

Managing Multiple Devices: Integrated Defense Against Cross-platform Threats



Macs Expand in the Enterprise

Businesses today are set on multidevice, cross-platform IT environments. Despite issues that come with the bring-your-own-device (BYOD) trend and consumerization of IT, these trends accelerate employee productivity, allow remote access to corporate data, and improves worker flexibility.¹

More and more businesses are using Macs in the PC-dominated enterprise. In 2012, almost half of enterprises issued Macs to at least some of their employees.² Experts predict that Apple will sell \$8 billion in Macs to companies in 2014.³

As different types of devices and operating systems (OSs) enter the workplace, maintaining IT control and protecting corporate data become more and more complex. This is also challenged by the OS's unique compatibility needs for security.

Multiplatform Business Risks and Impact

The complications that come with a multiplatform environment range from malware attacks and exploits to data leakages and amplified patching problems. Diminished IT control is an issue that causes an impact on enterprises.

Cross-platform Threats and Exploits

Malware attacks and exploits may target cross-platform organizations and expose confidential corporate information. Endpoints without security software may serve as vectors of malware infections and exploits.

¹ Forrester Consulting. *A Forrester Consulting Thought Leadership Paper Commissioned By Trend Micro*. "Key Strategies To Capture And Measure The Value Of Consumerization Of IT". May 2012. Last accessed September 2013. http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf

² Gillett, Frank. *Forrester's Blogs*. "Apple Infiltrates the Enterprise: 1/5 of Global Info Workers Use Apple Products for Work!". Last updated on Jan 26, 2012. Last accessed September 26, 2013. http://blogs.forrester.com/frank_gillett/12-01-26-apple_infiltrates_the_enterprise_15_of_global_info_workers_use_apple_products_for_work_0

³ Moore, Galen. *Boston Business Journal*. "Apple will sell \$39B worth of iPads and Macs to businesses over 2 years – Forrester". Last updated Jan 4, 2013. Last accessed. http://www.bizjournals.com/boston/blog/mass_roundup/2013/01/apple-ipad-mac-for-business.html

64%

of enterprises are likely to embrace Macs over the next few years.

Ellen Messmer
Source: Network World

Malware attacks targeting multiple OSs, such as DNS changer Trojans, are not new to the threat landscape.⁴

However, threats that exploit vulnerabilities in platform-agnostic programs are growing. For instance, a zero-day exploit in Java was used to deliver a Poison Ivy Trojan and targeted diverse OSs.⁵ Additionally, a Windows version of the Mac Crisis Trojan (aka MORCUT) infected VMware® virtual machines and Windows® mobile devices.⁶ A mobile threat also took advantage of spammed messages to lure users into downloading malicious apps.⁷

Magnified Deployment and Patching Issues

Multiplatform enterprises are more prone to exploits because of the challenges they present in covering security holes. Administrators must deploy different security mechanisms for each platform running on any given mixed-device environment. This is to ensure that the devices' hardware and software specifications and requirements are met. If the installed security solutions are not compatible across all endpoints, cybercriminals or attackers may leverage unsecure platforms for their malicious activities.

Another issue with multiplatform businesses is the distribution of platform fixes by their respective software vendors. These vendors may release patches on different dates, or may not release patches at all. Attackers can easily take advantage of the extensive time it would take to deploy necessary updates across multiple devices.

⁴ Trend Micro Incorporated. (2013). *Threat Encyclopedia*. "How DNS Changer Trojans Direct Users to Threats." Last accessed September 26, 2013, <http://about-threats.trendmicro.com/us/webattack/125/How+DNS+Changer+Trojans+Direct+Users+to+Threats>

⁵ Sumalapao, Jasen. (2013) *Trend Micro Threat Encyclopedia*. "JAVA_GONDY.A". Last accessed September 2013. http://about-threats.trendmicro.com/Malware.aspx?language=au&name=JAVA_GONDY.A

⁶ Asprey, Dave. (August 23, 2012). *Cloud Security Blog*. "Averting a 'Crisis' for your VMware environment." Last accessed September 26, 2013. <http://cloud.trendmicro.com/avertingcrisis/>

⁷ Yan, Peter. (September 13, 2013) (*TrendLabs Security Intelligence Blog*. "Spam Leads to Multi-Platform Mobile Threat". Last updated on September 13, 2013. Last accessed September 2013. <http://blog.trendmicro.com/trendlabs-security-intelligence/spam-leads-to-multi-platform-mobile-threat/>

Decentralized Endpoint Management

Maintaining different devices may mean managing separate consoles for Windows-based devices and Apple products. This setup would not only consume time and resources, but also reduce IT control and visibility to data security.

Case in point, Macs require a bigger cut in the budget when it comes to hardware, software, IT labor and administration. The table below shows that Macs are more costly to maintain than PCs by small margins.

AVERAGE COST	MAC	PC
Hardware and software	\$1,622	\$1,513
IT labor	\$781	\$636

Source: "Mac Workplace Penetration Loosens Window's Stranglehold on Enterprise"
http://appleinsider.com/articles/12/06/06/mac_workplace_penetration_loosens_windows_stranglehold_on_enterprise

Aside from budget concerns, device fragmentation in a multiplatform setup makes it difficult for IT administrators to monitor the data that goes in and out the network. This increases businesses' exposure to data leak and loss. Without centralized security deployment, confidential corporate information will be open to these risks.

An Integrated, Data-focused Approach to Security

Multiplatform business setups need a defense strategy composed of not only endpoint solutions, but also of data security policies for employees. This way, protective technology can be complemented with proactive security coverage from the actual people accessing data from different devices. These policies should be custom-built to the inherent IT structure of a given enterprise environment. For instance, IT administrators must limit the access of employees to highly confidential corporate data to prevent data leakage.

The following security technologies must be integrated to a well-crafted defense plan to improve management and protect data in cross-platform environments:

- **Centralized console:** A single console can help defragment threat and data protection policy management across multiple endpoints and infrastructure layers. It can also make policy enforcement easier and more consistent.
- **Comprehensive, reputation-based threat intelligence:** To spot and block emerging malware and exploits in enterprise networks, organizations need smart correlation technology and services that can actively check and analyze the threat landscape using both internal and external resources.
- **Data encryption and data loss prevention:** Integrate a full set of data security products that encrypts all the data that goes in and out the enterprise network. This is to safeguard the privacy of critical corporate data across all gateways and endpoints. Make sure that these solutions fulfill regulatory compliance as well.
- **Mobile and desktop virtualization:** A virtualized environment deployed for endpoints can provide a clear separation between personal and corporate applications or data. This solves one of the biggest data and security concerns especially among those that implement BYOD in the workplace.

Enterprises should not rely solely on security software for protection, however advanced they may be. The need to reinforce employee training in actual security incidents is also an important step toward security awareness and compliance.

Created by:
TrendLabs
Global Technical Support & R&D Center of TREND MICRO

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative security solutions for consumers, businesses and governments protect information on mobile devices, endpoints, gateways, servers and the cloud. For more information, visit www.trendmicro.com

©2013 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.



Securing Your Journey
to the Cloud