CSO SPONSORED CONTENT

Confronting the threats of cryptojacking and ransomware

Contents

intel®

Cybercriminals leverage software and cloud

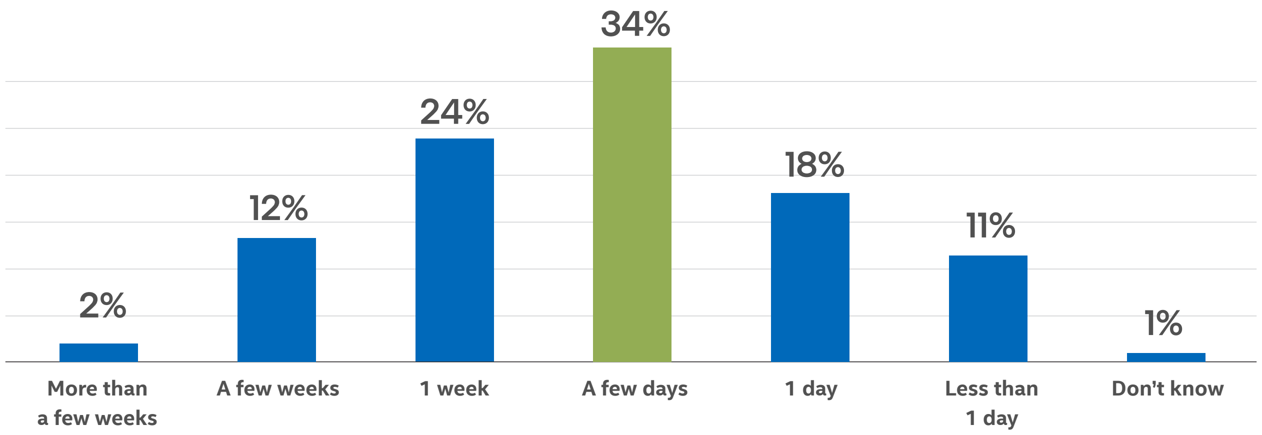
Malware is a technology scourge of the modern era, infecting computer assets for nefarious purposes, often without the knowledge of enterprises. Defenders are often left plugging security gaps after the fact, while the attackers are changing tactics and looking for new opportunities to wreak havoc.

Ransomware and cryptojacking—the hijacking of computer resources to mine cryptocurrencies—represent critical economic threats. Awareness of the ransomware threat has steadily increased due to the impact of successful attacks, while cryptojacking represents a more insidious assault.

Ransomware is on track to cause $1 trillion in financial damage in the U.S. in 2021. According to a recent U.S. Treasury Department analysis, the total value of ransomware-related suspicious activity reported during the first six months of 2021 was $590 million, exceeding the value reported for the entirety of 2020 ($416 million). (Remember: The impact of ransomware goes far beyond the ransom as the business disruption can be the costliest component of the attack.)
More than one-third of ransomware victims report a business disruption of at least one week, according to IDC. (See Figure 1.)

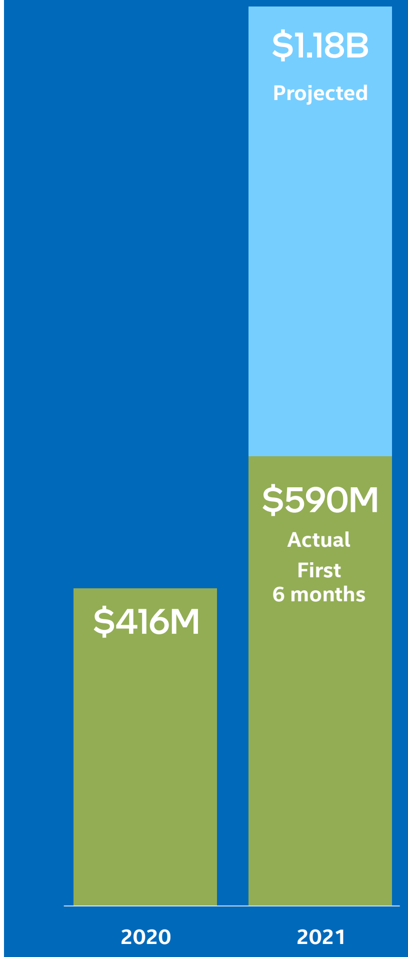
Figure 1: **Business Disruption Due to Ransomware**

Source: Future Enterprise Resiliency & Spending Survey, IDC, July, 2021 (N = 199)



Value of Ransomware Acitivity 2020 vs. 2021

Source: U.S. Treasury Department



“Ransomware and cyberattacks are victimizing businesses large and small across America and are a direct threat to our economy,” Treasury Secretary Janet Yellen has warned.

Cryptojacking is a less-publicized but equally concerning threat. “Because the cryptomining activity occurs in the background, there’s generally no indication that it’s happening other than a slight performance degradation,” explains managed security services provider SageNet. “However, cryptojacking drains systems resources, increases energy consumption, and can shorten the life of IT equipment. It also consumes precious network bandwidth.”

Easy to ignore

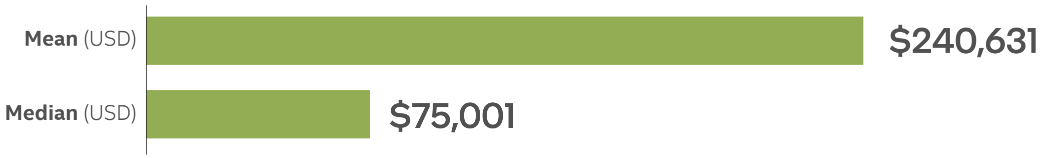
Unless you or your organization is a victim, it’s easy to view malware attacks as somebody else’s problem. But the escalation of ransomware payment demands demonstrates that criminals become more emboldened whenever an attack succeeds.

The Unit 42 security consulting group of Palo Alto Networks found that the average ransomware payment increased 82% to $570,000 in the first half of 2021 compared to 2020. In one widely publicized case, an energy company CEO paid ransomware attackers $4.4 million to reopen a critical fuel pipeline. According to IDC the median ransomware payment in 2021 was just over $75 million, while the average payment was over $240 million (See Figure 2.)

Figure 2: **Ransomware Bounties**

Source: Future Enterprise Resiliency & Spending Survey, IDC, July, 2021

If your organization paid a ransom in the past 12 months to regain access to systems or data, how much was paid? Include the total amount if multiple ransoms were paid.



Cryptojacking can seem abstract, as victims may not even realize they’ve been attacked. But that cost adds up for organizations that are running hundreds or thousands of devices, which may also negatively impact execution on key enterprise processes.

More worrisome is that cryptominers are creating backdoors that they or others can use to steal IP or inject ransomware code. One version of CPU mining software, XMRig, was the second most prevalent form of malware detected in June, according to Checkpoint Software’s Global Threat Index.

Cryptojacking code “could be installed directly on a host computer to always run in the background and potentially even to propagate across a local network or through phishing attacks,” write legal experts specializing in privacy and security. Such code, they warn, could contain ransomware, “or could even be a false flag intended to disguise delivery of a malicious payload.” It’s likely such infected computers could then become part of a botnet, exposing them to further attacks.

A costly arms race

Technological advances increase productivity, they also serve to escalate the continuing arms race between attackers and defenders.

Gartner Inc.'s 2021 CIO Agenda survey revealed that 61% of respondents planned to increase spending on cyber/information security in 2021, while Cybersecurity Ventures projected that global spending on cybersecurity products and services would exceed $1.75 trillion cumulatively between 2021 and 2025.

Despite the immense wealth expended on cyber defenses, attackers continue to find success. According to the Identity Theft Resource Center, by October 2021 the number of data breaches in the U.S. from cyberattacks exceeded the entirety of those reported the previous year.

Increasingly, attackers are targeting weak links in the software supply chain, targeting software vendors and service providers, as was the case in the breaches of SolarWinds and Kaseya, where initial attacks can compromise customers downstream from the initial attack. A single managed services provider (MSP) can serve many customers, providing cybercriminals opportunities to attack multiple companies, at scale.

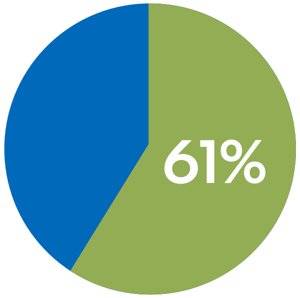
One weakness among enterprise security solutions is the constant stream of alerts and false positives that can create fatigue among IT teams and reduce their effectiveness. But while they're trying to sort through the noise to find the dangers, real ones may be slipping in undetected. According to FireEye's Mandiant Security Validation team, attack simulations determined that only 9% of cyber-attacks generated security alerts, and 53% of successful intrusions went undetected.

Clearly there is a need for a more unified effort aimed at detecting and preventing real cyber dangers. In today's fast-evolving threat environment, security systems must do more than log events; they must deliver timely alerts, autonomously and efficiently, while also reducing false-positive alerts.

Spending spree

Source: Gartner Inc. 2021 CIO Agenda survey

Firms that planned to increase spending on cyber/information security in 2021:



Cybersecurity Ventures projected that global spending on cybersecurity products and services would exceed $1.75 trillion cumulatively between 2021 and 2025

Debunking the myth of the “recent” ransomware problem

December 16, 2021 - By Frank Dickson, Program Vice President within IDC’s Cybersecurity Products research practice

Ransomware conversations have become increasingly common, moving from Pennsylvania Avenue and Wall Street to Main Street. In fact, the conversation has reached all way to the boards of directors. In IDC’s recent Future Enterprise Resiliency & Spending Survey in July 2021, almost half of US respondents reported that their “board of directors requested a presentation by our CIO/CISO” on ransomware. Globally, the figure is 30%. The elevation of the topic to boards of directors is a relatively recent phenomenon, but it’s more a reflection of a continually evolving cat-and-mouse struggle that’s been happening for decades.

Ransomware had its beginnings in 1989 with the AIDS trojan. Created by Joseph Popp, the malware was distributed by floppy disk at an AIDS conference. Post encryption, the malware asked users to mail $189 to “PC Cyborg Corporation” to obtain a repair tool. Popp claimed benevolence as he promised to donate the profits from the malware to fund AIDS research. Although there were several design flaws to the malware, the concept of encrypting files and extorting users was born. The evolution of ransomware from Popp’s nuisance to a debilitant of organizations has been the result of continuing improvements on two primary vectors: targeting and technical innovations.

The distribution of malware via floppy disk was effective. Gpcode leveraged this distribution method in 2006 with some success, but the approach is self-limiting. The distribution methodology has the natural physical inhibitor of requiring a user to obtain the disk and insert it in a drive, slowing distribution.

In 2013, CryptoLocker found email exponentially increasing distribution velocity by removing the physical distribution constraints. Thus, the application of a digital transformation principle to ransomware was born.

In 2013, CryptoLocker found email exponentially increasing distribution velocity by removing the physical distribution constraints. Thus, the application of a digital transformation principle to ransomware was born.

The distribution and targeting innovations were far from over. The leveraging of botnets soon followed. In 2015 and 2016, names like Chimera, SamSam, BitPaymer, Wannacry, and NotPetya furthered the digital transformation principle application, leading to targeting known and unknown vulnerabilities in our IT infrastructure.

As our defenses got better, so did the attackers, as spear phishing became the approach of Ryuk, FIN6, and Trickbot. In 2021, the state of the art is the supply chain attack, as malicious groups such as REvil leverage the trusted software of others in supply chain attacks to surreptitiously distribute ransomware on a large scale.

The pace of innovation for the targeting and distribution of ransomware has been equaled by the technical innovation of the malware itself. Early improvements of stronger encryption were key to ransomware effectiveness. Then cryptocurrency enabled anonymous monetization. Effective encryption and anonymous monetization became the foundation of the ransomware value proposition.

In 2015, the innovation moved from the ransomware to the ransomware target. Some ransomware victims unfortunately discovered that if the end-user devices connected to network stores at the point of ransomware encryption, those network stores would also accidentally be encrypted. Cybermiscreants consequently discovered that the willingness of the victim to pay the ransom, and the amount that the victim was willing to pay, were correlated to what was encrypted. Thus, ransomware attackers increasingly leveraged lateral movement, credential harvesting, and privilege escalation to find high-value targets.

By 2018, the focus turned to the active role of the attacker. Tools to enable attackers became the point of emphasis. Ransomware as a service, evasion, backdoors, and identity theft enabled attackers to better traverse networks and find organizations' most valued systems and IP. Consequently, ransom amounts moved from the tens of thousands of dollars to hundreds of thousands of dollars.

Today, the vilest attribute of ransomware may have nothing to do with the actual "ransomware" at all, as the core value proposition continues to evolve. Clearly, organizations are willing to pay so they can regain access to their data. What if a cyberattacker first exfiltrates the data, then encrypts? The threat of publicly exposing the data through double extortion not only increases the likelihood of ransomware payment but enables attackers to realize higher ransoms. If customer data happens to be exfiltrated, attackers have extorted the victim organization's customer as well with the threat of data being exposed, giving birth to multi-faceted extortion. The resulting ransom size continues to grow from hundreds of thousands of dollars to millions.

As IDC describes the evolution of ransomware, it's important to note that our use of terms "innovation," "improvement," and "value proposition," which are normally reserved to celebrate achievement, is clearly not complimentary. Nothing can be further from the truth. The impact of ransomware has been devastating, resulting in the closure of businesses. Even the loss of human life can be attributed to it. The purpose here is to illuminate and create a healthy respect for ransomware and ransomware attackers, a sophisticated cadre of individuals who are highly motivated and armed with destructive tools.

Defending against this scourge requires equally sophisticated security professionals with an even more sophisticated set of tools. Organizations must successfully defend against ransomware attacks 100% of the time. Attackers can fail many times but have to succeed only once.

Software alone can't solve the problem

The security software market is estimated to generate $224 billion in revenue annually, but that's cold comfort to individuals and organizations that have suffered malware infections. According to a Cisco report 69% of organizations experienced some level of unsolicited cryptomining in 2020, and 50% of organizations encountered malware-related activity.

Willie Sutton was reputedly once asked why he robbed banks and responded, "Because that's where the money is." Cyber criminals are similarly motivated to seek out targets where they can reap the most damage or collect the biggest payouts.

After the Colonial Pipeline attack, the U.S. Department of Justice gained wide acclaim after it announced it was able to recover $2.3 million of the ransom payment. But that recovery barely puts a dent in the ill-gotten gains from this type of assault.

"Despite authorities' recent success in busting several ransomware gangs, this particular breed of malware has proven to be a hydra—cut off one head and several appear in its place—and all signs are that the coming decade will be no less problematic," Cybersecurity Ventures warned.

Security solutions such as antivirus software detect new attacks based on heuristic rules that distinguish malware from nonvirus code. Another widely used technique scans all files in computer memory to identify potential viruses. But cyberattackers are constantly tweaking code to avoid detection, and many swap tips and techniques to improve attacks or pinpoint weak defenses. Some even offer ransomware-as-a-service, which provides subscriptions to proven tools and techniques that allow even unsophisticated attackers to launch potent assaults.

Commonly deployed detection techniques like static signatures, static/behavioral "honey pot" files, and behavioral file I/O all have bypasses exploited by ransomware using delayed arbitrary starts, avoiding hidden folders, using multiple threads for faster execution, and using memory mapped I/O for file encryption.

Software-based endpoint detection and response (EDR) solutions are designed to help organizations find, contain, and remove threats quickly. But EDR solutions are typically reactive; enterprises need proactive security.

The built-in, hardware-based security features of today's Intel processors provide a more secure foundation with protection against attacks below the operating system, coupled with remote recovery capabilities. That in turn can help endpoint security solutions harness CPU telemetry and hardware acceleration to identify threats and detect anomalous activity.

Unfortunately, many enterprises continue to operate old technology that is more susceptible to attacks. A report by J. Gold Associates estimates that "at least 35% of enterprise endpoints deployed at the start of the pandemic were 'old tech' that were at least three generations behind the current offerings, and therefore much more likely to be a security risk."

> "The ROI on avoiding potential data breaches and hacks can easily justify the cost of upgrading equipment, without waiting for the typical 3-5 year refresh cycle."
>
> —J. Gold Associates report

Software security solutions strengthened with Intel hardware features

Intel vPro® Enterprise for Windows comes equipped with Intel® Hardware Shield to deliver built-in security below the OS, application, and virtualization layers, and provides advanced threat detection capabilities including Intel® Threat Detection Technology (TDT).

Intel TDT gives software security solution providers a real-time, hardware-based signal that makes detection more proactive. CPU-level, real-time telemetry enables Intel TDT to track encryption at the lowest level, while machine learning (ML) heuristics allow Intel TDT to single out ransomware from other encryption behavior.

Intel TDT detects ransomware and other threats that leave a microarchitectural footprint on the CPU and can be analyzed with telemetry from the performance monitoring unit (PMU). The Intel PMU sits beneath applications, the OS, and virtualization layers on the system and delivers a more accurate representation of active threats systemwide.

Intel CPUs come with an integrated graphics controller (GPU), and Intel TDT can be used to offload ML inference processing and security vendor workloads such as advanced memory scanning (AMS). Memory scanning techniques have been shown to be effective in identifying threats, but often go unused because of their performance overhead, but when certain real-time memory-scanning operations are migrated to the GPU, threat detection is enhanced without decreasing performance, impacting the user experience, or reducing battery life.

With the industry's first silicon-enabled AI threat detection[1], software security providers can accelerate performance-intensive AI security algorithms without impacting the CPU.

Intel is "unlocking capabilities in its system-on-a-chip offerings that fundamentally change the ability of security vendors to implement security," says IDC.

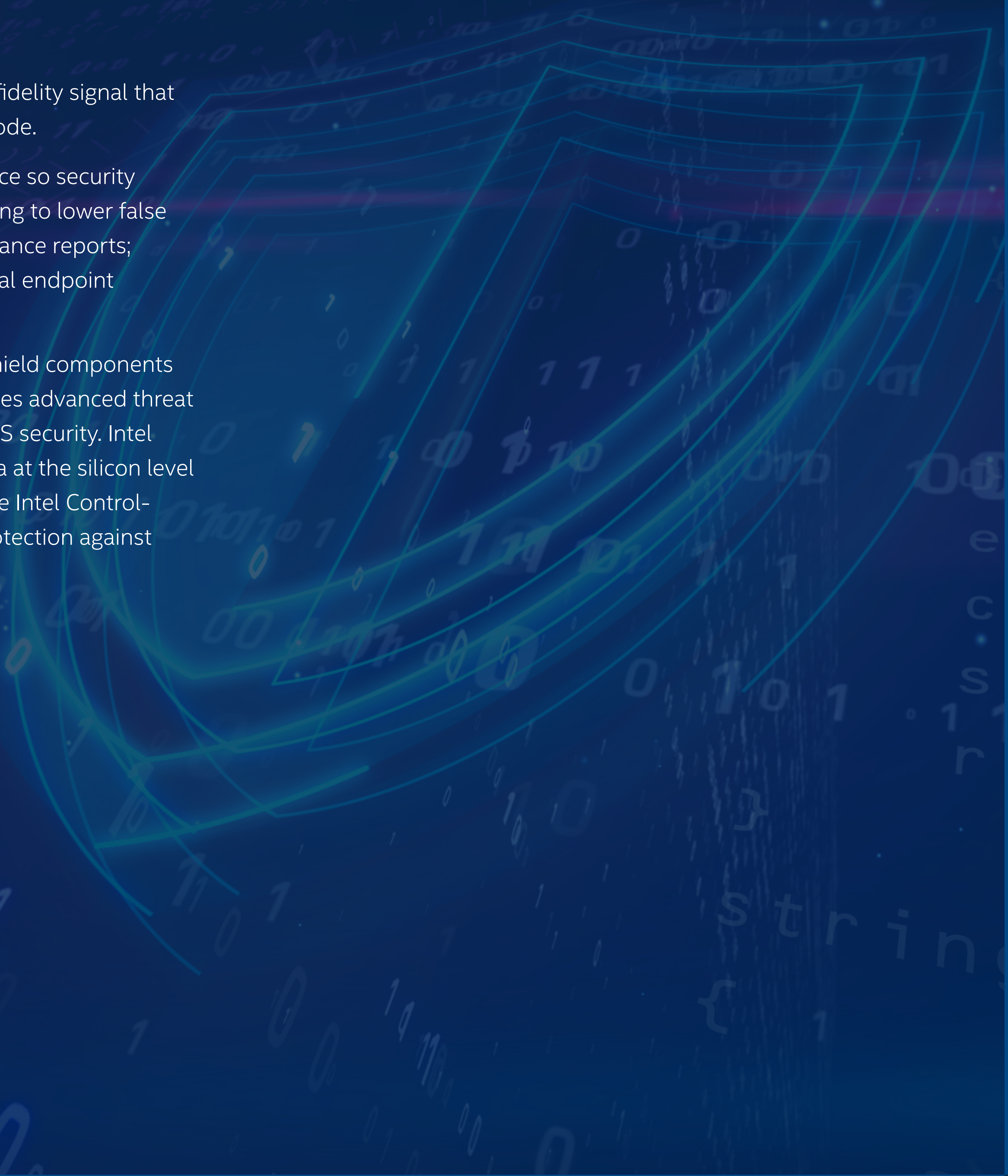
[1] The Intel vPro platform delivers the first and only silicon-enabled AI threat detection to help stop ransomware and cryptojacking attacks for Windows-based systems. Intel TDT Anomalous Behavior Detection (ABD) is a hardware-based control flow monitoring and anomaly detection solution able to monitor business apps for early indicators of compromise, leveraging the Intel CPU to build dynamic AI models of "good" application behavior. See www.intel.com/PerformanceIndex (platforms) for details. No product or component can be absolutely secure.

Real-time threat detection

When detecting threats in real-time, Intel TDT sends a high-fidelity signal that can trigger remediation workflows in the security vendor's code.

Intel TDT can parallelize multiple concurrent detectors at once so security vendors can run more scans—increasing efficacy while helping to lower false positives. Intel TDT issues no specialized efficacy or performance reports; rather, the data is seamlessly incorporated as a part of normal endpoint sensor reporting.

The Intel TDT technology works alongside Intel Hardware Shield components to provide integrated hardware-based protection that includes advanced threat detection, application and data protection, and below-the-OS security. Intel Total Memory Encryption encrypts all memory-resident data at the silicon level to help protect data in memory from cold-boot attacks, while Intel Control-Flow Enforcement Technology provides hardware-based protection against multiple classes of control-flow attacks.



More agile and data-driven cyberdefenses

The best enterprise security solutions capture real-time data from myriad sources and use it to identify rapidly evolving threats. Platform telemetry is becoming one of the most valuable sources of such data. When combined with machine learning, memory scanning, and other hardware-enhanced capabilities, it can significantly increase protection of IT systems.

The raw data that Intel TDT analyzes helps identify targeted attacks including polymorphic malware and cryptomining in real-time with minimal end-user impact. Intel TDT enables developers to incorporate these capabilities to extend their own threat detection solutions and uses ML heuristics to monitor malware activity at the CPU level with minimal false positives. Security solution developers can leverage the Intel technology and tune configuration parameters for the optim balance of efficacy, false positives, and performance.

Intel 10th Gen and newer Intel Core processor-based PCs are out-of-the-box capable to leverage Intel TDT CPU behavior monitoring and threat detection in conjunction with security vendors that have integrated the capability into their endpoint protection software. Intel TDT is enabled by leading security vendors, including Microsoft Defender, SentinelOne Singularity, and Blackberry Optics, with more providers currently working to enable their solutions to take advantage of these new capabilities, and Intel has a roadmap of future detectors.

The continuing evolution of security threats requires extraordinary measures of protection. Intel has built a suite of technologies to execute a defense-in-depth strategy that recognizes every component—from software to silicon—must work in concert to help secure data and maintain device integrity.

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.
Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See Performance Index for configuration details. No product or component can be absolutely secure.
Your costs and results may vary.
Intel technologies may require enabled hardware, software or service activation. No product or component can be absolutely secure. Your costs and results may vary.

Click here to learn more about Intel TDT and how how Intel vPro Enterprise for Windows delivers the performance, security, manageability, and stability to help propel your business safely.