WHITE PAPER

TREND MICRO AND MICROSOFT: A POWERFUL SECURITY PARTNERSHIP

A relationship that stretches back decades has helped two partners boost the cyberdefense their products offer.

EXECUTIVE SUMMARY

Almost every organization around the world depends on Microsoft's wide range of products. From operating systems and office productivity software, to Windows servers and Surface tablets, Microsoft products power the modern enterprise. As more organizations move to the cloud, Microsoft's Azure cloud computing platform and Office 365 cloud productivity solution present even more options for Microsoft adoption. Microsoft has made the security of its products a top priority, but the ubiquitous nature of its software makes it a target, leading enterprise security teams to be justifiably concerned about maintaining the security of their Microsoft implementations. Trend Micro's long relationship with Microsoft has led to the development of numerous products that address these concerns.

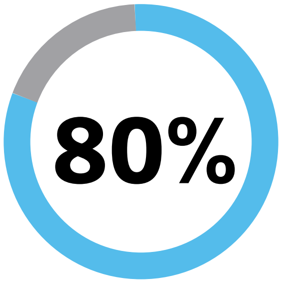
Trend Micro provides enterprise IT teams with a wide range of solutions that are specifically developed to enhance the security of Microsoft platforms and products. Trend Micro's products range from traditional anti-malware solutions to cloud-centric intrusion detection and prevention packages. IT professionals adopting Trend Micro solutions benefit from the company's long-standing partnership with Microsoft.

The Long Relationship Between Trend Micro and Microsoft

Trend Micro and Microsoft have a rich history of working together that dates back more than two decades. The strategic partnership between them means that both organizations share information and strategies as well as a common goal: providing customers with a safe and secure computing experience that leverages state-of-the-art security technology to protect valuable information and technology resources.

Microsoft is a global leader in providing operating systems for servers and desktops, collaboration software for teams and enterprises, and cloud-based solutions that empower a mobile workforce. Trend Micro is the global leader in the server security market, possessing more than 30 percent of market share, according to the analysis firm IDC. The market-leading positions of both companies make them natural strategic partners when it comes to enterprise information security. Together, the two firms collaboratively develop security solutions that reach deep into Microsoft's products and provide unparalleled security.

Microsoft's global team of security professionals invests a tremendous amount of time, talent and resources in the development of innovative security technology across the company's product lines. This team consistently deploys security tools that are native to Microsoft platforms and provide customers with deeper capabilities to proactively secure systems, detect intrusion attempts and remediate security vulnerabilities. Trend Micro's products don't replace these solutions; they enhance them to provide even greater value. Enterprises that adopt Microsoft products begin with a tremendous security foundation and may then achieve even greater security for systems and data by implementing Trend Micro's sophisticated solutions. Trend Micro products leverage and build on Microsoft technology to provide protection against advanced threats and prevent data loss.



The percentage of Fortune 500 companies that use the Microsoft Azure platform[1]

Trend Micro and Microsoft Azure

Many technology professionals consider cloud computing the most significant technology advancement of the past decade. Organizations are racing to adopt Infrastructure as a Service computing approaches that create flexible, agile computing platforms built on basic computing, storage and networking resources offered by cloud providers. Microsoft's Azure platform is one of the market leaders in this space and offers special appeal to organizations already leveraging Microsoft operating systems and other platforms in their on-premises data centers. As customers consider moving computing resources to the cloud, security is a primary consideration. Customers must feel confident that their data will be at least as secure in the cloud as it is in their on-premises environments.

Trend Micro has partnered with Microsoft from the very first days of the Azure platform to provide customers with the confidence they need to shift workloads to the cloud. The Trend Micro Deep Security platform integrates directly with the Azure Security Center to provide administrators with a comprehensive management approach to monitoring their Azure deployments that not only provides live monitoring of workloads, but also offers security remediation recommendations designed to bolster cloud security. This level of integration shows the deep partnership that Microsoft and Trend Micro have when approaching cloud security. Deep Security also embraces a cloud-centric pricing model, allowing enterprises to deploy advanced security technology on a pay-as-you-go basis with no long-term commitment. Organizations that choose to purchase Deep Security as an annual subscription receive a significant discount.

Deep Security is optimized for Microsoft Azure, allowing administrators to deploy the Deep Security agent directly from the Azure console. Once installed, the agent provides comprehensive security coverage for Azure virtual machines.

Deep Security in Action

Square Enix, a leading online gaming company, relies on Microsoft Azure to provide a rapidly scalable computing environment that supports more than a million users worldwide. Azure provides Square Enix with the on-demand access to computing resources necessary to support its global base of iOS and Android users. The popularity of Square Enix's Rise of Mana online role-playing video game makes it an attractive target for attackers, and security is a paramount concern.

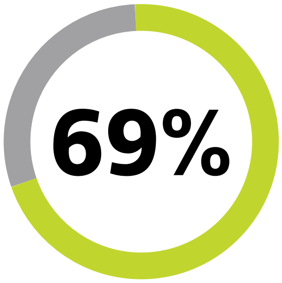
Square Enix relies on Trend Micro's Deep Security platform to provide advanced threat protection for its cloud computing environment. The company uses the platform's Deep Security Manager to maintain the security of the gaming platform and customer personal information through advanced intrusion detection and prevention, anti-malware protection, firewall services and other sophisticated security controls. Deep Security's native Azure integration allows it to rapidly scale up and down without any downtime as demand rises and falls for Square Enix's online games. Deep Security provides Square Enix with comprehensive security without slowing down the business.

The company also updates Rise of Mana frequently, which makes performing comprehensive security checks on the software impossible. Deep Security updates information on the kind of attacks the game faces and their timing, allowing the company to discern trends and pre-emptively deal with attacks.

Read the full success story here.

[1] **SOURCE:** Microsoft

Deep Security provides intrusion prevention services, along with advanced anti-malware protection. It continuously scans servers and applications to detect complex attacks and reduces the exposure of cloud systems by ensuring that servers communicate only in an expected manner. The platform's virtual patching technology reacts promptly to new threats, instantly protecting Azure instances against both zero-day and known vulnerabilities such as Shellshock and Heartbleed. It detects and alerts IT administrators of suspicious or malicious activity to proactively trigger preventive actions. Finally, Deep Security leverages Trend Micro's web reputation capabilities by preventing sessions being initiated with known malicious or harmful domains.



The percentage of organizations that use cloud-based cybersecurity services[2]

Accelerate PCI compliance and simplify security management across physical, virtual and cloud environments with a single tool, Trend Micro Deep Security. Deep Security addresses intrusion detection and prevention; anti-malware; file system integrity monitoring; security logs; and firewall requirements for PCI workloads; and shields out-of-support platform or zero-day vulnerabilities.

Trend Micro and Office 365

The Office 365 productivity suite provides users with access to enterprise email, calendaring and collaboration in the cloud.

Organizations migrating to Office 365 free themselves of the burden of maintaining on-premises email servers and gain the advantage of immediate upgrades as Microsoft releases new features. Trend Micro's Cloud App Security product integrates directly with Office 365 to provide added assurance to securely work with sensitive information in the cloud.

After only six months on the market, Cloud App Security detected and blocked more than 500,000 threats destined for customer inboxes. Cloud App Security provides this protection by continuously scanning the contents of email messages, OneDrive and SharePoint content, including Office 365 documents, for the presence of advanced malware. The product leverages sandbox-based malware analysis, document exploit detection and web reputation scoring to provide customers with the full benefit of Trend Micro's 15 years of experience securing Microsoft Exchange and SharePoint environments.

Cloud App Security is the only Office 365 security add-on that leverages direct cloud-to-cloud integration to provide enhancements to the built-in security features of Office 365. Unlike products that simply redirect messages through a hosted service, Cloud App Security accesses the Microsoft application programming interface to reach directly into Office 365 and provide an integrated approach to enterprise security. This direct integration offers a significant advantage over other products because it allows Trend Micro to protect *every* email message sent or received within an enterprise, even those sent between two internal users. Products that use the redirect option never see those internal messages because they are delivered directly to inboxes within the Office 365 environment.

Organizations handling sensitive and regulated information also benefit from the data loss prevention features available within Cloud App Security. The product includes more than 200 DLP templates that allow organizations to immediately begin scanning email messages, OneDrive documents and SharePoint content for the presence of unsecured compliance-related information. Administrators can choose to automatically quarantine file sharing content for further analysis, reducing the likelihood of a security breach.

Trend Micro and Windows Server 2003

In July 2015, Microsoft ended support for the 12-year-old Windows Server 2003 operating system, leaving many organizations in situations where mission requirements forced them to continue using an out-of-support operating system. With the end of support, Microsoft no longer issues Windows Server 2003 security updates, even when security researchers or hackers discover critical vulnerabilities in the product. At the same time, organizations using legacy equipment or software that depends on a Server 2003 environment must continue to run these systems in the face of serious security issues. That's an untenable situation for IT leaders who find themselves

Trend Micro Secures More Than the Cloud

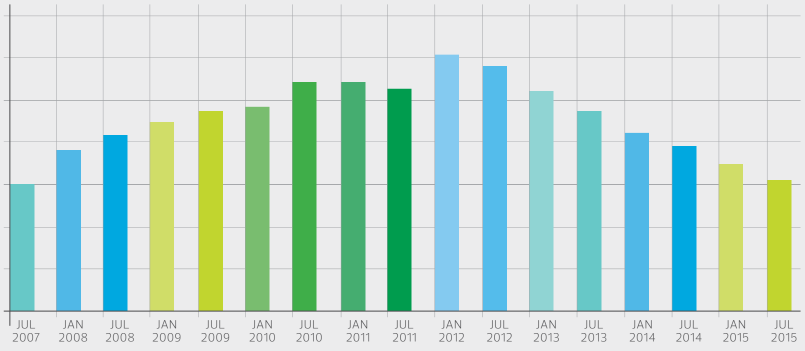
Organizations that continue to operate on-premises messaging and collaboration platforms may also benefit from the Trend Micro—Microsoft partnership. Trend Micro remains committed to providing security solutions across the full range of Microsoft product deployment options, including on-premises Exchange and SharePoint environments.

Exchange users benefit from Trend Micro's ScanMail Suite for Microsoft Exchange. ScanMail offers enterprise security protection integrated directly into Exchange servers. It provides protection against advanced persistent threats, malicious URLs and highly targeted attacks, along with traditional spam and malware filters.

SharePoint environments are attractive targets for attackers. Typically found on corporate intranets, users know and trust their SharePoint environments, making them more susceptible to attacks waged on that platform. Trend Micro PortalProtect integrates directly with SharePoint to provide a secure collaboration experience, free from malware and malicious URLs. PortalProtect also offers data loss prevention and content-filtering services that further enhance SharePoint security.

[2] **SOURCE:** PwC, "The Global State of Information Security Survey 2016," October 2015

Number of web-facing servers still running Windows Server 2003



SOURCE: Netcraft

forced to choose between security and meeting the needs of the organization.

Windows Server 2003 deployments are a large-scale problem. Two months after the end of Microsoft support, a Netcraft analysis found that more than 600,000 servers running Windows Server 2003 were still directly accessible on the Internet. That data includes only servers reachable from external networks and is likely only the tip of the iceberg, considering that most servers reside behind enterprise firewalls. It's possible that millions of servers still run this unsupported operating system, at the risk of security breaches and compliance violations.

Trend Micro Deep Security offers a compromise solution for enterprises unwilling or unable to upgrade their Windows Server 2003 systems to a more recent operating system. While they prepare to eventually upgrade or decommission those servers, Deep Security uses intrusion detection and prevention functionality to shield devices from emerging attacks. The virtual patching capabilities found in Deep Security watch for attempts to exploit unpatched vulnerabilities and block them before they can result in a successful attack. Deep Security extends the life of legacy systems by adding current and reliable security protection that picks up where Microsoft support left off.

CDW: A Security Partner That Gets IT

CDW is uniquely positioned to help enterprises leverage the Trend Micro—Microsoft partnership. As a long-standing partner with both companies, CDW works closely with the Trend Micro and Microsoft security teams to provide enhanced security services.

CDW takes a comprehensive approach to identifying and meeting the needs of every customer. Each engagement includes five phases designed to help an enterprise achieve its security objectives in an efficient, effective manner. These phases include:

- Initial discovery session
- Assessment review
- Detailed manufacturer evaluations
- Procurement, configuration and deployment
- 24/7 telephone support

In addition to assisting with the design and implementation of security solutions, CDW staff are available to perform a wide range of security assessments.

To learn more about the Trend Micro security solutions available through CDW, contact your CDW account manager, call 800.800.4239 or visit CDW.com/trendmicro

The CDW Approach

ASSESS

Evaluate business objectives, technology environments and processes; identify opportunities for performance improvements and cost savings.

DESIGN

Recommend relevant technologies and services; document technical architecture, deployment plans, "measures of success," budgets and timelines.

DEPLOY

Assist with product fulfillment, configuration, broad-scale implementation, integration and training.

MANAGE

Proactively monitor systems to ensure technology is running as intended and provide support when and how you need it.

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed.

CDW®, CDW·G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC.
All other trademarks and registered trademarks are the sole property of their respective owners.

Together we strive for perfection. ISO 9001:2000 certified

MKT13913— 160108 — ©2016 CDW LLC