

DELLTechnologies /Forum

REAL TRANSFORMATION

GLOBAL SPONSORS



DELLTechnologies /Forum

Endpoint Security Strategy for the Digital Age

Aarron Quach

Security Engineering Lead
Dell Technologies

Keeping the business free from cyber attacks is an impossible task...



EXTERNAL THREATS



USER BEHAVIOR



LIMITED SECURITY RESOURCES

108

Days before a silent
attack is detected

72%

Of end users share
confidential data
externally

3.5M

Security professionals
needed by 2022 to fill
labor shortage



The impossible becomes possible with Dell Endpoint Security

Protect your ecosystem, giving you the freedom and peace of mind to focus on other strategic initiatives that enable workforce transformation



Secureworks[®]

Trusted Security Partner

Trusted Devices

Security foundation and trust begins at the endpoint



- SafeBIOS
- SafeID
- SafeScreen

Trusted Data

Cutting edge business protection to enable smart collaboration



- SafeGuard and Response
- SafeData

Built-in security

Most secure commercial devices

Comprehensive ecosystem protection

Smart collaboration

Trusted Devices with Dell Commercial PCs

Security begins with the endpoint with built-in security, where establishing platform root of trust can help ensure your device can be trusted.



Intel vPro platforms include Intel Authenticate and Intel Hardware Shield

SafeBIOS

Visibility to BIOS tampering with Dell exclusive off-host BIOS verification

SafeID

Only Dell secures end user credentials with a dedicated security chip designed into the PC

SafeScreen

Keep data safe from prying eyes with improved battery life consumption over the competition

Trusted Data with Dell SafeGuard and Response

Intelligent and prompt security decisions powered by endpoint telemetry and validated by dedicated security experts

Comprehensive threat management

- **Prevent** 99% of endpoint threats from contaminating your environment
- **Detect** non-malware threats already lurking in the environment and obtain an action plan for focused remediation
- **Respond** to cyber incidents quickly and efficiently or even prepare in advance for the unthinkable



SafeGuard and Response powered by Secureworks

Prevent

Next generation Anti-Virus (NGAV): A next-gen antivirus solution using artificial intelligence, (AI), and machine learning, (ML), that is cloud-hosted and helps stop 99% of all malware and non malware attacks.

Stops malware

99% efficacy – both online and offline

Improved system performance

Low impact on endpoint resources with ~ 1% CPU usage

Port blocker

Device Control enables protection of USB devices

SafeGuard and Response powered by Secureworks

Detect

Endpoint Detection and Response (EDR): Unified platform that combines NGAV with the ability to detect malware and non-malware attacks in real time with speed and efficiency.

Advanced protection

Protects against malware and non-malware threats

Full spectrum visibility

Identifies attacks quickly – silent attacks can go unnoticed for an average of 108 days

Includes NGAV

Integrated solution for unified protection

SafeGuard and Response powered by Secureworks

Detect

Managed EDR (MDR): Secureworks utilizes skilled professionals to manage the EDR solution, providing the resources and intelligence to quickly and efficiently remediate identified threats

Continuous Monitoring

Security experts monitor logs and identify issues 24 x 7 x 365

Fast detection

Reduced time to detect from ~28 weeks to days or even hours

Includes NGAV and EDR

Combines the power of NGAV and EDR with security horsepower

SafeGuard and Response powered by Secureworks

Respond

Incident Response: A 40 hour retainer for on-demand assistance from the Secureworks Incident Response team to respond to and mitigate cyber incidents efficiently and effectively.

Help when you need it most

Emergency incident response to handle the crisis a breach creates

Proactive

Readiness assessments develop detailed action plans for when the unthinkable happens

Targeted threat hunting

Identities hidden threats lurking in the environment

Trusted Data with Dell SafeData

Protect, control and monitor data across hybrid applications, devices or operating systems all without disrupting user workflows.

Smart collaboration

- Collaboration must be secure
- Fines and penalties for not protecting data are growing
- Data breaches cause brand damage



Why Dell

Trusted Devices enable Trusted Data - helping protect your competitive advantage while freeing up time to focus on additional strategic priorities

Built-in Security



SafeID and SafeBIOS SafeScreen

Foundational to Dell's most secure commercial PCs

Comprehensive threat management



SafeGuard and Response

Intelligent security decisions powered by telemetry and security experts

Smart collaboration



Safe Data

Data security wherever data roams

Trusted endpoint security partner



Trusted Devices enable Trusted Data from a single, trusted partner