IT SECURITY OR IT MANAGEMENT FOR SMBS?

CAN YOU HAVE ONE WITHOUT THE OTHER?

panda

pandasecurity.com

Malware is now focused on economic gain not economic havoc.

The nature of security is evolving to keep up with an ever changing threat landscape. As most industries are in the grips of technological transformation fuelled by the cloud, mobility and, to some extent Big Data, the evolution of the IT security is not exempt and must also respond to profound change.

The malware industry for a long time has been driven by financial gain and has long ceased to gravitate around the personal egos of programmers, hackers etc. as was the case in its early days when **I Love You* and Anna Kournikova where the malware that got the public and the media's attention.**

Like any other industry when dollar signs start to appear able parties will come on the scene to leverage the opportunities that are up for grabs.

The goal now is clearly economical and the longer malware can stay on systems undetected the more profitable it can be for its owner.

The I love you virus is estimated to have affected 45 million PCs and have caused US $5.5-8.7 billion in damages worldwide and estimated to cost US $15 billion to remove the worm.

However, it created no economic gain for its developers (Wikipedia)

Investment in malware is driving historic numbers

This influx of investment in malware development is breaking all malware creation records; in 2013 the number of malware created represented 20% all of historic malware, resulting in 84.000 new malware strains created per DAY.

At the head of the threat list we can still find Trojan horses, which are a type of malware designed to leverage systems and application vulnerabilities which in themselves represent another part of the overall protection problem.

31,53%
INFECTED COMPUTERS IN THE WORLD

3.800
EVERY HOUR

84.000
A DAY

30
MILLIONS
2013

PANDALABS
HAS REGISTERED OVER

145
millions
DE EJEMPLARES DE MALWARE

28,96%	USA
24,84%	Spain
54,03%	Brasil
38,01%	Argentina
22,68%	UK
20,28%	Sweden
22,14%	Germany
38,18%	Russia
34,99%	China
32,72%	Japan

Today's disperse mobile, heterogeneous environments are creating new management headaches and additional security gaps.

As expenditure and dependency on hardware and software increases **(«State of SMB IT» Report from Spiceworks),** IT systems are becoming more heterogeneous, disperse and complex to manage. Simply from a volume perspective, IT professionals now face the challenge of managing multiple sites, various operating systems and multiple devices per user. Each additional device adds to a company's efficiency but also creates an additional vulnerability.

When it comes to mobile, in the case of SMBs, we can clearly see how this problem is even more accentuated, as analyst firm Gartner mentioned in a recent report*; SMBs face many of the same challenges as larger/ enterprise companies when getting their mobile devices under control and secure.

All of this complexity stretches tech teams to the limit and creates additional weak links in the security armor.

For instance, one of the problems in protecting this new technological mash-up is caused by a false sense of security in the belief that some devices are not vulnerable, such as MAC and or Linux devices.

«The greatest vulnerability of Macintosh is the belief among devotees that the Apple operating system is superior and that this makes them immune to malware»**. This misconception leaves an inviting open door for malware (including Windows malware) to enter unchallenged and take advantage of those weaker links.

*Gartner_March 2014

The Six Pain Points of Managing Mobile Devices for Small or Midsize Businesses.

** Whitepaper_May 2014 Should I be worried about viruses in my MAC?

• Mobility-related spending by US and Canada SMBs is poised to reach $71.5 billion by 2018, says AMI, an example is a 21% CAGR in the U.S. and Canada for tablet data plans alone.

http://www.ami-partners.com/index.

• Gartner BYOD by 2017 http://www.gartner.com/newsroom/id/2466615

• Gartner forecasts Gartner Predicts by 2017, Half of Employers will Require

Employees to Supply Their

Own Device for Work Purposes

First step in the right direction: The cloud, from an early adopter option to an industry necessity.

With malware numbers breaking all records, security vendors can no longer rely solely on on-premise, signature file based solutions to protect their customers IT systems. In addition to reduced detection capacity, as the malware volumes increase, such solutions leave heavier foot prints on networks.

Security vendors now look towards the cloud and the immense processing power of big data to respond to the vast and ever growing threat while transferring the work load from the network / device to the cloud. This has, in part, enabled some security vendors to get a strong grip on the new threat landscape while allowing companies to focus on their businesses and not on the security management. A great step in the right direction but, as we mentioned, this only covers part of the problem.

Systems and software vulnerabilities are now the cause of the great majority of infections to such an extent that savvy IT managers know that just focusing on best of breed AVs and Firewalls, even those in the cloud, is no longer a full response to an ever growing problem.

Over 90% of all infections are caused by non patched vulnerabilities, typically in third party software such as Java, Adobe, Flash etc.

PandaLabs 2013

The majority of on-premise solutions depend on signature files that generally update once every 24 hours, in some cases less but clearly insufficient for the daily rate of 82.000 new malware that appear on the Internet, PandaLabs 2013.

Having a cloud based solution means that everything is constantly up to date, one less management task and zero hardware or additional software is required on your network.

The convergence of security and management.

As systems and application vulnerabilities become ever more critical, a logical convergence of device **security and device management** is taking place. Security goes beyond the traditional AV and FW approach and takes on a much broader scope which begins with visibility and ends with enforced policies. This new scope must also contemplate remediation for it to be considered complete and needs to be applicable across the entire IT systems with zero exceptions.

Up to some time ago (PC era), in LAN based networks with a vast majority of windows desktops and servers with few exceptions, managing most aspects of systems and software updates was doable although very time consuming. Now, in the Post PC era, the exception is the rule but the challenge is the same; IT managers, to reduce the overall security threat, MUST be capable of managing every device regardless of its location. Put into tangible terms: they must guarantee permanent device visibility, guarantee that devices are up to date, fully patched and optimized. And if something goes wrong, there must be mechanisms in place to respond rapidly and effectively.

Unfortunately in today's companies just having permanent visibility of dispersed and heterogeneous environments is far from the norm.

Microsoft estimates that only 40% of enterprises have any real credible device management in place.

Decreasing fragmentation and complexity.

Dispersed

Fragmented environments with so many device types can lead to the implementation of quick fixes, fragmented solutions; one solution for software updates, one for security, one for remote support, MDM...etc. To be able to get the problem under control and gain new levels of efficiency with the same team members the solution must be centralized. All devices, all IT tasks from one centralized solution for the entire IT team, anywhere, anytime.

Complexity

Is inherent in the problem, various devices per user, various sites, BYOD. However, responding to the problem with fragmented solutions only creates a vicious circle where complexity is increased with each additional solution that is implemented.

The solution you chose must have a quick route to value, be easy to implement, and manage with a near zero learning curve, a solution that simplifies the complexity of today's IT systems.

To summarize

Malware, driven by economic gain, is growing exponentially. SMBs are challenged with managing more heterogeneous, dispersed and complex IT systems which only enlarges the security problem.

This creates additional gaps and stretches current human resources to the limit and beyond.

Cloud, mobile and big data are not only part of this new IT reality but also an intrinsic part of protecting and managing it. Device management is now converging with security so that companies can address security from a broader perspective while gaining great efficiencies. This convergence, for it to be adopted and leveraged by SMBs, must be centralized, complete yet NOT complex.

The question is NOT do I need to manage and secure every device. It is how can I BEST do that?

The underlining issues here have been fragmentation and complexity.

Panda Cloud Fusion

Panda Cloud Fusion is about simplifying and centralizing cloud security, management and support. Panda Security has a complete approach to systems management in that every device counts; regardless of if it is a Windows XP desktop, a Linux Sever, a MAC book or a tablet / Smartphone, if it is on or off the LAN, you can manage, secure and support them all from one centralized console.

As Gartner mentioned in Jan 2014, EEP Magic Quadrant, «Panda is [also] the first End Point Protection vendor to fully embrace cloud delivery of security services.» Classified as a visionary in End Point Protection, Gartner underlines Panda's protection capability and capacity to «catch latest threat's» thanks to behavioral based detections and cloud based knowledge, Collective Intelligence.

In the same report Gartner mentions the strengths of the «recently added [a] remote endpoint system management solution, which includes audit, configuration, patch and software distribution capabilities, as well as remote control».

Centralized auditing means IT administrators can have permanent visibility of their entire IT systems from one console, including mobiles and smartphones.The out of the box patch management and software distribution functionalities ensure systems are patched and optimized which in turn reduces the threat of attack via vulnerabilities.

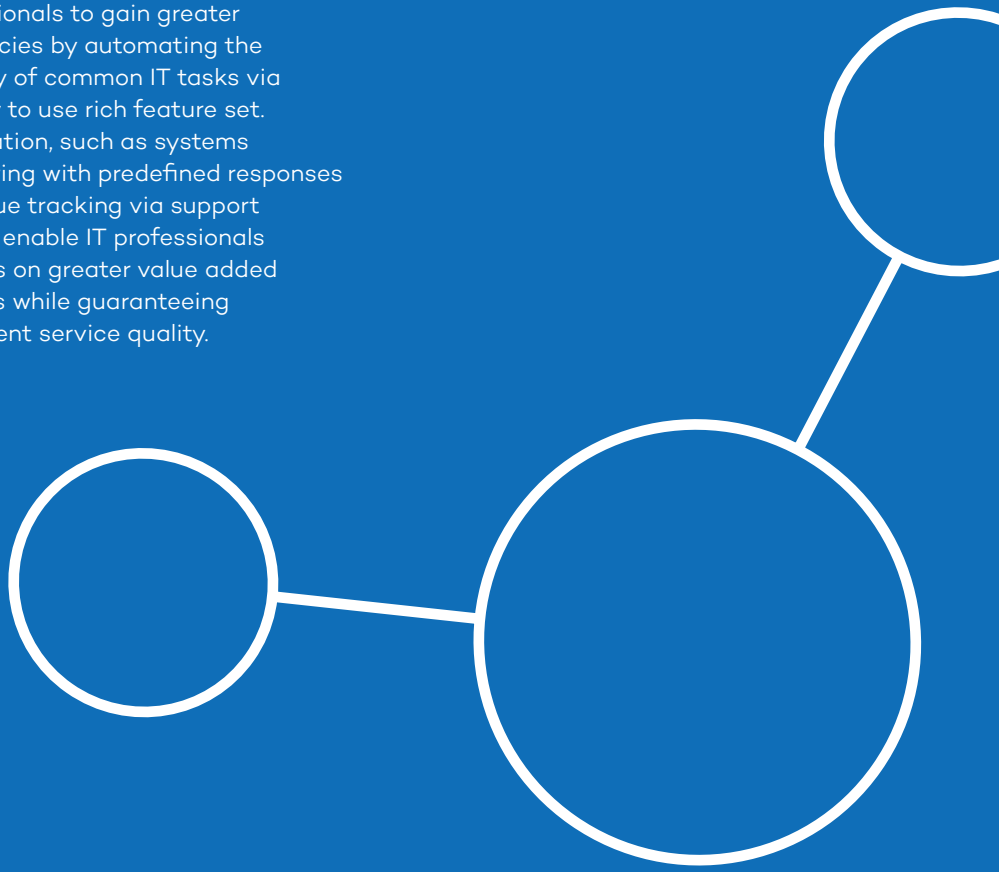
Non-intrusive remote support completes the offering by enabling technicians to run extensive problem diagnostics and implement solutions in the background while end users continue to use their systems.

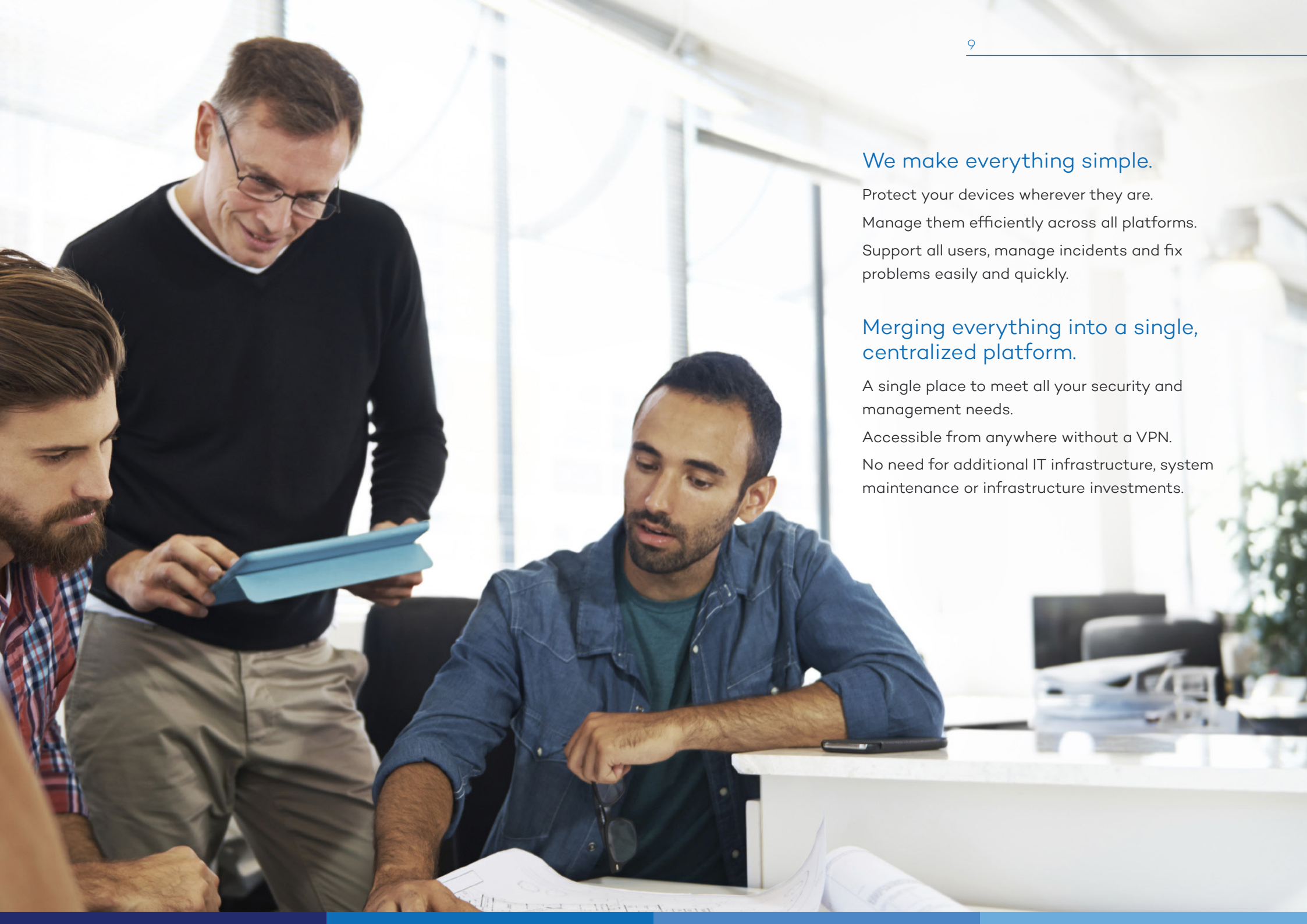
In addition to optimizing and securing all your devices Panda Cloud Fusion also empowers IT professionals to gain greater efficiencies by automating the majority of common IT tasks via an easy to use rich feature set. Automation, such as systems monitoring with predefined responses and issue tracking via support tickets, enable IT professionals to focus on greater value added projects while guaranteeing consistent service quality.

Find out more about Panda Cloud Solution

Try it yourself for 30 days

Download here





We make everything simple.

Protect your devices wherever they are.

Manage them efficiently across all platforms.

Support all users, manage incidents and fix problems easily and quickly.

Merging everything into a single, centralized platform.

A single place to meet all your security and management needs.

Accessible from anywhere without a VPN.

No need for additional IT infrastructure, system maintenance or infrastructure investments.


panda