Evolving cyber threats circumvent software-only defenses.

Help Shrink the Attack Surface of Endpoints with Hardware-Assisted Security

THE CHALLENGES

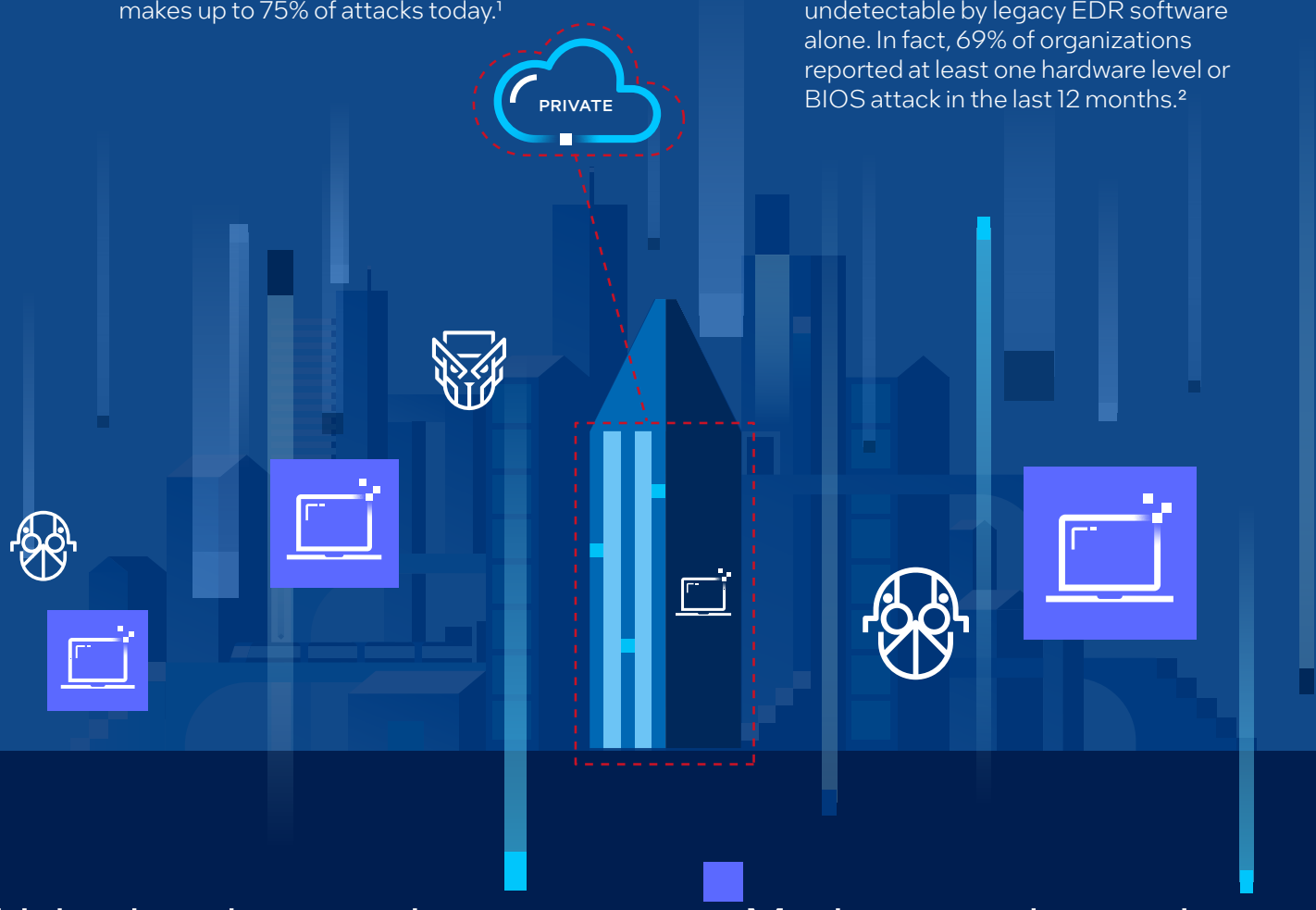
Emerging Attack Vectors Creating New Risk

Fileless Techniques

Threat actors can orchestrate fileless attacks entirely in memory, leaving little to no trace. This malware-free approach makes up to 75% 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, 69% of organizations reported at least one hardware level or BIOS attack in the last 12 months.[2]



Hybrid work expands the attack surface.

Since the pandemic, device-based attacks have **increased by 1.5x**.[2]

Modern attacks evade software-only protections.

90% of successful cyberattacks originate at endpoints devices.[3]

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%[4]

Shut down entire classes of threats with Dell Trusted Devices, the industry's most secure commercial PCs[5], running the latest generation of Intel® Core™ Ultra 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.

Work with Zero Trust-Capable Solutions

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 with Ease

Get hardware-assisted security that's easy to set up and configure:

- Accelerated memory scanning for fileless attacks
- Hardware enhanced exploit detection (HEED) return-oriented programming (ROP) attacks to memory
- Below-the-OS defenses including Dell SafeBIOS Indicators of Attack and device telemetry
- 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

Sources and Disclaimers

1. CrowdStrike 2024 Global Threat Report
2. The Futurum Group, Endpoint Security Trends, 2023.
3. IBM Endpoint Security
4. 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.
5. Based on Dell internal analysis, September 2023. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features.

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.