Evolving cyber threats circumvent software-only defenses.

Help Shrink the Attack Surface of Endpoints with Hardware-assisted Protections

THE CHALLENGES

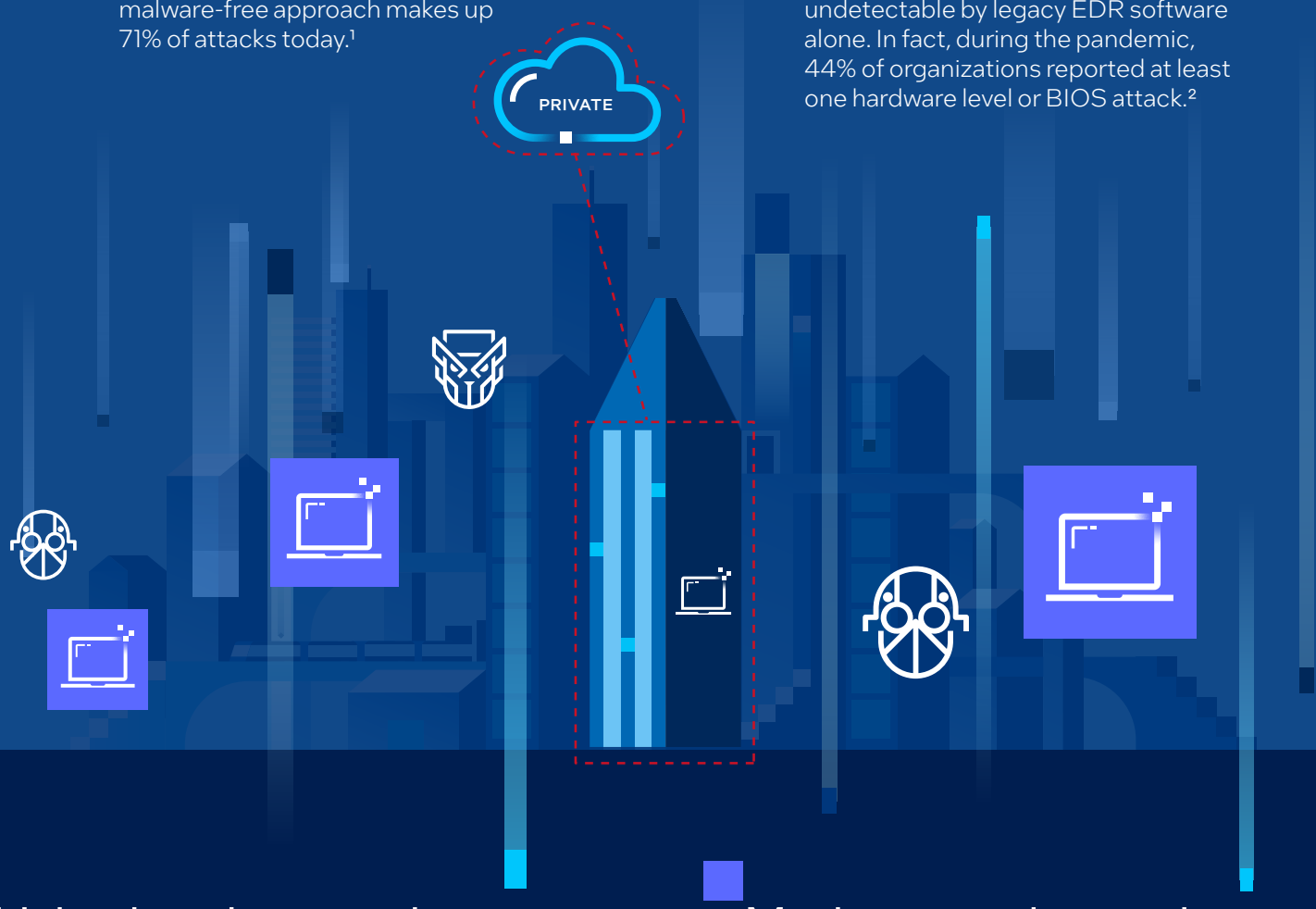
Emerging Attack Vectors Creating New Risk

Fileless Techniques

Threat actors can orchestrate fileless attacks entirely in memory, leaving little to no trace. This malware-free approach makes up 71% of attacks today.[1]

Firmware Attacks

Attackers are increasingly targeting rootkits and other firmware vulnerabilities which are largely undetectable by legacy EDR software alone. In fact, during the pandemic, 44% of organizations reported at least one hardware level or BIOS attack.[2]



Hybrid work expands the attack surface.

69% of organizations reported a cyberattack as a result of a poorly managed internet-facing asset.[3]

Modern attacks evade software-only protections.

90% of successful cyberattacks originate at endpoints devices.[4]

Effective endpoint security requires multiple layers of defense that work together.

THE SOLUTION

Dell Trusted Devices, Intel silicon protections, and CrowdStrike Falcon Insight XDR work together to **help detect and stop modern threats.**

Reduce Endpoint Attack Surface by 70%[5]

Shut down entire classes of threats with Dell PCs running the latest generation of Intel® Core™ processors on the Intel vPro® platform. Enhance and extend protection across the stack with the CrowdStrike Falcon® platform.

Enhance Threat Detection

Uncover early indicators of attack (IOAs) with hardware enhanced exploit detection.

Establish Zero Trust Readiness

Maintain device trust with full control over security posture via remote access (SaaS) to hardware telemetry and below-the-OS alerts.

Optimize Security Investments

Realize the efficiencies of consolidating security providers.

Activate in Seconds

Get hardware-based security right out of the box and toggle on:

- Accelerated memory scanning for fileless attacks
- Hardware enhanced exploit detection (HEED) return-oriented programming (ROP) attacks to memory
- Below-the-OS protections including Dell SafeBIOS BIOS Events & Indicators of Attack
- Dell remediation solutions

Deep ecosystem collaboration enables advanced threat detection and response.

Contact **global.security.sales@Dell.com** and ask for CrowdStrike Falcon on Dell commercial PCs on the Intel vPro platform.

→ Intel / Dell / CrowdStrike Solution Brief

→ Dell commercial PCs based on Intel vPro

→ The Intel vPro platform

Sources and Disclaimers

1. CrowdStrike 2023 Global Threat Report
2. Futurum Research, 2021.
3. ESG Complete Survey Results, Security Hygiene and Posture Management, Jan. 2022.
4. IBM Endpoint Security
5. The latest Intel vPro based PCs provide an estimated 70% attack surface reduction compared to four-year-old devices. Based on IOActive's "Intel vPro 13th gen Attack Surface Study" published March 2023 (commissioned by Intel), which evaluates Intel vPro devices powered by 13th gen Intel Core processors against four-year-old Intel-based PCs on Windows OS. Details at www.intel.com/performance-vpro. Results may vary.

Performance varies by use, configuration and other factors. Learn more at www.intel.com/PerformanceIndex or your Intel representative.
Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates.
No product or component can be absolutely secure.
Your costs and results may vary.