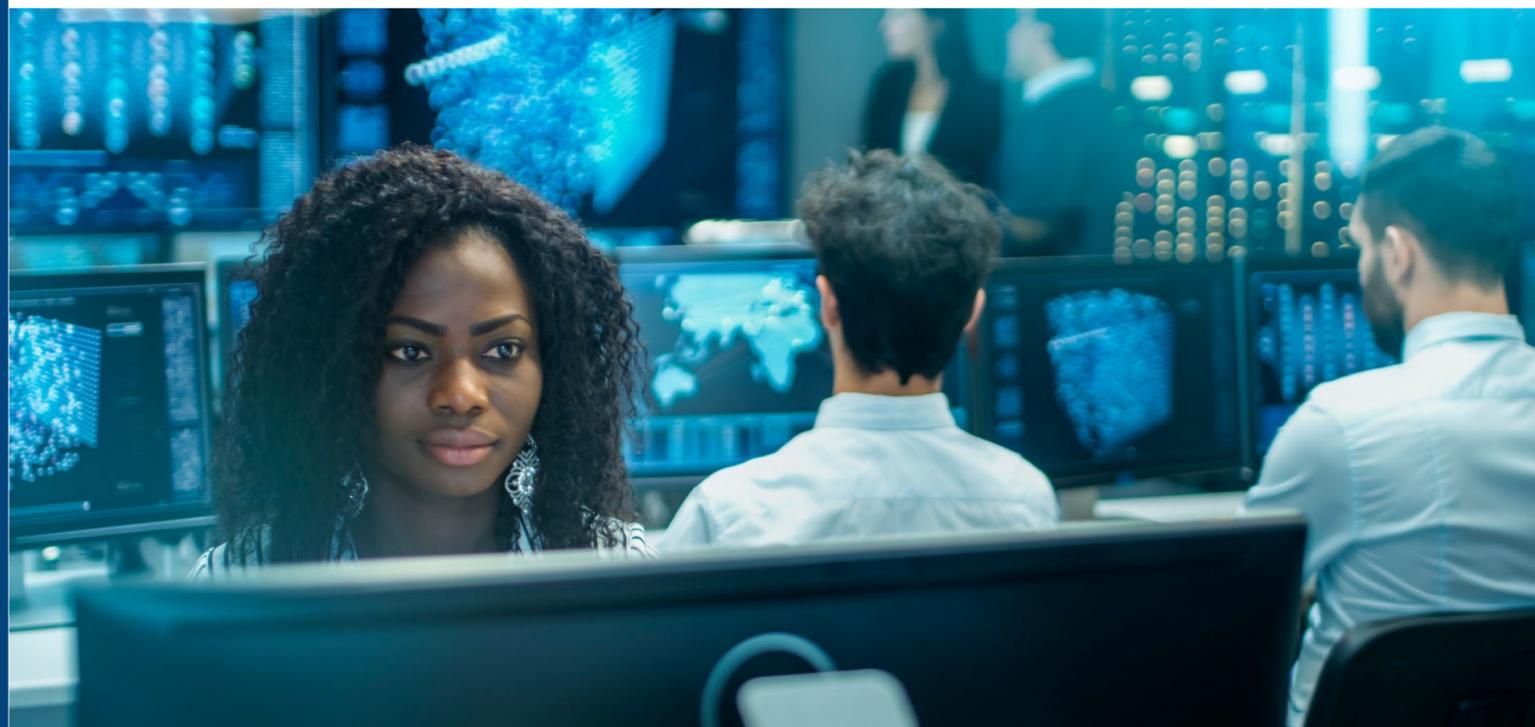
## How to combat modern cyber threats

with integrated endpoint security & manageability



## Executive summary

Emerging attack vectors are creating new risk. Stay ahead of modern endpoint threats with multiple layers of defense that work together. Learn how hardware telemetry can integrate with software to improve fleet-wide security and manageability. Disrupt attacks faster, support zero trust principles and innovate securely with simple-to-manage devices and solutions.



## Table of Contents

[The threat landscape](#)

[Challenges](#)

[Solution](#)

[Use cases & countermeasures](#)

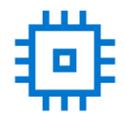
[Takeaways and call to action](#)

# The threat landscape

## Case study

In 2023, [Eclypsium](#) discovered a flaw in the firmware of motherboards sold by a Taiwanese manufacturer. Intended simply to keep the firmware updated, researchers found that the code was implemented insecurely, potentially allowing the mechanism to be hijacked and used to install malware.

### A few reasons why this discovery was particularly alarming



Customers were exposed via a firmware vulnerability.



The vulnerability existed in an area of the device where, traditionally, it has been hard to detect threats.



It could be used to launch a remote attack that bypassed credential checks.

## Ripped from the headlines...



### Millions of PC Motherboards Were Sold With a Firmware Backdoor

Hidden code in hundreds of models of motherboards invisibly and insecurely downloads programs – a feature ripe for abuse, researchers say.



# The threat landscape

## Implications

That's a key driver that keeps IT and Security teams up at night:

### Device-based attacks.

These sophisticated, malicious attacks can allow adversaries to gain privileged access. What's more, many of these can turn off traditional software-only protections, e.g., antivirus, completely undetected.



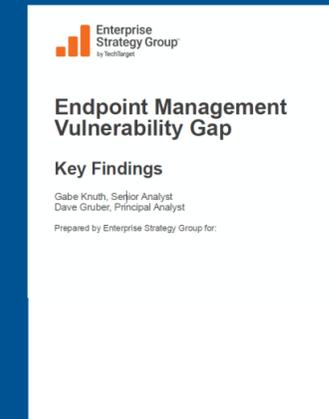
According to a global survey of IT and security professionals<sup>1</sup>, as organizations source new hardware, among their top evaluation criteria:

## Automating detection of BIOS firmware events



Sixty-nine percent of organizations reported at least ONE device-level attack in the last twelve months. That's up 1.5 times from the 2020 study!<sup>2</sup>

## High-risk configurations



More than 75% of organizations report that they have experienced at least one cyberattack caused by an unknown, unmanaged, or poorly managed endpoint device.<sup>3</sup>

# Challenges

So, what makes a device an easy target?



**Visibility**



**Actionability**

These attacks are hard to see – executed at a part of the device that's traditionally lacked visibility and observability.

Often organizations have dozens of tools in place that operate in silos – so if an attack is detected, swift response and remediation is a major challenge and a lot of manual work.



# Solution



Visibility



Actionability

As one of the world's largest technology providers, Dell thinks about security a lot. That's why **we build our commercial AI PCs to prioritize visibility and actionability right out of the gate.** This puts power in the hands of IT and security operations.

Our commercial AI PCs come with **unique built-in security features** like BIOS Verification<sup>4</sup> and Indicators of Attack<sup>4</sup> to help detect threats before they do damage. We make these detections visible with **Dell-only device telemetry**<sup>4</sup>. When a Dell commercial AI PC on Intel vPro<sup>®</sup> detects a potential threat at the device level, it can send that to the operating system for faster, more effective investigation and response

## Industry Leadership

### Dell offers the World's Most Secure Commercial AI PCs<sup>4</sup>

Learn what it takes to maintain device trust against modern threats.



[Read the Principled Technologies Study on Device Security →](#)



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

#### Approach

Dell<sup>™</sup> 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<sup>®</sup> 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<sup>®</sup> 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<sup>®</sup>. 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.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

# Solution

## Combat threats with security & manageability working together

Dell and our connected partner ecosystem are working to bring visibility and actionability to the workspace. This includes:

- Supply chain security and built-in hardware and firmware defenses from Dell
- Core silicon and 'below-the-OS' protections from Intel
- Manageability via Dell and unified endpoint management consoles
- Advanced threat protection covering endpoints, networks and the cloud from partners including CrowdStrike and Absolute

The ecosystem uses PC telemetry as the connector, helping close the gap between IT and security solutions where threats can slip through. Not only can this approach help prevent attacks, but it can also detect, respond to, recover from, and remediate them.

### Software Solutions

CrowdStrike Falcon  
Endpoint Security



THE OS

### Hardware & Firmware Security

PC security leveraging Intel and Absolute

Dell Trusted Device Application (PC 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)

### Core Silicon

intel vPRO



### Secure PC Foundation

Secure development lifecycle (SDL)  
Secure supply chain

# Use cases & countermeasures

To demonstrate how integrated security and manageability works to improve cyber resilience, we will look at two use cases including attack scenarios and countermeasures.

First, an attack on the BIOS firmware. Here, we see how the [cyber kill chain](#)<sup>5</sup> of a BIOS downgrade attack can play out.

## BIOS downgrade attack

### Initial Access: Replication Through Removable Media + Phishing

#### Step 1a

Malicious insider exploits an existing BIOS vulnerability to steal OS credentials remotely. Hacks device and downgrades BIOS.



#### Step 1b

Attacker initiates a spear-phishing attack, stealing a session token when an admin mistakenly authenticates on a malicious site.



#### Step 2

### Credential Access

Attacker achieves persistence by creating additional admin accounts and proceeds to move about the network.



#### Step 3

### Lateral Movement

Attacker maps the network and locates system management servers.



#### Step 4

### Exfiltration

Attacker exfiltrates data over a web service.



# Use cases & countermeasures

## BIOS downgrade countermeasures

Adversaries are breaking into the network faster than ever before. In fact, according to [CrowdStrike's Global Threat Report](#), in 2024, the average eCrime breakout time (the time it takes to break into a system and move laterally) dropped to 48 minutes, with the fastest recorded at 51 seconds!<sup>6</sup>

Here's how Dell and our partners Intel<sup>®</sup> and CrowdStrike help to catch and repel a BIOS downgrade attack along the kill chain with [hardware-assisted security](#).



**Secure supply chain:** Rigorous controls safeguard PCs from design and development, through sourcing and assembly, on through delivery. Dell and Intel work tirelessly to ensure products are developed to mitigate the risk of product vulnerabilities and product tampering throughout their lifecycle.



# Use cases & countermeasures

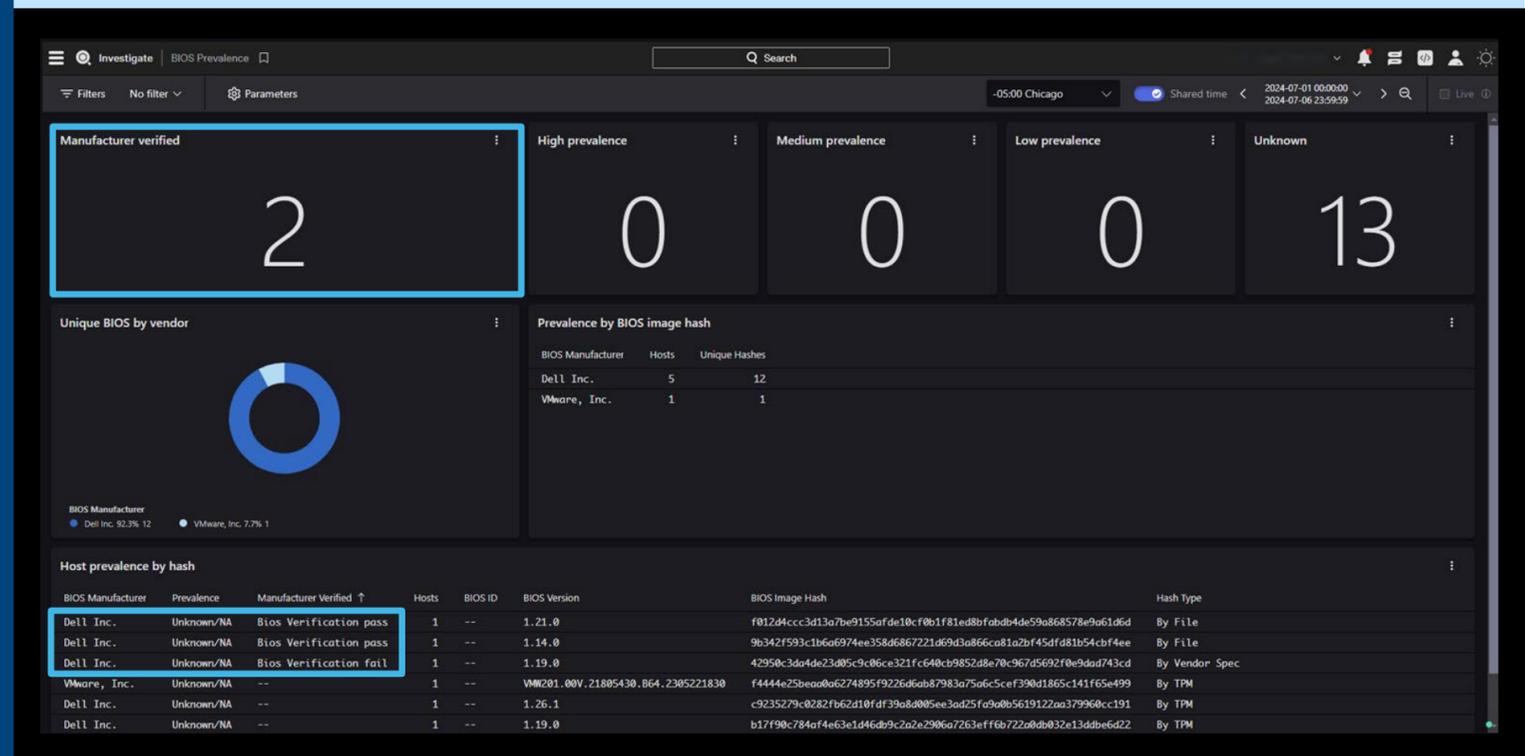
## BIOS downgrade countermeasures

Adversaries are breaking into the network faster than ever before. In fact, according to [CrowdStrike's Global Threat Report](#), in 2024, the average eCrime breakout time (the time it takes to break into a system and move laterally) dropped to 48 minutes, with the fastest recorded at 51 seconds!<sup>6</sup>

Here's how Dell and our partners Intel<sup>®</sup> and CrowdStrike help to catch and repel a BIOS downgrade attack along the kill chain with [hardware-assisted security](#).



**Detect BIOS attestation in the CrowdStrike Falcon platform:** With the Dell device telemetry enabled, an admin can view notifications from built-in security features like BIOS Verification remotely in CrowdStrike Falcon, helping speed detection of suspicious activity before any lasting damage occurs.



# Use cases & countermeasures

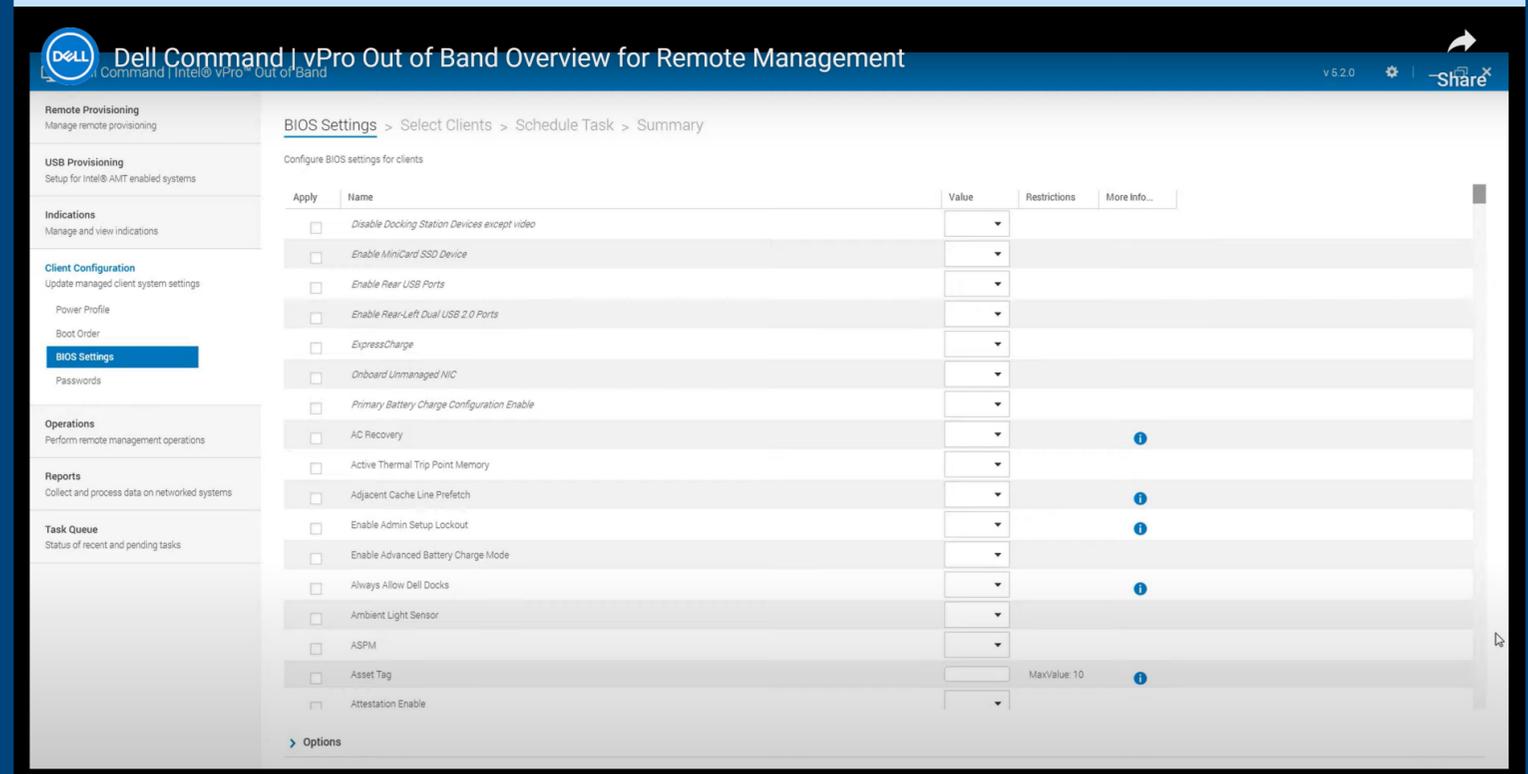
## BIOS downgrade countermeasures

Adversaries are breaking into the network faster than ever before. In fact, according to [CrowdStrike's Global Threat Report](#), in 2024, the average eCrime breakout time (the time it takes to break into a system and move laterally) dropped to 48 minutes, with the fastest recorded at 51 seconds!<sup>6</sup>

Here's how Dell and our partners Intel<sup>®</sup> and CrowdStrike help to catch and repel a BIOS downgrade attack along the kill chain with [hardware-assisted security](#).



**Remediate BIOS downgrade:** Help prevent future threats for out-of-band systems. Dell Client Command Suite with Intel vPro enables remote remediation.



# Use cases & countermeasures

In this second use case, here's how the step in the kill chain of a software supply chain attack could play out.

## Software supply chain attack

### Step 1

#### Initial Access: Supply Chain Compromise

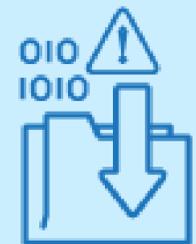
Attacker injects malicious code into a software utility (BIOS/firmware).



### Step 2

#### Persistence

Customers download the malicious code when they go to update their devices. Attacker installs malware.



### Step 3

#### Lateral Movement

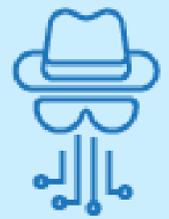
Attacker spoofs a user they just attacked and sends a malicious link to another user. That user clicks the link and attacker steals their credentials.



### Step 4

#### Exfiltration

Attacker exfiltrates data.



# Use cases & countermeasures

The supply chain has become a key target for attackers. While these attacks are less common, the results of a successful one can be devastating because organizations are still learning how to shore up their defenses against them.

A core responsibility of all technology providers is to ensure what they sell doesn't unintentionally present risk to users through vulnerabilities.

To help prevent attacks and provide resiliency to the security stack, Dell and Intel® abide by the strict process and protocols of our [Secure Development Cycle](#)<sup>7</sup>.

Additional supply chain assurance, e.g., [Dell Secured Component Verification](#)<sup>8</sup>, plus firmware-level security from Absolute (depicted on the right) gives customers confidence throughout the lifetime of the PC.



**Endpoint visibility from the factory:** See all devices on and off the network with Absolute embedded in Dell-managed factories. Absolute Custom Factory Install (CFI) removes a step in deployment and protects devices that may be shipping to warehouses and multiple end-user locations. Mitigate risk with a full view of the fleet from a cloud-based dashboard.



Easily find and maintain complete inventory of your IT assets and applications



Locate and map your entire fleet



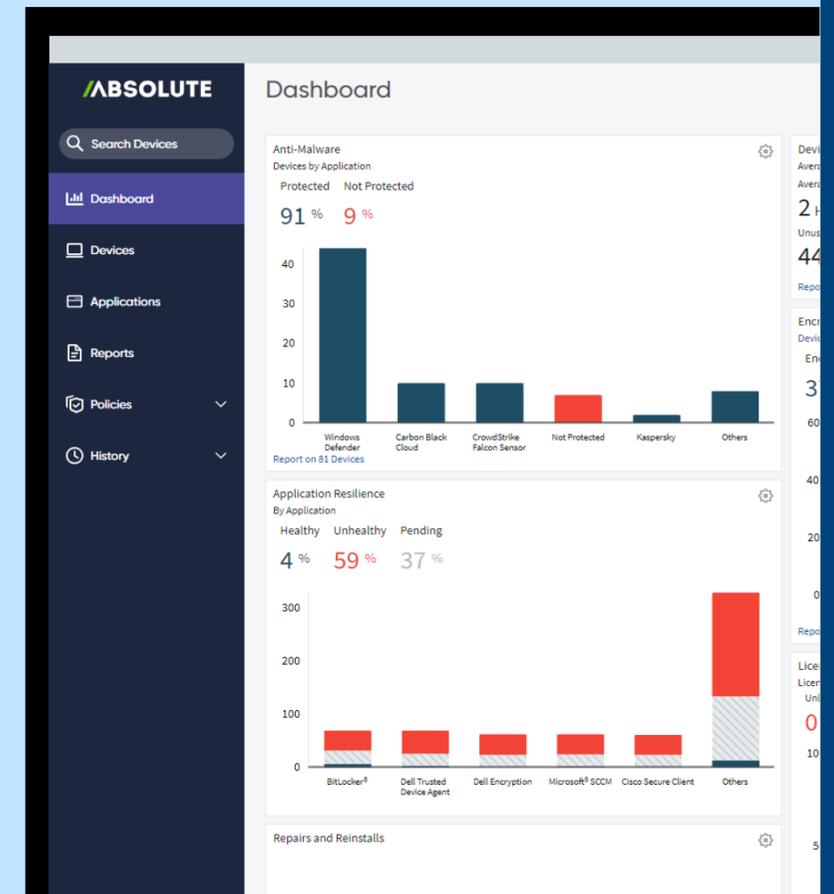
Optimize Asset Usage and monitor security posture



Cross-platform support (Windows, Mac & Chrome)



Embedded in the BIOS of 27 Leading PC OEMs



# Use cases & countermeasures

The supply chain has become a key target for attackers. While these attacks are less common, the results of a successful one can be devastating because organizations are still learning how to shore up their defenses against them.

A core responsibility of all technology providers is to ensure what they sell doesn't unintentionally present risk to users through vulnerabilities.

To help prevent attacks and provide resiliency to the security stack, Dell and Intel® abide by the strict process and protocols of our [Secure Development Cycle](#)<sup>7</sup>.

Additional supply chain assurance, e.g., [Dell Secured Component Verification](#)<sup>8</sup>, plus firmware-level security from Absolute (depicted on the right) gives customers confidence throughout the lifetime of the PC.



Prevent



Detect & respond



Recover & remediate

**Control endpoints:** With Absolute, detect when endpoints are compromised (e.g., a critical app is corrupted by malware or a PC goes missing in transit). Take remote action to remediate threats immediately by rendering devices useless and/or deleting the data they contain.



Protect devices when they move beyond defined fences



Remotely protect and sanitize critical data



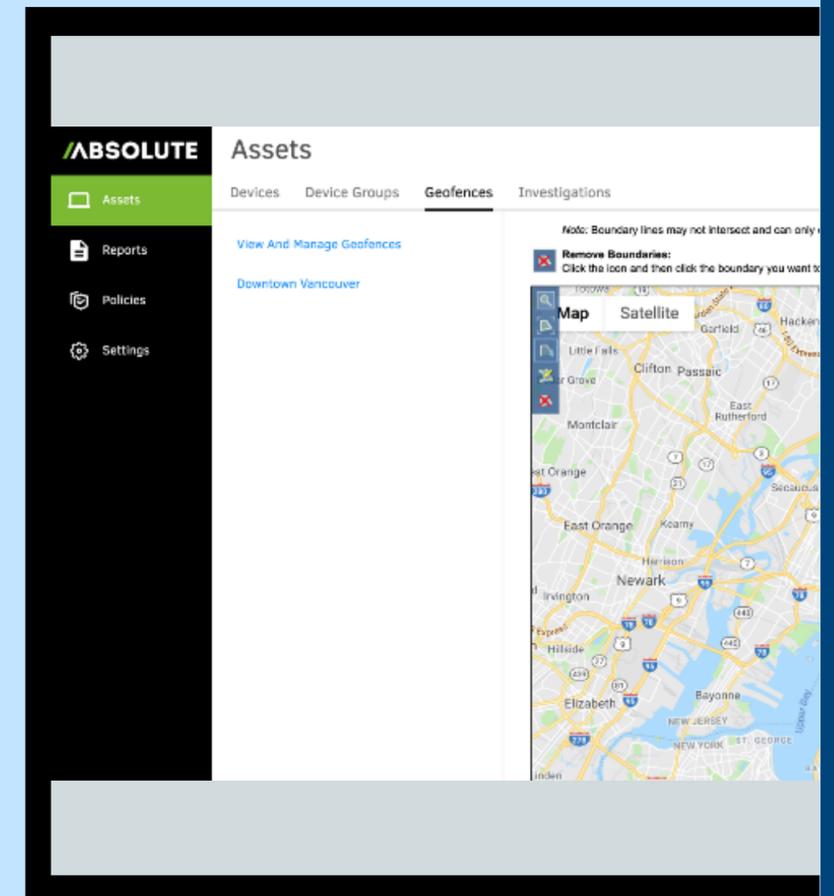
Perform end-of-life data wipe with compliance certificates



Lock devices to protect critical assets on demand



Enable remote firmware protection



# Use cases & countermeasures

The supply chain has become a key target for attackers. While these attacks are less common, the results of a successful one can be devastating because organizations are still learning how to shore up their defenses against them.

A core responsibility of all technology providers is to ensure what they sell doesn't unintentionally present risk to users through vulnerabilities.

To help prevent attacks and provide resiliency to the security stack, Dell and Intel® abide by the strict process and protocols of our [Secure Development Cycle](#)<sup>7</sup>.

Additional supply chain assurance, e.g., [Dell Secured Component Verification](#)<sup>8</sup>, plus firmware-level security from Absolute (depicted on the right) gives customers confidence throughout the lifetime of the PC.



**Self-healing:** With Absolute Persistence embedded in the Dell BIOS firmware, get back to original state when tampering is detected. Absolute can self-heal, or persist, any compromised endpoint or supported application in the Application Resilience catalog (80+ Applications), including a library of other countermeasures in place, e.g., Dell Trusted Device Application, Zscaler.



Find and easily delete sensitive data on endpoints



Take remedial action across devices via a library of customized scripts



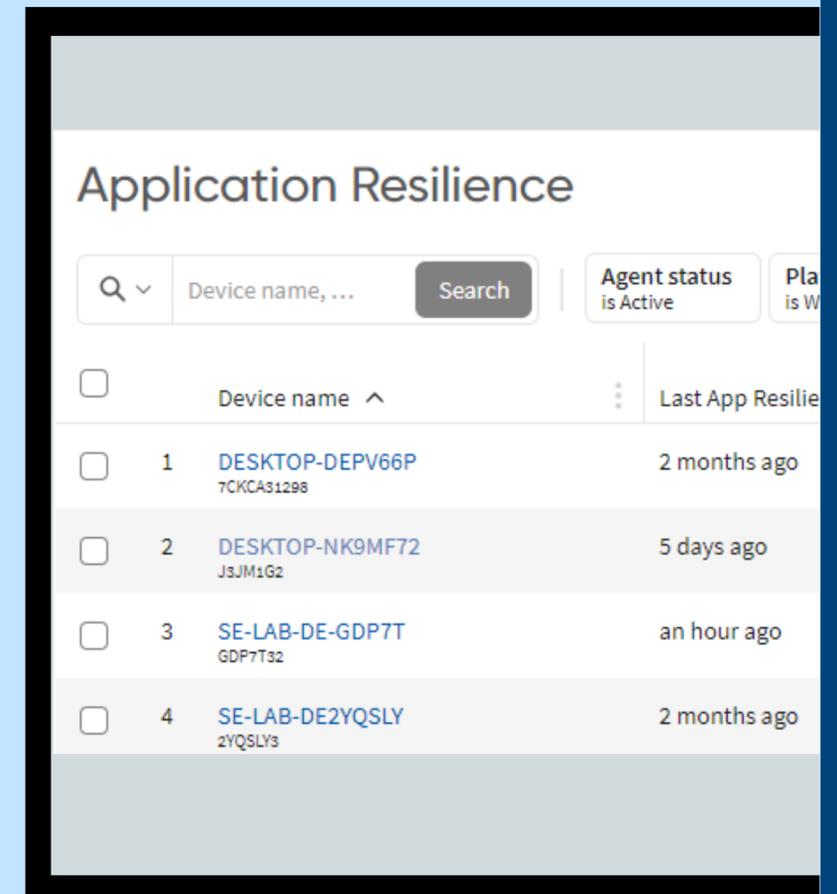
Monitor and Self-Heal Applications



Large and growing Application Resilience catalog of 3<sup>rd</sup> party endpoint controls



Investigate and locate lost or stolen devices with Absolute Investigations Team



# Key takeaways

A fleet is only as secure as its individual PCs.

To combat modern threats, devices must be built securely and have security built in.

Catch, repel and recover from attacks by ensuring endpoint security and manageability work together.

Security is a team sport. Leverage both hardware and software for the best defense.



## To learn more:

**Contact us:** [Global.Security.Sales@Dell.com](mailto:Global.Security.Sales@Dell.com)

**Visit us:** [Dell.com/Endpoint-Security](https://Dell.com/Endpoint-Security)

**Follow us:** LinkedIn [@DellTechnologies](https://www.linkedin.com/company/delltechnologies) | X [@DellTech](https://twitter.com/DellTech)

# Take the next step

Security is a daunting topic for organizations of all sizes. **Engage an experienced security and technology partner to modernize endpoint security.**

Dell Trusted Workspace helps secure endpoints for a modern, zero trust-ready IT environment. Reduce the attack surface with a comprehensive portfolio of hardware and software protections exclusive to Dell. Our highly coordinated, defense-based approach offsets threats by combining built-in protections with ongoing vigilance. End users stay productive, and IT stays confident with security solutions built for today's cloud-based world.



1. Source: Enterprise Strategy Group, a division of TechTarget, Custom Research Survey Commissioned by Dell Technologies, [Assessing Organizations' Security Journeys](#), November 2023.
2. Source: [Futurum Group, Endpoint Security Trends, 2023](#).
3. Source: Enterprise Strategy Group, a division of TechTarget, Research Report, [Managing the Endpoint Vulnerability Gap: The Convergence of IT and Security to Reduce Exposure](#), May 2023.
4. 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.
5. Source: [What is the Cyber Kill Chain? Introduction Guide – CrowdStrike](#).
6. Source: [CrowdStrike 2025 Global Threat Report](#).
7. Source: [Three Considerations for Establishing Device Trust | Dell USA](#).
8. Source: [How to Keep Device Trust Close to the Vest | Dell USA](#).

Copyright © 2025 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

