Endpoint Protection

Securing enterprise endpoints with comprehensive security technology infrastructure

Contents

Executive summary

The pandemic saw the fastest digital transition the world had ever experienced. It became apparent that companies adopting new technologies and embracing hybrid work models quickly were that ones that would remain resilient, or even thrive. However, allowing the flexibility to work from home also meant that companies would need to secure data on employees' laptops that are outside the firewalls of an enterprise.

With this, organizations have lost their ability to protect their data as there are various vulnerable endpoints., which lead to security risks, including expanding threat perimeters, cyber threats, critical data breaches, and revenue loss. IT departments are now in charge of averting this crisis, and they must achieve this by adopting a comprehensive modern security plan that can accommodate the complexity of today's corporate environment.

The Intel suit of security technologies provides the right solution to this problem, serving as an arsenal that can provide enterprises with a chance to guarantee safety to their users. And how does Intel's comprehensive security toolset deliver this?

The toolset comprises tech elements such as:

- Intel vPro® Platform
- Intel® Hardware Shield
- Intel® Threat Detection Technology
- Intel® Remote Secure Erase
- Intel® Active Management Technology

It is designed to holistically deliver built-in advanced security at every layer: the hardware, the firmware, and the operating system. This is achieved by establishing a trusted software architecture that prevents attackers from spoofing identity or hijacking the device for any malicious purpose. The next step is proper device monitoring and management to monitor the health and behavior of devices as well as detect any attempts at tampering with their integrity, achieving advanced security at each level of IT infrastructure.

Highlighting the above information, this paper explores the need to revolutionize IT workplace security and explains in detail how **Wipro's Live Workspace™ Secure360** powered by **Intel's comprehensive set of technologies**, serves as a solution to achieve this while elevating device security, thus achieving complete endpoint protection.

Modern workplace has evolved over time; workspaces no longer rely on the traditional 9 to 5 clock, and most employees prefer seamless and flexible work environments spread across geographical time zones. But along with the benefits, "the modern workplace" also brings with it complex security issues that go beyond the concern of just protecting the "perimeter" of any organization's infrastructure.

The need to revolutionize IT workplace security

The threat landscape has become more complex, and with enterprises adopting connected devices at an exponential rate, there is an evident increase in the attack surface. **As per the latest IBM Data Breach 2022, the global average total cost of a data breach is USD 4.35 Mn, representing a 17 year high. Additionally, it takes 277 days on average to identify & contain a breach.**

The above-stated figures point to the fact even though remote work is gaining approval and is being considered a modern approach for a virtual office, it still comes with weight of challenges related to privacy, security & business protection issues.

Rise in unmanaged endpoints: Growing undefined network perimeter with mobile-first, cloud-first strategy allowing users to access corporate resources from anywhere is among the most significant security vulnerabilities.

Obsolete and ineffective security policies and strategies: This is a result of lack of agility in redesigning and adopting regulatory frameworks and policies.

Limited data capturing capabilities: There is an urgent need for real-time data visibility for risk analysis, identification, and remediation.

Multiple protection and backup tools: Multiple security tools and integrations adding to the complexity of scaling and managing the environment with constant patch repairs, complex authentication processes and security protocols.

The above challenges & facts indicate that organizations need to undergo transformation in order to safeguard their endpoints & data.

Future outlook on workplace security

Even though many employees are beginning to return to the office, we see that hybrid working will be the norm. **As per a McKinsey's survey, around 90% of the organizations have embraced hybrid working models post pandemic.** With more employees opting for hybrid work model, the on-premise and on-network Windows PC management is being tested to its limits. Enterprises are struggling with even the basic day-to-day routine procedures such as deploying, configuring, patching machines or even supporting them where issues arise because devices are not connected to the on-premises network.

Given the proliferation of cybersecurity threats and numerous sources of vulnerability, there is a need for a solution that seamlessly solves the security challenges. This is where Intel's comprehensive security toolset comes in, bearing a solution that encompasses all the device security elements.

Secure360 powered by Intel for critical IT infrastructure

Connected devices, whether on- or off-site, have become critical to rapidly changing businesses. But as connected devices gain prominence in the modern business landscape so do cyber-attacks. Threats can easily move across the IT infrastructure using remote devices endpoints as direct routes into networks, clouds, and SaaS applications. Thus, with sophisticated threats focusing their targets on hardware infrastructure, the need for organizations to deploy security that defends every layer of infrastructure and application has become the need of the hour. This requires defense at each layer of infrastructure and application, ranging from hardware, network, cloud to firmware, virtual machines, etc.

> Hence, enterprises need a 360-degree approach to their security needs that can deliver unified endpoint management while ensuring adequate security compliances and patch updates.

Wipro's Live Workspace™ Secure360, a layered endpoint security management solution leveraging AI/ML, advanced analytics and automation, is a zero-trust based integrated platform ensuring detection, investigation, and remediation of threats through four key segments – Identity & Access Management, Information Protection, Vulnerability Management and Antivirus Management, all accelerated through Extended Detection & Response (XDR).

Furthermore, the solution ensures the implementation of a multi-layered endpoint security approach that enables healthy and compliant endpoint management along with restricted access from vulnerable devices. This is achieved leveraging Intel's extensive endpoint security ecosystem – **Intel® Active Management Technology, Intel® Hardware Shield, Intel® Threat Detection Technology, Intel® Remote Secure Erase, and Intel vPro® Platform.** Powered by the above stated capabilities, the solution delivers threat detection, prevention, vulnerability management, and real-time monitoring of attacks. These technologies, when combined, bring together the hardware and software elements for the endpoint device security, enabling organizations achieve a robust and responsive security posture.

Endpoint security enablers:

Intel vPro® Platform

Intel vPro® platform aims at providing enterprise-grade technologies through advanced security provisions, top-notch performance enablement for the endpoints. Equipped with features like Intel® Hardware Shield, control-flow enforcement technology, encryption capabilities and new hardware virtualization to better secure the OS. The new 12th Gen and 13th Gen Intel vPro® platform provides leading productivity and best performance along with a comprehensive platform security for all enterprises.

The platform combined with 12th Gen and 13th Gen Intel Core processors offers the most comprehensive security for businesses with:

Intel® Threat detection technology

As the only provider of hardware-based security capabilities, Intel's Threat Detection Technology enhances industry security software and delivers effective detection of threats. It brings together tools and techniques leveraging combination of signature-based detection, behavioral analysis, and machine learning for intrusion detection and prevention.

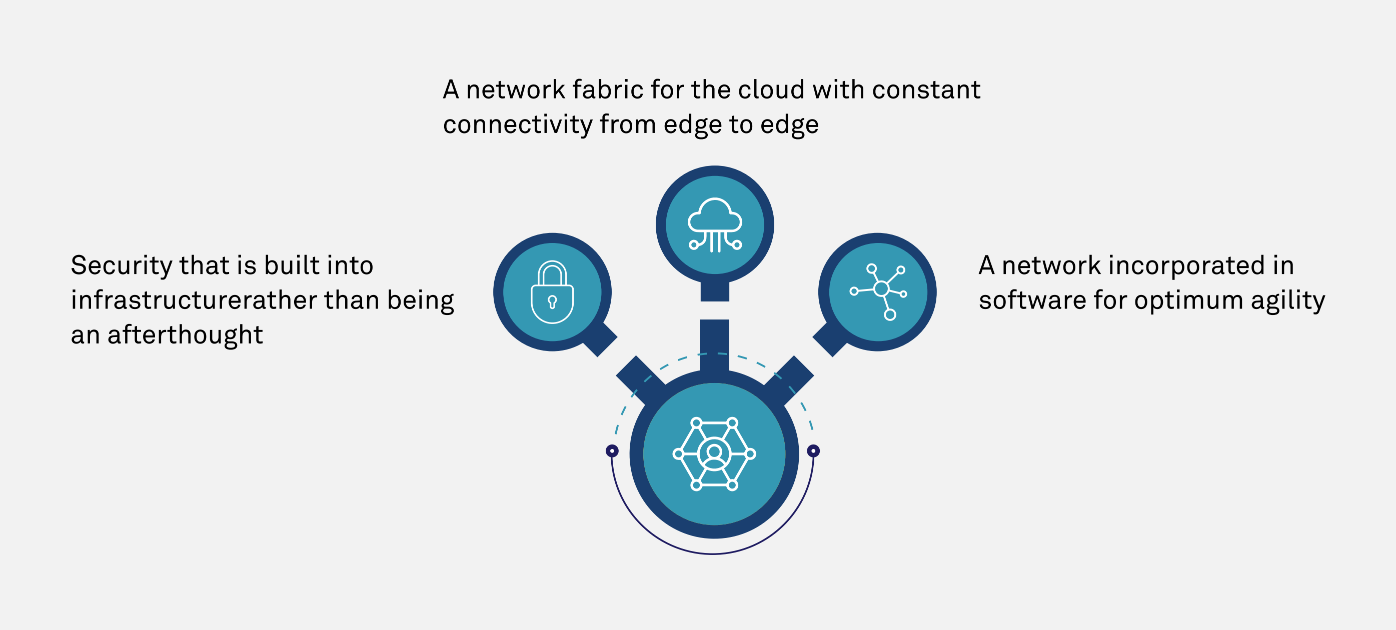
- Intel® TDT increases the effectiveness and speed at which the most recent attacks are discovered.
- Intel® TDT allows anomalous behavior detection and uses AI to profile "good app behavior" along with notifying for anomalies occurring to the endpoint security software.
- New silicon-based detection capabilities help in preventing malicious code invasions.

Intel® TDT is the first silicon-enabled AI threat detection to help stop ransomware and cryptojacking attacks as it executes on CPU microarchitecture. This enables threat detection ability to the new level with full-stack visibility that helps uncover malicious code that is cloaked in a Virtual Machine or in obfuscated binaries.

Chip-to-cloud

To fully utilize the solutions to defend your environment, it is critical to have complete visibility of all the devices in your organization, whether the devices are connected or not. This is where Chip-to-cloud technology helps, as it enables the creation of secure-by-design devices that are always connected to the cloud. By providing solutions to build a digital foundation for modern IT, it efficiently handles endpoint management challenges with intrinsic security. The said technology isolates software from hardware, helping in:

- Securing access to sensitive data, including encryption keys, user passwords, and other sensitive data behind a hardware barrier.
- Preventing malware and blocking attackers from accessing or tampering with that data during the boot process.
- Enables businesses to easily distribute and manage any software on any device, anywhere.


A network fabric for the cloud with constant connectivity from edge to edge
Security that is built into infrastructurerather than being an afterthought
A network incorporated in software for optimum agility

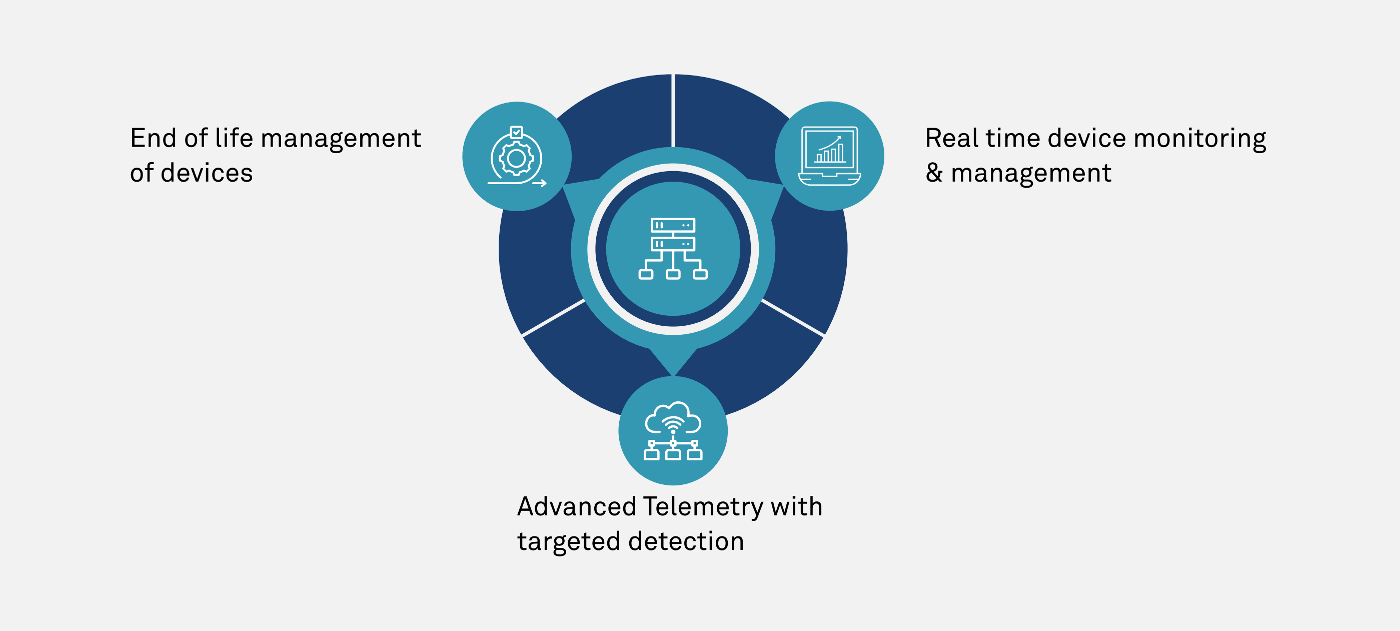
Description: Capabilities achieved via chip-to-cloud technology

With this, businesses can secure their application infrastructure regardless of where the application resides, by embracing cloud connectivity and unifying branch and edge environments across the entire enterprise. Furthermore, this will enable organizations to have a cloud-native, simplified activation experience, as well as granting admins access to UEM consoles to view device information, relevant device group details, and deploy platform configurations.

These capabilities must be complemented by a wide array of reliable software and enterprise hardware solutions.

> It must further enable remote configuration, maintenance, and provide access to useful insights such as device information, device group details, and successfully deployed platform configurations.

With this direct connection to endpoints at the hardware layer, remote management will be extended to Intel® Active Management Technology enabled devices, including devices that are powered-off or having operating systems that are not functioning correctly.


End of life management of devices
Real time device monitoring & management
Advanced Telemetry with targeted detection

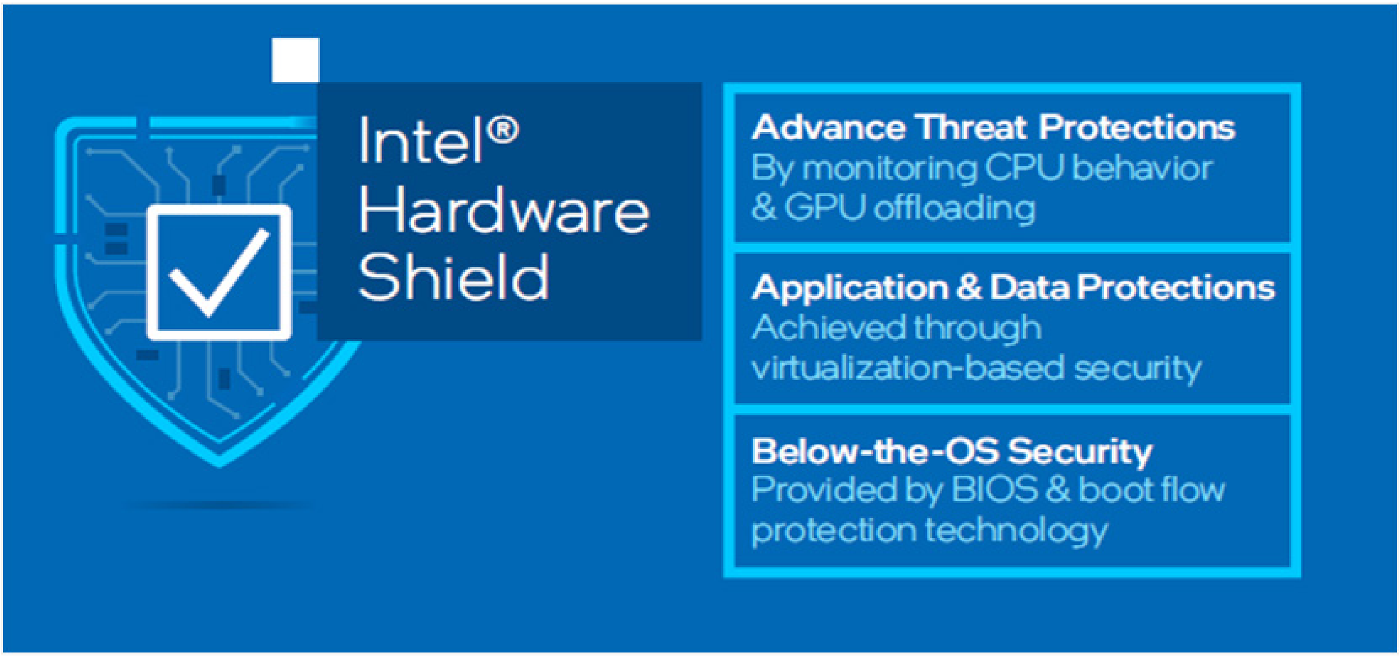
Description: Enhancing the Security Posture of Enterprises through Chip-to-Cloud Technology Capabilities

With Drop Ship Provisioning, IT administrators can remotely reset PCs, making PC recovery simpler. Additionally, thanks to cloud-to-chip technology, IT administrators may perform remote maintenance on devices with full keyboard, video, and mouse access, even without a functional operating system.

The solution also brings in **Hardware Manageability (Out-Of-Band)** for managing users' different work schedules and compliance requirements. Leveraging Intel® AMT, it can remotely act on a threat vulnerability without disturbing the user. Because of the cloud-native management features, patching is enabled without the use of a VPN, leading to enhanced device security.

Additionally, with **advanced telemetry capabilities, it utilizes** the dual technologies of machine learning and hardware telemetry to ultimately help businesses recognize exploits evading software-only anti-malware solutions. This enhances malware detection by adding a very efficient, low-maintenance tool that does not require intrusive scanning methods or signature databases.

Intel® Hardware shield


Intel® Hardware Shield
Advance Threat Protections
By monitoring CPU behavior & GPU offloading
Application & Data Protections
Achieved through virtualization-based security
Below-the-OS Security
Provided by BIOS & boot flow protection technology

Complementing this Chip-to-cloud technology is the **Intel® Hardware Shield**, which specializes in driving below the OS security. It comprises of hardware-based technologies to provide a trusted execution atmosphere and helps protect the BIOS firmware and the main memory starting at boot-up. Thus, this technology offers enterprises with built-in security features to help detect, protect, and recover from endpoint attacks in an increasingly challenging threat environment. As security threats continue to evolve and attack lower levels within a system's resources, so does Intel's hardware shield, delivering hardware enhanced, built-in protection, ultimately denying attackers access to modify or manipulate the hardware and firmware.

Intel® Remote secure erase

End of life management is a sensitive practice that typically requires IT possession of the devices. While existing solutions offer remote device reset and wipe, data can persist on the drives if IT does not have hardware access. Serving as a response to such vulnerabilities, **Intel® Remote Secure Erase** (available with supported SSDs) and Wipro's Live Workspace™ Secure360 with Vulnerability Management capabilities lower the possibility of data misuse even for devices mounted in inconvenient locations, such as industrial PCs operating in dangerous environments, and retail point-of-sale systems, etc.

Wipro and Intel collaboration to deliver robust security solutions

Intel and Wipro share a 360-degree strategic partnership that focuses on co-innovation, joint engineering capabilities to deliver NextGen Digital Workplace solutions that drive shared value for our customers. Through co-authored POVs, whitepapers and participation in round table discussions, Intel and Wipro have been able to create an environment of incubating new business opportunities. The robust partnership has taken great strides in building joint value propositions and solution development to delight employees with latest technologies and boost their productivity, enhancing workplace security to unlock the full potential. Through Wipro Live WorkspaceTM Secure360, leveraging Intel's security expertise, we have been able to provide enterprises with smart security solutions to easily manage, secure, and monitor their entire fleet of devices ensuring end-to-end security and compliance.

Further, Wipro is focused on utilizing its strong partnership with Intel to create an efficient endpoint security model. To deliver distinctive, contextualized employee experiences with the highest level of security and flexibility.

Wipro and Intel believe that security is not a one-time event; it's a continuous process. This strategic partnership is committed to significantly accelerating businesses on their security journey while upholding all security standards and best practices.

What's next for endpoint device security

There is a need to understand that the profit-before-security outlook won't work now. Leaving endpoints vulnerable to attacks is something that organizations can't afford, which is precisely why many tech giants around the world are investing billions into this capability. For instance, Microsoft announced Windows 11 to boost security baselines with new hardware security requirements supported via Intel's platform technologies, helping to proactively secure businesses from zero-day exploits. Devising processor-based security solutions is vital for staying diligent against ever increasing cyber-threats, and here at Wipro, we too are exploiting the potential of chip-to-cloud technology to enhance the security capabilities of the hardware. Wipro understands the need for a security in the workplace and looks at security and connectivity in an integrated manner. So, it has invested in a zero-trust based, SASE-led workplace integrated proposition in its portfolio with Wipro Live Workspace™ Secure360. Further, Wipro is continuously improving on evolving its Live Workspace™ security portfolio to include Intel's next-gen computing capabilities, including out-of-bandremote management, secure sharing, PP-based device management, XDR & SIEM services and threat intelligence.

Great periods of innovation and change often arise from moments of crisis. Building on this principle, Wipro understands that addressing these security risks will be crucial to the success of the modern hybrid workplace. To do so, a new endpoint security strategy will be required: one that is based on zero trust principles and created from the hardware up. At Wipro, we are prepared to deliver this strategy with precision.

Authors

Sidharth Mukherjee,
Global Practice Head,
Digital Workplace Services, Wipro Ltd

Sanjay Aghara,
System Software Architect, Intel

Ambitions Realized.

Wipro Limited
Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading technology services and consulting company focused on building innovative solutions that address clients' most complex digital transformation needs. Leveraging our holistic portfolio of capabilities in consulting, design, engineering, and operations, we help clients realize their boldest ambitions and build future-ready, sustainable businesses. With over 250,000 employees and business partners across 66 countries, we deliver on the promise of helping our customers, colleagues, and communities thrive in an ever-changing world.

For more information,
please write to us at **info@wipro.com**