Solution Brief

Enhance End Point Protection and Simplify Security Management with bytesatwork and Intel

bytesatwork

contact@manage4all.com

+49 231 860233-0

As the business world transitions into hybrid and remote models, cyberattacks are becoming increasingly more sophisticated. For organizations with remote locations and workforces, protecting devices and IT assets from cyberthreats is a key challenge, particularly for small to mid-size businesses (SMBs) with finite resources and limits on capital expenditures.

Without the right security features, detecting and mitigating threats to your endpoints throughout the device life cycle can be time-consuming and costly—and it can ultimately weaken industry competitiveness. Today's SMBs require flexible, customized, cost-efficient security management solutions that allow their end-users to do business safely from anywhere, anytime.

bytesatwork and Intel help you protect your fleet of computing devices by supplying you with the tools for remote, intelligent and automated security management of your hardware, software, apps and data.

bytesatwork's device life cycle management solutions, myCloudCenter and manage4ALL, enable IT teams to support, service and secure end-devices remotely. Their seamless integration with Windows-based Intel vPro® platforms delivers business-class performance and hardware-based security to help them achieve greater IT visibility of potential cyberthreats by leveraging the Intel hardware security features built into the endpoints.

The bytesatwork Solution

myCloudCenter and manage4ALL comprise an easy-to-use, single software solution that enables SMBs to manage the full lifecycle of disparate devices easily and cost effectively.

myCloudCenter

myCloudCenter enables IT teams to choose, configure and order the devices, software and services they need from a virtual, self-service portal. This process can be performed manually, or it can be automated by establishing predetermined settings within the portal. IT teams can then choose where to ship devices, whether it's to company locations or to remote employees' home offices. The solution saves SMBs time and money by providing an all-in-one location to acquire devices that are preconfigured and customized upon receipt with productivity and security applications, as well as value-added services that are ready to meet consumer expectations and demands.

manage4ALL

Once devices are ready for onboarding, the manage4ALL remote management and monitoring solution allows for zero-touch installation, roll out and provisioning, which enables IT teams to provide remote support, security updates and system upgrades—and to power up or power down devices during off-peak hours to save energy. Most manageability tasks can be completed manually or be pre-configured for automated delivery. The solution empowers IT teams to achieve remote visibility across the whole fleet and maintain control of management and security functions to improve end-user productivity, as well as streamline IT workflows with greater speed, less effort and more control—so SMBs can remain focused on growth and profitability.

Intel® Threat Detection Technology Augments bytesatwork's manage4ALL solution

On the Intel vPro platform, Intel® Threat Detection Technology (Intel TDT) operates seamlessly with manage4ALL. The Intel vPro platform augments manage4ALL with security capabilities rooted in the hardware that helps to detect cyber-attacks as they move down the compute stack.

Augmentation

Intel TDT provides an augmentation for partner platforms to increase detection efficacy, lower false positive alerts, expand visibility to catch advanced evasion techniques, and boost the overall security performance of your endpoints. Intel TDT is not a standalone product but provides the source code that is integrated into ISV partner software platforms to enable these CPU-assisted capabilities.

Hardware-Enhanced Capabilities

manage4ALL leverages unique CPU telemetry from Intel TDT to help detect the most advanced ransomware attacks and unauthorized cryptojacking software—whether they run as a native app, within the browser, or as a virtual machine— across all types of workloads executing on Windows operating systems. Intel TDT helps reduce impacts to the end-user's compute experience with performance offload from the CPU to the Intel integrated GPU.

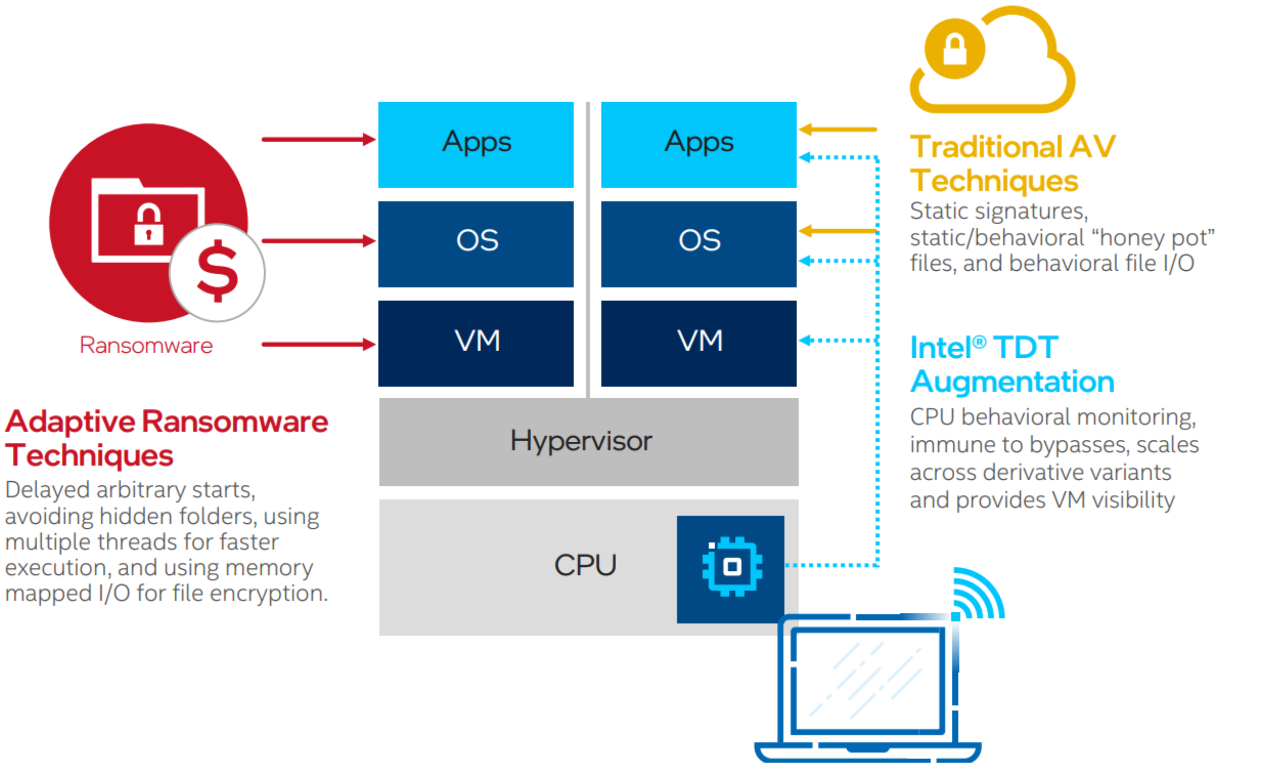
Intel TDT enables manage4ALL to go beyond signature and file-based techniques, equipping your endpoints with hardware-enhanced capabilities to identify polymorphic malware, file-less scripts, and other targeted attacks with minimal end-user impact.

Protection After System Infiltration

Even after ransomware has infiltrated a system, the Intel vPro platform empowers manage4ALL to collect additional context on Intel TDT-signaled threats to enable remediation with patches, segmentation of machines using perimeter network defenses, or restriction of lateral movement through hardware-enforced isolation of virtualized containers.

Recovery

Intel TDT dispatches early detection signals to aid with better ransomware analysis-based recovery. manage4ALL leverages Intel vPro platform capabilities to manage OS independent hardware manageability over WiFi.


Ransomware
Apps
Apps
OS
OS
VM
VM
Hypervisor
CPU
Traditional AV Techniques
Static signatures, static/behavioral "honey pot" files, and behavioral file I/O
Intel® TDT Augmentation
CPU behavioral monitoring, immune to bypasses, scales across derivative variants and provides VM visibility
Adaptive Ransomware Techniques
Delayed arbitrary starts, avoiding hidden folders, using multiple threads for faster execution, and using memory mapped I/O for file encryption.

Minimized Security Complexity for Enhanced Manageability

Complex interconnected solutions are now ubiquitous in the modern global information environment, and software-level security manageability can be challenging for SMBs, as IT teams are required to perform deskside visits for OS problems and be proficient in multiple solutions to manage security throughout the device lifecycle.

But integrated with Intel TDT, manage4ALL automates the remote security management of your endpoints, essentially creating self-protecting devices. Utilizing the capabilities of the Intel vPro platform, manage4ALL can execute assessment, diagnosis, stabilization and recovery functions at the software and hardware level, allowing it to intervene in the BIOS and access devices without a functioning operating system—anytime, all the time—through only one working device in network.

Emergency Plan Execution

manage4ALL receives the notification of compromise from Intel TDT and automatically executes a defined emergency response plan to minimize damage, protect your data, and help your organization recover from the incident as quickly as possible.

Isolating and Reboot

manage4ALL automatically isolates the potentially corrupted device—and possibly other devices, depending on the threat—and then boots for scanning and cleaning.

Scan and Clean

With existing Intel vPro platform capabilities, manage4ALL boots into a modified OS via storage redirection from its gateway to remove malware or other viruses lurking on your system.

Reactivation

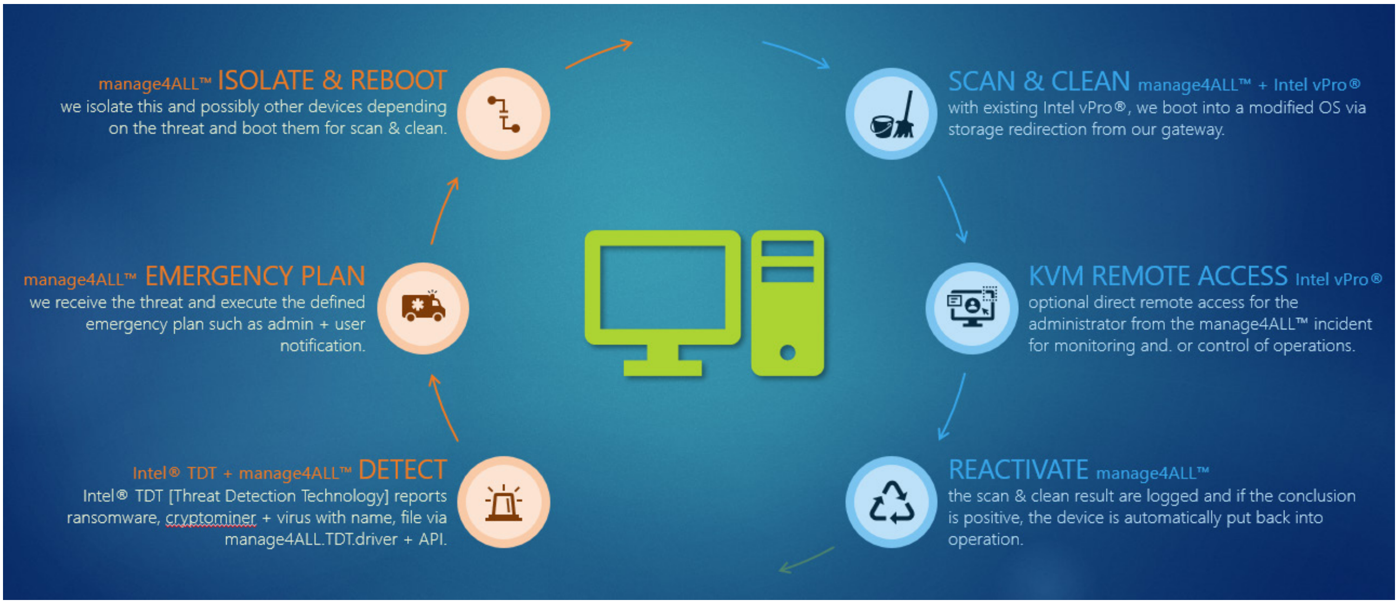
The scan and clean results are logged and—if the conclusion is positive—devices are then automatically restored to full operation. This gives IT teams the advantage of avoiding manual recovery, which cannot be completed without a functioning OS, unless back-up cloud-connectivity is available.

Security Manageability Challenges

- ☒ Workflow disruption
- ☒ Required proficiency in multiple solutions
- ☒ Deskside visits
- ☒ Consistent visibility and continuity between device lifecycle stages

Security Manageability Solutions

- ☑ Reduce workflow disruption through automated threat detection, emergency plan execution, and device reactivation
- ☑ Eliminate the need for diverse solutions and remove silos between IT teams by enabling them to use the same support, service and security tools
- ☑ Virtualize deskside visits by managing security remotely throughout the device life cycle and automating security protocols to occur during off hours
- ☑ The Intel security features built into your endpoints can be managed remotely and preconfigured for automated threat detection and mitigation, enabling your end-devices to be virtually self-protecting



manage4ALL™ ISOLATE & REBOOT
we isolate this and possibly other devices depending on the threat and boot them for scan & clean.

manage4ALL™ EMERGENCY PLAN
we receive the threat and execute the defined emergency plan such as admin + user notification.

Intel® TDT + manage4ALL™ DETECT
Intel® TDT [Threat Detection Technology] reports ransomware, cryptominer + virus with name, file via manage4ALL.TDT.driver + API.

SCAN & CLEAN manage4ALL™ + Intel vPro®
with existing Intel vPro®, we boot into a modified OS via storage redirection from our gateway.

KVM REMOTE ACCESS Intel vPro®
optional direct remote access for the administrator from the manage4ALL™ incident for monitoring and. or control of operations.

REACTIVATE manage4ALL™
the scan & clean result are logged and if the conclusion is positive, the device is automatically put back into operation.

bytesatwork + Intel: Better Together

The Intel vPro platform enables manage4ALL to access and manage end-devices, while giving SMBs greater IT visibility of potential cyberthreats for faster detection and mitigation response.

Intel vPro® Enterprise | Intel vPro® Essentials

Intel vPro® Essentials

For a growing small business today, consumer devices aren't enough. Trusted business-class PCs with power, flexibility, and built-in security can keep any small business productive—and help protect sensitive data. And with the management options of Intel vPro Essentials, the technology can scale alongside the business as it matures—even for companies without a dedicated IT team.

Intel vPro® Enterprise

Devices built on Intel vPro Enterprise are built for business—with optimized performance for improved productivity, hardware-based features to boost security, and tools to make fleet management easier. Intel vPro Enterprise provides more for businesses of any size with advanced out-of-the-box capabilities and support for multiple operating systems, so organizations can thrive in a rapidly changing digital world.

Why bytesatwork with Intel Works for SMBs

Leverage Hardware Security Already in Your Fleet

manage4ALL utilizes the powerful capabilities on the Intel vPro platform and leverages Intel TDT security features to provide you with the infrastructure to manage and automate security remotely throughout the device life cycle. This unique integration of software and hardware gives IT teams visibility across the whole fleet to enable more agile threat detection and mitigation. These solutions also reduce or eliminate the need for deskside visits, decrease IT workloads, and streamline device life cycle management.

Acquire More Flexibility

Whether you're a small or mid-size business, bytesatwork and Intel can help simplify security and manageability so IT teams can execute detection and response procedures at the endpoint. Even in the event of a system crash, a technician can remotely respond to advanced threats, retaining end-user productivity.

Optimized for Intel

The integration of bytesatwork with the Intel vPro platform gives manage4ALL seamless access to Intel TDT, which enables the solution to carry out automated threat detection and mitigation, so IT teams can focus on business-critical operations instead of on time-consuming security management.

Learn More

Take the next step in protecting your business by leveraging bytesatwork's easy-to-use, cost-effective device life cycle management tools integrated with advanced Intel vPro platform security capabilities to manage and secure your entire fleet more efficiently—from anywhere, anytime.

Visit www.bytesatwork.de to get more information about myCloudCenter and manage4ALL.

Visit Intel.com/tdt to learn more about Intel Threat Detection Technology

Notices & Disclaimers

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary. Intel Corporation, Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

Intel performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex