PROWESS

# Are You Fighting Today's Threats with Yesterday's Defenses?

The role of hardware-based security in the battle against advanced and below-the-operating-system attacks, including ransomware.

**Today's client-security environment is more complex than ever.** Attacks are growing in number and sophistication,[1] while well-established cybercrime methods, such as phishing, continue to open doors to hackers. At the same time, the attack surface has increased due to many more employees working from home, outside the protection of the corporate firewall.

These realities pose a serious challenge to traditional client-security software, which resides above the operating system (OS). Due to their lack of visibility below the OS, traditional client-security programs have limited ability to protect system software. A thorough security solution for desktop or laptop PCs should use hardware-based security capabilities, which extend protection below the OS, to augment software-only detection techniques. As you will see in this paper, hardware-enabled security can help detect and protect against new types of threats, including ransomware and cryptomining attacks. And in fact, hardware-based security has the potential to eliminate an entire class of attacks: control-flow hijacking.

## Cybercriminals Are Highly Motivated

Hacking is big business. In fact, global damage related to cybercrime is projected to hit $6 trillion annually by 2021 and $10.5 trillion by 2025—a 15-percent-per-year growth rate.[2] To put those numbers in perspective, the US spent $3.5 trillion on healthcare in 2017.[3] How could $6 to $10 trillion in damages even be possible?

Many factors contribute to this sobering reality, including the vast scale of threats. For example, experts predict "skyrocketing" numbers of attacks, such as ransomware and those targeting vulnerabilities in firmware, as criminals seek new revenue streams.[4] Worldwide, McAfee Labs observed 375 threats per minute in Q1 2020 and a 689 percent increase in new malware targeting Windows PowerShell®,[5] and nearly 1 in 5 people were hit by at least one malware-class web-based attack in 2019.[6]

As high as those numbers are, what might be more alarming is the rise in social engineering tactics that play on public pandemic fears. For example, Trend Micro reported nearly 9 million COVID-19-related threats in just the first half of 2020.[7] What's worse is those social engineering tactics are working. Fifty-three percent

### Why hardware-based security is crucial

**1,185**

per month—average number of phishing emails received by enterprises[8]

**77%**

of ransomware victims had up-to-date endpoint protection in place[14]

**53%**

of organizations are seeing increased attacks due to COVID-19[8]

**70%**

of organizations without a firmware upgrade plan will be breached[16]

of respondents to one study say their organizations are seeing an increase in phishing attacks during the COVID-19 pandemic, and nearly one-third say those attacks have become more successful.[8] And the recovery cost alone is astronomical to IT departments, considering that 15 percent of enterprise security teams spend anywhere between one and four days remediating a cyberattack.[8]

## Ransomware, Cryptomining, and Below-the-OS Attacks Are Rising

Ransomware and cryptomining are rising in popularity among hacking groups. Indeed, new coin-miner malware increased by 26 percent in the first half of 2020,[5] while the number of ransomware attacks grew by 715 percent in 2020 compared to 2019.[9] By another measurement, more than 750,000 computers of unique users of Kaspersky software were targeted by encryptors (ransomware) and more than 2.2 million were targeted by cryptominers.[6] Ransomware is most often delivered by phishing attacks (of which enterprises receive on average 1,185 per month).[8] In 2019, ransomware affected 51 percent of businesses and represented 26 percent of all reported e-crime.[10,11] And what might surprise you is that 77 percent of organizations hit by ransomware in 2018 were running up-to-date endpoint-protection software.[12] Clearly, traditional client-security software is not enough to counteract today's threats—even if it is up to date.

> "James Morrison, a computer scientist with the FBI's Houston Cyber Task Force, explained that criminal organizations are constantly looking for new avenues of attack, with ransomware and attacks on firmware and hardware gaining prominence as holes in operating systems and software are patched."
> — HPE[4]

As if the threat landscape were not complex enough, hackers are now turning to attacks below the OS, on firmware. Gartner reports that by 2022, 70 percent of organizations that do not have a firmware-upgrade plan in place will be breached due to a firmware vulnerability.[13] One example of malware that exploits firmware is LoJax, a Unified Extensible Firmware Interface (UEFI) rootkit capable of writing and executing malware on disk during the boot process, before software-based anti-malware tools are running.[14]

Today's malicious actors understand that traditional approaches to anti-malware lack visibility into firmware, both within hardware components and at the system level. These attackers use firmware implants and back doors to bypass security controls, to persist, and to disrupt enterprise infrastructure. According to the National Vulnerabilities Database maintained by the National Institute of Standards and Technologies (NIST), firmware vulnerabilities increased by 757 percent between 2016 and 2019.[15] And BIOS attacks, practically unheard of until 2019, are likely to go unnoticed, thereby allowing hackers to disable secure booting, downgrade the BIOS to a vulnerable version, or even wipe data and ransom a device.[16] In one study, 73 percent of participants who didn't prioritize firmware security reported experiencing a high rate of unknown malware breaches, which made them almost impossible to track and neutralize.[17]

If you think below-the-OS attacks are too difficult to pose a serious threat, think again. In a Forrester Consulting survey, 63 percent of companies said their data was potentially compromised within the last 12 months due to malware taking advantage of vulnerabilities in firmware.[18] And researchers detected vulnerabilities stemming from unpatched BIOS in up to 80 percent of computers they examined.[17] Even so, it is not yet industry-standard practice to look for threats below the OS, nor even to update the BIOS/UEFI layer as frequently as the OS and applications. Which means, as Gartner stated, that "many current approaches to improve cybersecurity fall short of providing appropriate and defensible levels of protection."[19]

# Hardware-Enabled Security Enhances Protections

Advanced attacks that target client memory, hypervisors, or firmware require advanced defenses that extend protection beyond the spaces that are typically patrolled by security software running on top of the OS. Those defenses should be rooted in hardware and should perform their functions without impeding the user experience or requiring extensive administrative involvement.

Intel® Hardware Shield provides one such example of hardware-based defenses. It is a suite of hardware-enabled features that extends security below the OS and provides advanced threat detection and app and data protection. It is available on business clients powered by Intel vPro® platform processors (see Figure 1). It helps reduce the risk that a bug or vulnerability in firmware could be used to inject malicious code into the platform at runtime and hide that code from traditional client security solutions. It helps detect and protect against advanced threats like ransomware, cryptomining, and control-flow hijacking.

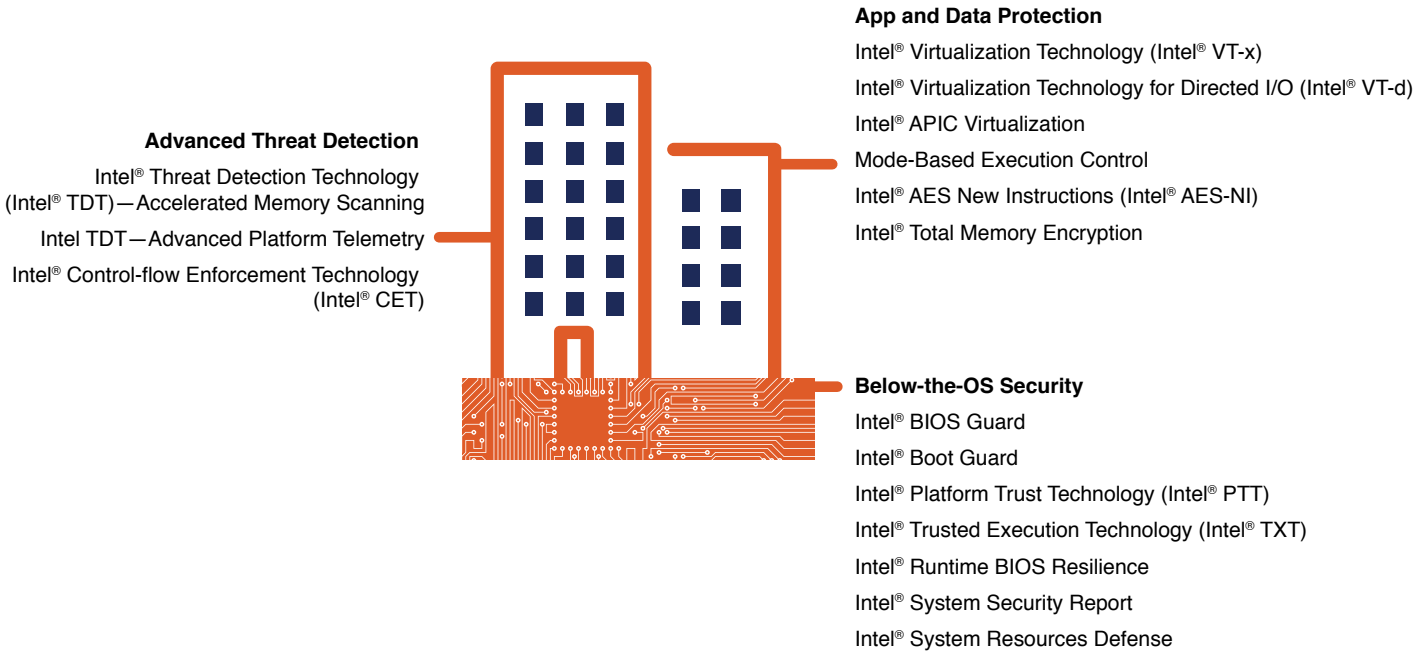


**Figure 1.** Intel® Hardware Shield provides hardware-based security to enhance protection and detection

# How Intel® Hardware Shield Provides Below-the-OS Protection

During boot processes, Intel Hardware Shield helps protect components below the OS with several features that harden the client's environment on top of which the OS and applications run. This approach is analogous to ensuring that the basement-level access points to a house are closed and locked. Traditional OS-based security solutions help protect upper floors from intrusion; but if the basement remains unprotected, the whole house is vulnerable.

One of the Intel Hardware Shield technologies that helps protect the hardware environment is Intel® Runtime BIOS Resilience (IRBR). This technology prevents modification of the memory policy that defines what can be accessed from within System Management Mode (SMM). SMM is a privileged execution mode of the processor that is invisible to the OS and used by firmware for many important background tasks. IRBR also prevents code that SMM can access from being modified during runtime after the platform has completed its initial boot process. Another component of Intel Hardware Shield, Intel® System Resources Defense, takes a similar approach to help protect apps and data. It goes further than IRBR and creates least-privileged access to other critical system resources, such as model-specific registers, memory-map input/output (MMIO), hypervisor memory, and more.

Intel® Trusted Execution Technology (Intel® TXT) is another component of Intel Hardware Shield that enhances below-the-OS security. It provides a hardware-based root of trust to help ensure that a client boots with a known-good configuration. It does this by performing a dynamic launch, which resets the software environment without having to go through the reset vector and all the BIOS-reset processes. In the dynamic launch, dynamic platform configuration registers (PCRs) inside the Trusted Platform Module (TPM) are reset to their initial measurement value, and an authenticated code module (ACM) verifies that the platform is configured correctly. If it is, the ACM transfers control to the measured launch environment (MLE). This is an environment "surrounded" by hardware-based protections that ensure the MLE hasn't been modified by something that is not part of the dynamic launch measurements. Finally, Intel® System Security Report works with Intel TXT to give the OS unique and increased visibility into SMM protections that have been implemented with Intel Runtime BIOS Resilience and Intel System Resources Defense. This visibility shows what system hardware and resources can be used or are accessible by firmware system management interrupt (SMI) handlers. The MLE can then make policy decisions about what services it wants to perform based on the information from Intel System Security Report.

# Defend System Memory Against Control-Flow Attacks

Intel Hardware Shield also includes Intel® Control-flow Enforcement Technology (Intel® CET), which helps prevent the hijacking of legitimate code, thus protecting against an entire class of hacking techniques called control-flow attacks. In this type of maneuver, a hacker misuses existing code in executable memory and assigns it new return pointers, which can change program behavior in nefarious ways. These types of attacks have been difficult to mitigate through software alone, so deep integration with hardware is needed to deliver better protection with minimal performance impact. That's what Intel has done with Intel CET, and as of this writing, comparable capabilities are not available on AMD processors.

To help prevent return-oriented programming (ROP) attacks, Intel CET creates a "snapshot" of the program's stack of return instructions called a "shadow stack," and stores the snapshot in CPU cache. Even if attackers are successful in modifying the return addresses of the data stack, they cannot modify the shadow stack. Intel CET then compares the

addresses on the data stack to the addresses on the shadow stack, and if a mismatch is detected, it helps prevent the attack by reporting an exception to the OS. Intel CET also tracks indirect branch-jump instructions and assesses them for legitimacy, which helps software detect call-oriented programming (COP) and jump-oriented programming (JOP) attacks.

## Extend Protection of Apps and Data with Virtualization-Based Security

Intel Hardware Shield also enables virtualization-based security (VBS) to help protect users' access credentials, applications, and data in virtual secure mode (VSM) enclaves. In this way, Intel® Virtualization Technology (Intel® VT) features in Intel Hardware Shield enable VBS to protect credentials and the OS from kernel-level malware.

Additionally, with major operating systems such as Windows 10 using OS virtualization as the new baseline, Intel Hardware Shield enables isolation of applications to help prevent malware from infecting or compromising an entire system. For example, if a user visits an untrusted website in Microsoft Edge® or Internet Explorer®, Microsoft® Defender Application Guard opens the site in an isolated Hyper-V® container, separate from the host OS. If the site runs a malicious script, the host PC is protected because the script runs in a virtualized, isolated environment.[20] Because hardware-based virtualization makes virtualization practical by reducing performance overhead, users can run multiple virtualized environments on the same PC for better app and data security through isolation. These environments can even support different operating systems, such as Linux and Windows 10, running as guest operating systems alongside the host OS, with negligible impact on system performance. If a malicious payload such as ransomware successfully infects an opaque container, Intel Hardware Shield provides detailed CPU telemetry to detect those attacks, as you'll see below.

Hardware-supported VBS provides the performance needed to run virtualized environments on clients with minimal impact on the user experience, all while protecting those environments with hardware-enforced isolation and encryption. These protections make it difficult for attackers to inject malicious code into the guest OS, host OS, or applications running on them. Owing to the great performance of Intel's hardware-based virtualization, its use has now become prevalent in enterprises.

## Hardware-Based Security Can Detect Ransomware Attacks Early

Ransomware is one of the most urgent problems that enterprises face. It can move laterally throughout an organization and, when triggered, encrypt critical files in a matter of seconds. Ransomware attacks have brought businesses and government organizations to a halt in several high-profile attacks, and they are projected to cause more than $20 billion in damages in 2021—57 times more than in 2015.[21] Beyond the monetary costs, these attacks had real impacts on human life: medical records became lost or inaccessible, 911 services were disrupted, badge scanners and building-access systems ceased to work, online payment portals went down, and email and phone systems stopped working, among other consequences.[22]

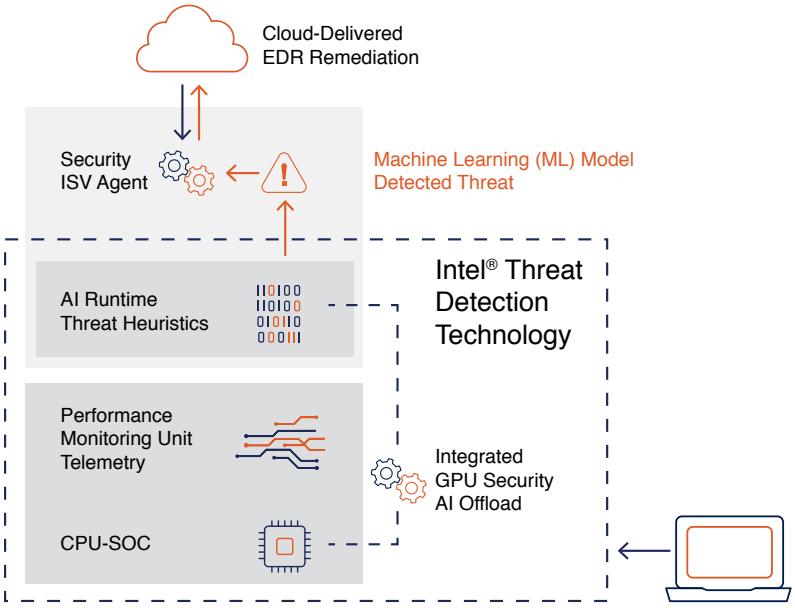


**Figure 2.** Intel® Threat Detection Technology provides hardware-based protection against advanced threats

Software-based solutions struggle to stop ransomware because criminals introduce small variants into the malware to change its signature enough to thwart detection by anti-malware scanners. Remember, 77 percent of organizations hit by ransomware in 2018 were running up-to-date endpoint-protection software.[14] That's why hardware-based protection like Intel® Threat Detection Technology (Intel® TDT) is a critical piece of defense against ransomware and other advanced threats, including cryptominers.

Intel TDT takes advantage of telemetry generated by the CPU's performance monitoring units (PMUs), which track the micro-behaviors of CPU instructions. The Intel PMU sits beneath applications, the OS, and virtualization layers on the system and delivers a more accurate representation of the behavior of active threats, system-wide. Using machine learning (ML)-based runtime algorithms, Intel TDT analyzes patterns in PMU data and detects in real time when the CPU is starting behavior that is consistent with malware, such as cryptomining or ransomware. It then passes a warning signal into an Intel partner's anti-malware application, along with information on the specific OS process that is exhibiting the malware-like behavior. This enables the anti-malware application to quickly remediate before all of a platform's files have been encrypted (in the case of ransomware) or before the hidden cryptomining app has a chance to consume so many resources that it disrupts the performance of legitimate software. In addition, Intel TDT offloads this computationally intensive artificial intelligence (AI)-based security algorithm processing to the integrated graphics processing unit (GPU), minimizing the impact on system performance from the increased detection capability of Intel TDT.

Intel TDT also offloads scanning of memory-based software for malware to the integrated GPU in a feature called Accelerated Memory Scanning (AMS). Scanning memory for known malware signatures is typically a processing-intensive activity. With AMS, Intel TDT takes advantage of the millions of instructions per second (MIPS) available on the on-die GPU, which means ISV software scanning of memory can be accelerated because it is immediately parallelized. That increases the capacity of the security vendor's software to do more scans, which increases efficacy and lowers false positives inherent in threat detection.

Intel TDT also includes additional accelerators for operations such as string extraction, entropy calculation, and generalized pattern extraction. These accelerators help improve independent software vendor (ISV) anti-malware application effectiveness without significant impact on CPU performance. As of this writing, capabilities such as those provided by Intel TDT are only available on Intel-based platforms.

# ISV Support for Intel® Hardware Shield

The hardware-based security capabilities of Intel Hardware Shield are normally leveraged through software. Intel Hardware Shield data is passed to anti-malware software to accelerate and enhance detection and protection, allowing quicker responses to threats. Several of Intel's ISV partners' products already take advantage of Intel Hardware Shield features. For example, Microsoft® Defender and BlackBerry® Optics use Intel TDT to detect cryptomining malware, and Microsoft Defender and SentinelOne® use AMS to strengthen their products' capabilities.

**Intel's Commitment to Security**

Intel has formalized its stance on security through a "Security First Pledge," which affirms that the security of Intel® products is an ongoing priority, not a single once-and-done event. For Intel, this commitment begins with engineering security capabilities into products from the beginning. Then, once products are released, Intel continues to actively support them and address vulnerabilities that might arise.

Through its Bug Bounty program, Intel incentivizes security researchers to report security vulnerabilities in Intel products to enable a coordinated response. When a vulnerability is found in one of its products, Intel acts quickly to mitigate the issue following a five-stage process:

- Initial evaluation, which includes verifying the vulnerability and identifying its scope
- Architectural assessment, which includes identification of mitigation options
- Mitigation development and assurance
- Mitigation deployment
- Public disclosure

Intel's deep and broad ecosystem relationships foster security-related collaboration and innovation on multiple fronts, including hardware, software, and service vendors, to develop and deploy mitigations.

To learn more about Intel's approach to security in its products and across the industry, visit **www.intel.com/content/www/us/en/corporate-responsibility/product-security.html**.

# Deploy a Hardened Foundation for Client Devices

As you evaluate client devices for your users, make sure they include hardware-based security capabilities. These capabilities create a foundation for improved defenses below the OS, for improved protection for apps and data, and for enhanced detection of and protection against advanced threats including ransomware and cryptomining. Hardware-based capabilities to look for in modern client devices are shown in Table 1.

**Table 1.** Intel® Hardware Shield helps protect business clients from today's evolving threats by providing security capabilities rooted in silicon; some of these security capabilities are shown here

| Capability | What It Does |
|---|---|
| Protection below the OS | Verified boot helps ensure that the client boots with a known-good configuration of hardware, firmware, and OS.<br>Firmware protection gives System Management Mode (SMM) least-privileged access to system resources to help prevent firmware-based malware execution. |
| Data and app protection | Enables virtualization-based security (VBS), which provides isolation for apps and data and helps prevent kernel-level malware. |
| Advanced threat detection | Enhances detection of advanced threats, including ransomware and crypto mining, and helps prevent memory-based attacks without impeding the user experience.<br>Has the potential to eliminate an entire class of attacks: control-flow hijacking. |

In today's security landscape, with ever-evolving attacks and increasing numbers of threats, software-only solutions are no longer adequate. Cyber criminals are finding clever ways for their malware to evade traditional software-based detection, and they are driving attacks lower down the computing stack. That's why a hardened client fleet is critical to businesses that want to strengthen their protection against advanced threats such as ransomware and control-flow programming attacks.

For more information about the security features of the Intel vPro platform, contact an Intel sales representative or visit the following links:

**intel.com/vpro**

**intel.com/hardwareshield**

[1] Dark Reading. "Malware Variety Grew by 13.7% in 2019." December 2019. www.darkreading.com/threat-intelligence/malware-variety-grew-by-137--in-2019/d/d-id/1336611.

[2] Cybercrime Magazine. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

[3] US Centers for Disease Control and Prevention (CDC). "Health Expenditures." April 2020. www.cdc.gov/nchs/fastats/health-expenditures.htm.

[4] HPE. "FBI warns of increasing ransomware, firmware attacks." June 2018. www.hpe.com/us/en/insights/articles/fbi-warns-of-increasing-ransomware-firmware-attacks-1806.html.

[5] McAfee. "McAfee Labs COVID-19 Threats Report." July 2020. www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-july-2020.pdf.

[6] Kaspersky. "Kaspersky Security Bulletin '19." https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf.

[7] Trend Micro. "Securing the Pandemic-Disrupted Workplace." August 2020. www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report.

[8] GreatHorn. "2020 Phishing Attack Landscape Report." https://info.greathorn.com/report-2020-phishing-attack-landscape.

[9] Bitdefender. "Mid-year Threat Landscape Report." 2020. www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf.

[10] Comodo. "Ransomware Attacks 2020." June 2020. https://enterprise.comodo.com/blog/recent-ransomware-attacks/.

[11] CrowdStrike. "2020 Global Threat Report." 2020. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf.

[12] Sophos. "Businesses Impacted by Repeated Ransomware Attacks and Failing to Close the Gap on Exploits, According to Sophos Global Survey." January 2018. www.sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacks-according-to-sophos-global-survey.aspx.

[13] Eclypsium. "Device Risk Assessment and Patching." https://eclypsium.com/risk-assessment/.

[14] Help Net Security. "The importance of hardening firmware security." July 2019. www.helpnetsecurity.com/2019/07/17/hardening-firmware-security/.

[15] National Institute of Standards and Technology. "National Vulnerability Database." September 2020. https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=firmware+&search_type=all.

[16] Government Technology. "BIOS Attacks and Four Other Security Trends from VMworld 2019." August 2019. www.govtech.com/biz/BIOS-Attacks-and-Four-Other-Security-Trends-from-VMworld-2019.html.

[17] The SSL Store. "Firmware Attacks: What They Are & How I Can Protect Myself?" February 2020. www.thesslstore.com/blog/firmware-attacks-what-they-are-how-i-can-protect-myself/.

[18] Forrester Consulting. "BIOS Security – The Next Frontier for Endpoint Protection." Commissioned by Dell Technologies. June 2019. www.dellemc.com/en-us/collaterals/unauth/analyst-reports/solutions/dell-bios-security-the-next-frontier-for-endpoint-protection.pdf.

[19] Gartner. "The Urgency to Treat Cybersecurity as a Business Decision." February 2020. www.gartner.com/en/documents/3980891/the-urgency-to-treat-cybersecurity-as-a-business-decisio.

[20] For more information about virtualization-based security and how hardware enables it, see: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview and https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs.

[2] Cybercrime Magazine. "Global Ransomware Damage Costs Predicted to Reach $20 Billion by 2021." October 2019. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[22] CPO Magazine. "Ransomware Costs in 2019." January 2020. www.cpomagazine.com/cyber-security/ransomware-costs-in-2019/.