DELL Technologies

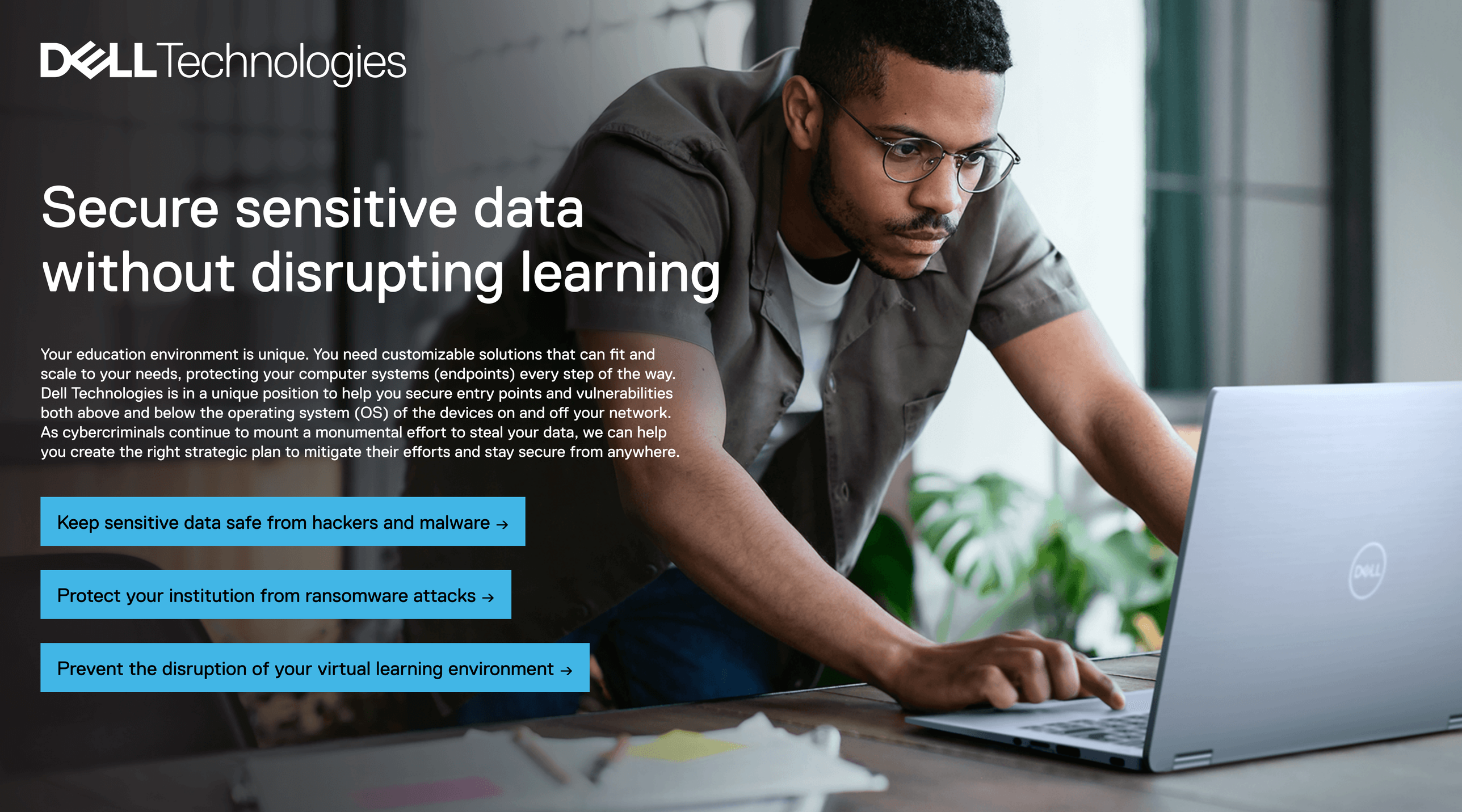
Secure sensitive data without disrupting learning

Your education environment is unique. You need customizable solutions that can fit and scale to your needs, protecting your computer systems (endpoints) every step of the way. Dell Technologies is in a unique position to help you secure entry points and vulnerabilities both above and below the operating system (OS) of the devices on and off your network. As cybercriminals continue to mount a monumental effort to steal your data, we can help you create the right strategic plan to mitigate their efforts and stay secure from anywhere.

Keep sensitive data safe from hackers and malware →

Protect your institution from ransomware attacks →

Prevent the disruption of your virtual learning environment →



Keep sensitive data safe from hackers and malware

Block unknown threats

Unsecured laptops and tablets are ideal targets for viruses, phishing scams, adware, and worms.

Dell SafeGuard and Response, powered by VMware Carbon Black Cloud™ Prevention and Secureworks Taegis™ XDR, can be included on your Dell Latitude laptops or 2-in-1 PCs. Dell SafeGuard and Response is also certified to run in a mixed OS environment to further protect your educational institution from cyberattacks.

VMware Carbon Black Cloud Prevention is a next-generation antivirus solution that protects against malicious behavior to stop the full spectrum of modern cyberattacks, whether the Windows 10 or macOS device is online or offline.

Learn more →

Secureworks Taegis XDR is investigation and response software that combines the power of human intellect with security analytics to unify cyberattack detection and response across your entire ecosystem.

Learn more →

Meet compliance requirements

Encrypted web and app traffic is extremely difficult to inspect, which makes it harder to monitor online activity.

Dell SafeData with Netskope Security Cloud and Absolute protects data on school-issued computers and secures information in the cloud so teachers and students can safely collaborate.

Netskope Security Cloud protects assets in institution-managed and unmanaged apps to meet compliance requirements and prevent data loss.

Learn more →

Absolute enables safer, smarter and more secure learning. You can manage and secure devices and data with a persistent, unbreakable connection on or off your network. Absolute supports Windows and Chrome OS environments.

Learn more →

Thwart advanced cyberattacks

Dell Education Latitude laptops and 2-in-1 PCs, along with Optiplex and Precision workstations, come with built-in intelligence and security.

Dell SafeBIOS prevents malware from sneaking in during the start-up process and hiding under the operating system until it can access your institution's network and wreak havoc there.

Dell SafeBIOS alerts you to threats lurking below the operating system and the applications layered above it.

Learn more →

Protect your institution from ransomware attacks

Prevent, detect and remediate ransomware attacks quickly and efficiently with Dell SafeGuard and Response, powered by VMware Carbon Black Cloud Prevention and Secureworks Taegis XDR. Dell SafeGuard and Response can be included on your new Dell Latitude laptops or 2-in-1 PCs and added to other Windows 10 computers in your inventory.

Learn and Prevent

VMware Carbon Black Cloud Prevention advanced machine learning models analyze device data to uncover malicious behavior to stop all types of attacks, online and offline.

Capture and Analyze

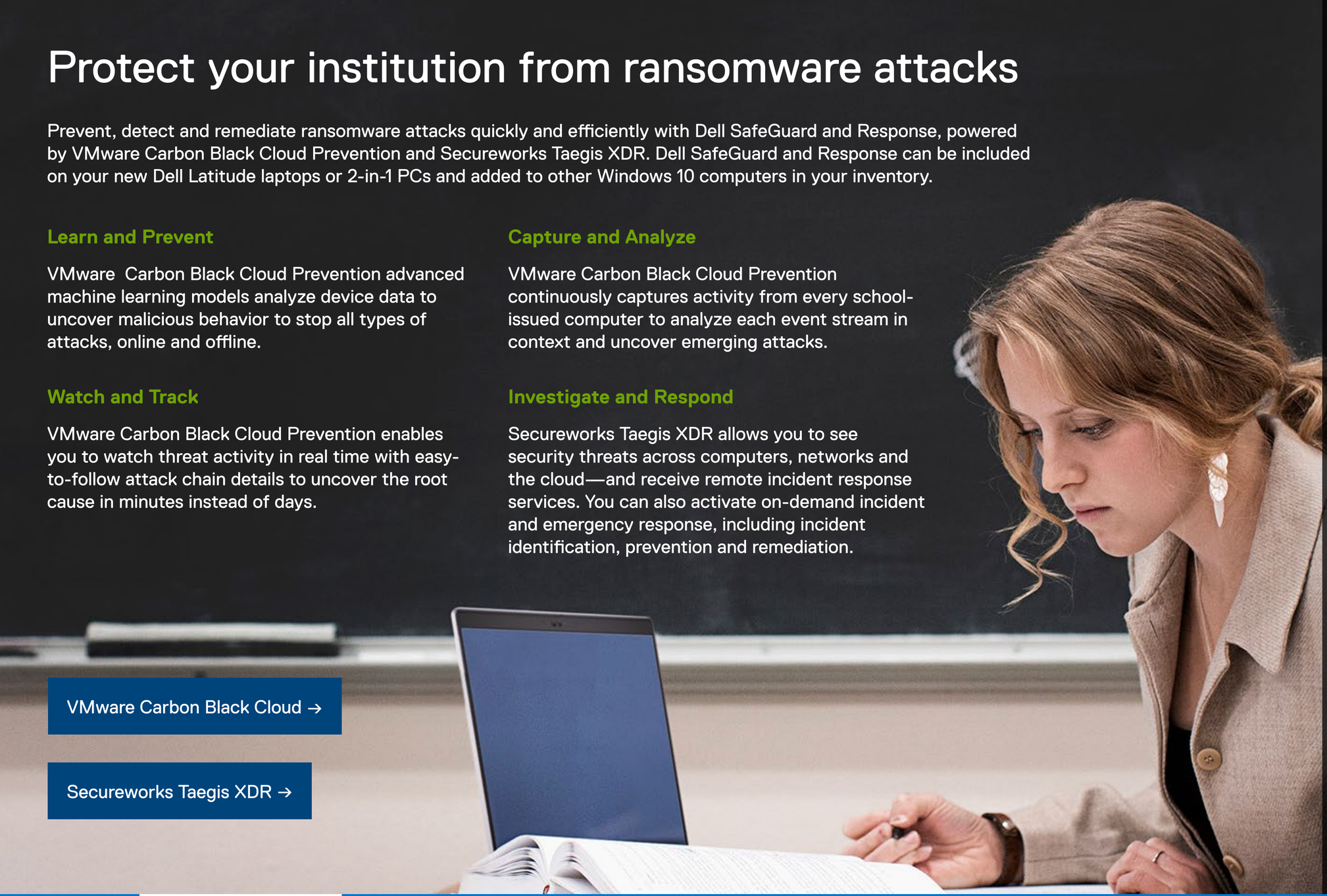
VMware Carbon Black Cloud Prevention continuously captures activity from every school-issued computer to analyze each event stream in context and uncover emerging attacks.

Watch and Track

VMware Carbon Black Cloud Prevention enables you to watch threat activity in real time with easy-to-follow attack chain details to uncover the root cause in minutes instead of days.

Investigate and Respond

Secureworks Taegis XDR allows you to see security threats across computers, networks and the cloud—and receive remote incident response services. You can also activate on-demand incident and emergency response, including incident identification, prevention and remediation.



VMware Carbon Black Cloud →

Secureworks Taegis XDR →

388%

"The number of successful ransomware attacks on the education sector increased by 388 percent between the second and third quarters of 2020." This was not a once-in-a-lifetime occurrence due to COVID-19. A similar jump in numbers happened in 2019.[1]

57%

of all reported ransomware incidents involved K-12 schools in August and September of 2020.[2]

1. Emsisoft Malware Lab, "Ransomware surges in education sector in Q3 as attackers wait patiently for start of school year," November 2020. https://blog.emsisoft.com/en/37193/ransomware-surges-in-education-sector-in-q3-as-attackers-wait-patiently-for-start-of-school-year/
2. ZDNet, "CISA and FBI warn of rise in ransomware attacks targeting K-12 schools," December 2020. https://www.zdnet.com/article/cisa-and-fbi-warn-of-rise-in-ransomware-attacks-targeting-k-12-schools/

Prevent the disruption of your virtual learning environment

With the shift to online and hybrid education, educational institutions are more vulnerable to cyberattacks than ever before. Dell SafeGuard and Response, Dell SafeData and Dell Trusted Devices work together to ensure applications and devices are protected.

- VMware Carbon Black Cloud →
- Secureworks Taegis XDR →
- Netskope Security Cloud →
- Absolute →
- Dell Trusted Devices →

Dell Trusted Devices

For the industry's most secure commercial PCs*

Prevent, detect & respond to attacks
Dell SafeGuard and Response, powered by VMware Carbon Black and Secureworks

Encrypt sensitive information & protect data
Dell SafeData with Netskope and Absolute

Access your device securely from anywhere
VMware Workspace ONE

Above the OS & added on

DETECT

PREVENT

RESPOND

Ensure hardware is tamper-free on delivery
Dell SafeSupply Chain*

Maintain on-screen digital privacy
Dell SafeScreen
Dell SafeShutter

Below the OS & built-in

Gain visibility to BIOS tampering
Dell SafeBIOS

Secure end user credentials
Dell SafeID

VMware Carbon Black Cloud Prevention device protection

VMware Carbon Black Cloud™ Prevention combines intelligent system hardening and behavioral analytics to keep emerging threats at bay on an easy-to-use console. By analyzing more than 1 trillion security events worldwide per day, VMware Carbon Black Cloud Prevention proactively uncovers attackers' behavior patterns and empowers defenders to detect and stop cyberattacks before they happen.

Cyber incidents are on the rise

During the 2020 calendar year, the K-12 Cyber Incident Map reported a rate of more than two cyber incidents per school day.[3]

Extortion is on the rise

In early 2019, hackers demanded thousands of dollars for stolen information after accessing the admissions databases for colleges in Ohio, Iowa and New York.[4]

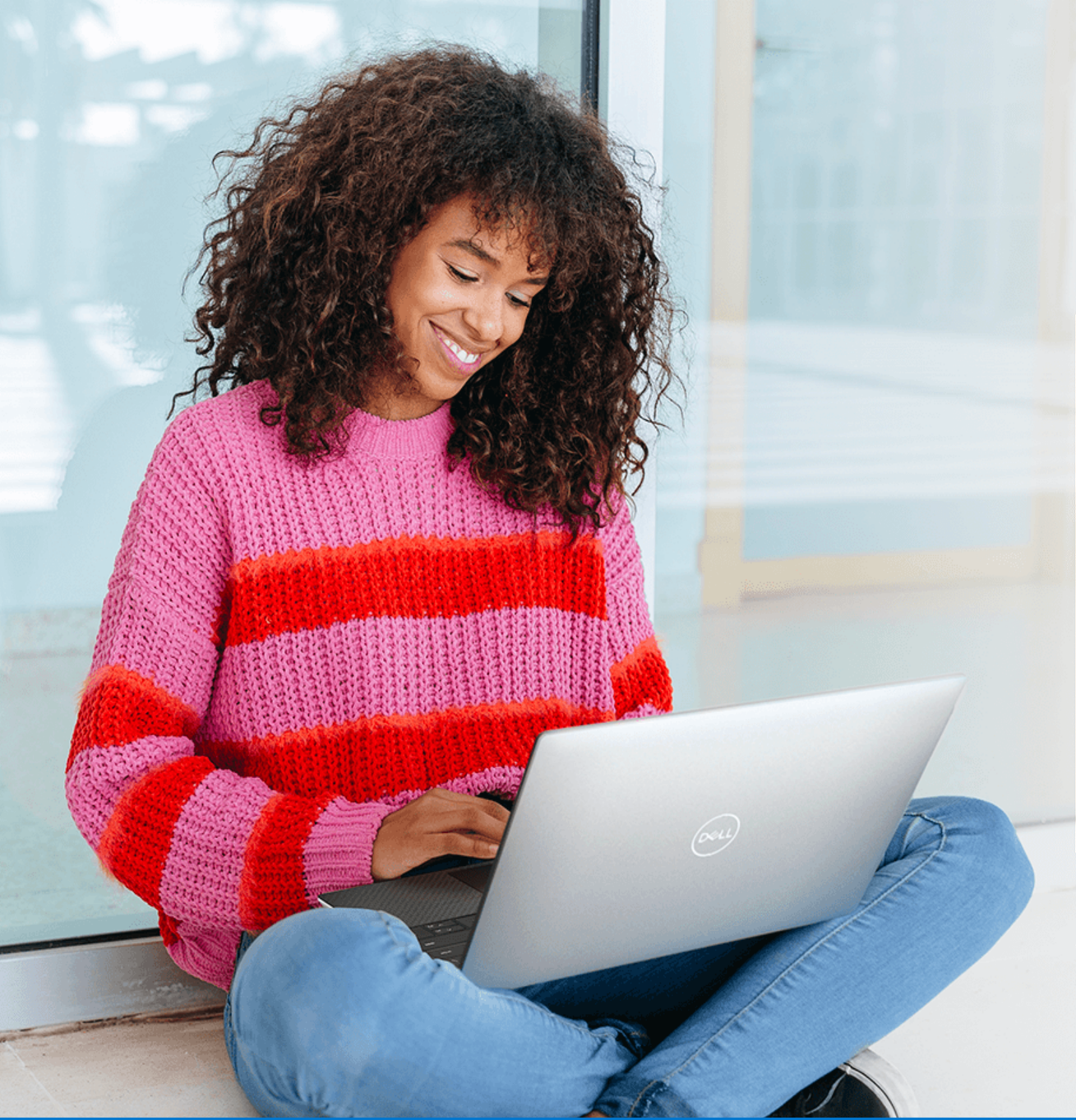
In December 2020, K-12 was the No. 1 target for ransomware and received the majority of all ransomware attacks.[5]

Benefits

- Next-generation antivirus solution replaces and extends traditional antivirus solutions
- Protection from common and advanced attacks on student devices
- Full visibility into Windows 10 or macOS computers to close security gaps and identify indicators of attack (IOA) and indicators of compromise (IOC)
- Clear alerts and context on any blocks that occur
- Simplified operations with a cloud-based platform, no infrastructure required
- The ability to leverage default prevention policies

VMware Carbon Black Cloud Prevention offers immediate protection for your learning environment across any app, any cloud and any Windows 10 or macOS device.

1. Levin, Douglas A. "The State of K-12 Cybersecurity: 2020 Year in Review." EdTech Strategies/K-12 Cybersecurity Resource Center and the K12 Security Information Exchange. 2021. https://k12cybersecure.com/year-in-review/
2. Marquita Brown, "With Lingering Security Gaps, Higher Ed Student Data Breaches Remain a Concern," EdTech, June 26, 2019. https://edtechmagazine.com/higher/article/2019/06/lingering-security-gaps-higher-ed-student-data-breaches-remain-concern
3. The Journal, "K-12 Has Become the Most Targeted Segment for Ransomware," December 11, 2020. https://thejournal.com/articles/2020/12/11/k12-has-become-the-most-targeted-segment-for-ransomware.aspx



Secureworks Taegis™ XDR and MDR

Secureworks Taegis™ XDR combines the power of human intellect with security analytics to unify detection and response across your entire cloud, endpoint, and network ecosystem. This management service provides continuous security monitoring and operational administration of managed endpoints to safeguard investments and meet compliance regulations.

Benefits

- Detect endpoint, network and cloud security threats.
- Stay protected with remote incident response services.
- Activate on-demand incident and emergency response, including incident identification, prevention and remediation.

Secureworks Taegis XDR also provides informed remediation guidance as a response, a service where trained cybersecurity experts scour your logs and provide insight on cyber activity that might otherwise be missed. This service can reduce detection time from ~28 weeks to days or even hours.

Combine Dell Technologies' security expertise and deep knowledge of IT environments with the leading Secureworks Taegis XDR. Dell Technologies Managed Detection and Response (MDR), powered by Secureworks Taegis XDR, is a fully managed service that monitors, detects, investigates and responds to threats across the entire IT environment.

$6 trillion

The estimated cost of global damage from cybercrime in 2021[6]

91%

of cyberattacks begin with a spear-phishing email[7]

6. The National Law Review, "Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion," February 2020. https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion
7. The National Law Review, "Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion," February 2020. https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion

Netskope Security Cloud threat assessment

The Netskope Security Cloud helps stop ransomware, malware, botnet, phishing, and trojan attempts without disrupting benign activities and internet access. It provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites and private apps from anywhere, on any device.

FERPA compliance: The Netskope Security Cloud helps schools with FERPA compliance by detecting and remediating violations that exist in cloud and web services today and preventing new violations from occurring in the future.

CIPA compliance: The Netskope Security Cloud provides 130 polices that block or filter Internet access to anything that violates CIPA rules. These policies can be enforced on and off networks.

HIPAA compliance: IT teams can use Netskope reverse proxy to prevent unauthorized access of data in managed apps and online protections to prevent data misuse on managed devices.

GLBA compliance: The Netskope Security Cloud provides the visibility and control your educational institution needs to safeguard private financial information.

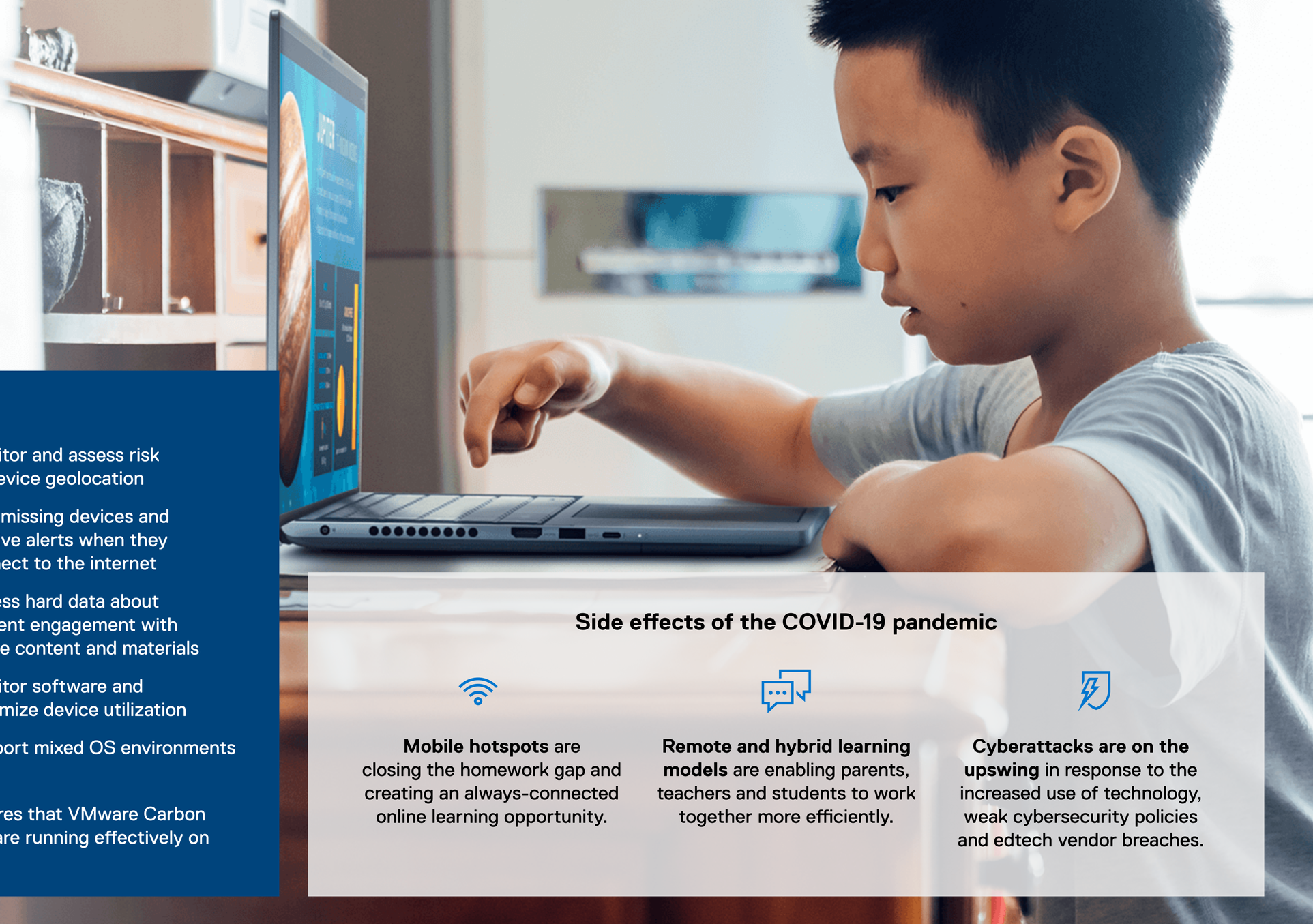
Benefits

- Eliminate threats and remediate incidents in the cloud without admin interaction
- Protect assets in institution-managed apps without touching school-issued or personal devices
- Inspect web transactions to managed apps on personal devices
- Neutralize threats hiding in cloud services such as Google Workspace for Education, Microsoft 365, Box and Dropbox
- Block downloads of sensitive content on personal devices

Real-time data and threat protection

Absolute device health and tracking

Absolute, in partnership with Dell, provides educators, students and administrators with solutions to track, manage and secure all school-owned devices from anywhere in the world. Absolute is firmware-embedded and provides an unbreakable connection to all encrypted devices.



Benefits

- Eliminate blind spots and address breaches in real time
- Detailed usage reports show time spent using each device — and how much active time is spent on approved educational resources
- See and secure data and devices, on and off your network
- Track, freeze, and wipe any missing devices
- Prove compliance and value of existing IT investment
- Monitor and assess risk by device geolocation
- Flag missing devices and receive alerts when they connect to the internet
- Access hard data about student engagement with online content and materials
- Monitor software and maximize device utilization
- Support mixed OS environments

Absolute Persistence technology also ensures that VMware Carbon Black Cloud and Netskope Security Cloud are running effectively on all managed computer systems at all times.

Side effects of the COVID-19 pandemic

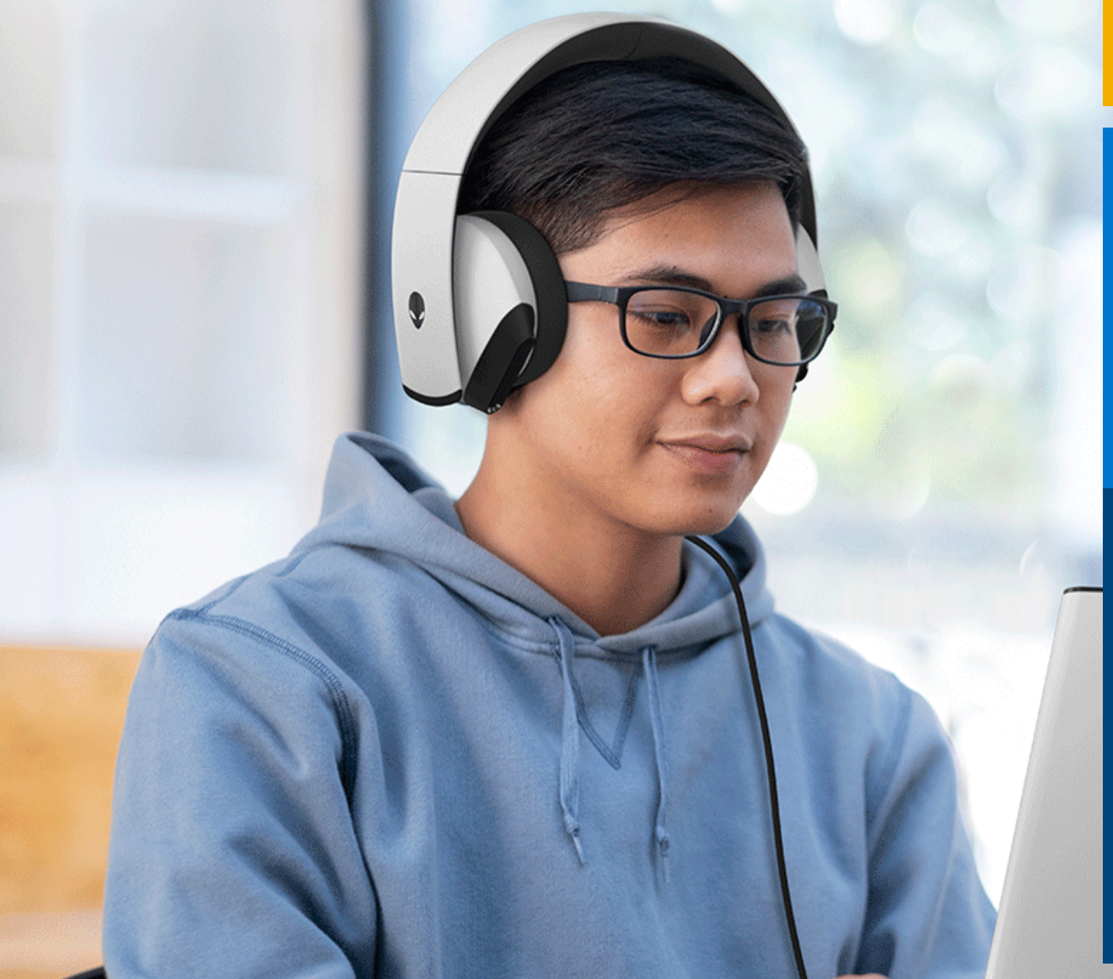
Mobile hotspots are closing the homework gap and creating an always-connected online learning opportunity.

Remote and hybrid learning models are enabling parents, teachers and students to work together more efficiently.

Cyberattacks are on the upswing in response to the increased use of technology, weak cybersecurity policies and edtech vendor breaches.

Dell Trusted Devices

Rather than storing BIOS information on the hardware itself, which is susceptible to corruption, Dell Education Latitude laptops, 2-in-1 PCs and OptiPlex and Precision workstations go through an extra security check at every start-up. Dell SafeBIOS uses a secure off-host cloud environment to compare a stored BIOS image to the new one—making sure nothing is hiding under the operating system.



Benefits

- Thwart advanced cyberattacks
- Secure information on the cloud
- Give students and faculty the freedom to safely collaborate

A BIOS-specific attack is highly technical and, when executed correctly, very damaging. This gaping vulnerability has become an area of increasing concern as attackers look for new vectors of attack.

How Dell SafeBIOS stops malware before it corrupts a Dell Trusted Device and infects the entire network

From the Dell Trusted Device user's perspective:

User turns on Dell Trusted Device → Dell Trusted Device boots up → The device works normally

What's going on in the background:

1. Malware attacks the BIOS on a Dell Trusted Device →
2. User turns on the Dell Trusted Device →
3. Dell SafeBIOS sees that the BIOS is compromised →
4. Dell SafeBIOS replaces the corrupted code with uninfected code from yesterday
5. The Dell Trusted Device boot process proceeds, uninterrupted →
6. Dell SafeBIOS quarantines the infected BIOS →
7. Dell SafeBIOS notifies a Dell SOC Analyst of the attack →
8. Your IT team completes the recommended action

Additional resources

1. Dell Technologies Endpoint Security website: https://www.delltechnologies.com/en-us/endpoint-security/index.htm#scroll=off.
2. Secureworks Taegis XDR: https://www.delltechnologies.com/en-us/collaterals/unauth/data-sheets/products/security/vmware-carbon-black-endpoint-standard-swx-threat-detection-and-response-datasheet.pdf.
3. Netskope Security Cloud: https://www.delltechnologies.com/en-us/collaterals/unauth/data-sheets/products/security/netskope-real-time-protection-datasheet.pdf.
4. Absolute: https://www.delltechnologies.com/en-us/collaterals/unauth/data-sheets/products/security/absolute-visibility-control-resilience-datasheet.pdf.
5. Dell SafeGuard and Response data sheet: https://www.delltechnologies.com/en-us/collaterals/unauth/data-sheets/solutions/vmware-carbon-black-cloud-endpoint-standard-datasheet.pdf.
6. Dell SafeData data sheet: https://www.delltechnologies.com/en-us/collaterals/unauth/white-papers/products/security/dell-trusted-device-below-the-os-whitepaper.pdf.
7. Dell SafeBios data sheet: https://www.delltechnologies.com/en-us/collaterals/unauth/data-sheets/products/security/dell-safebios-datasheet.pdf.
8. Securing K-2 with VMware Carbon Black Cloud: https://www.delltechnologies.com/en-us/events/webinar/home.htm?commid=469758.

For additional assistance, email Endpointsecurity@Dell.com