Close the Mac Security Gap in your Enterprise

Bit9

Key Facts about Mac® OS X® Attacks

!

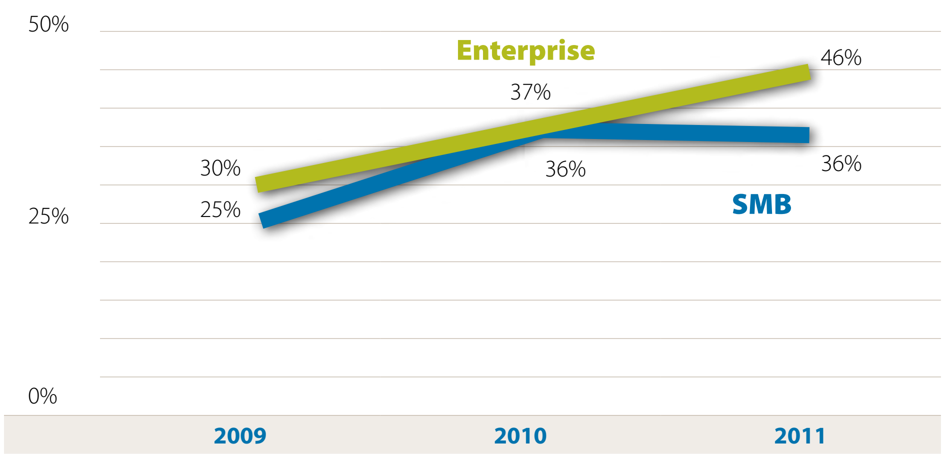
In 2011, IT decision-makers forecast a **52%** increase in the number of Macs they will issue in 2012.

In Companies that issue Macs, **7%** of all personal computers issued are Macs.

> "By 2014, Macs will be as accepted by enterprise IT as Windows PCs are today."
> *Source: Gartner, 2012*[1]

IT support for Apple Mac personal computers is significant and rising.

Percentage of Companies Issuing Personal Computers Running Mac OS X



Source: Forrester Research, 2012[2]

As cyber threats become more sophisticated, and Windows security sees increasing investment, Macs have emerged as an attack vector opportunity.

Mac Malware: Slower to Develop, Catching Up Fast

2011	2012 Increasing Capabilities, Knowledge of OS X				2013	
MacDefender Fake AV	Flashback Trojan	OSX/NetWrdRC-A Kit with Backdoor	Mal/DevGen-M Key Generators	Morcut/Crisis Spyware with Command & Control	"Watering hole" attack on Apple Inc., Facebook, etc.	OSX/KitM.A and variants

[1] Gralla, Preston, *Apple Storm's Microsoft's Castle*, Computerworld, February 4, 2013.

[2] Gillette, Frank, et. al., *Apple Infiltrates the Enterprise and Reshapes the Markets for Personal Devices at Work*, Gartner, January 26, 2012.

Emerging Enterprise Vulnerability

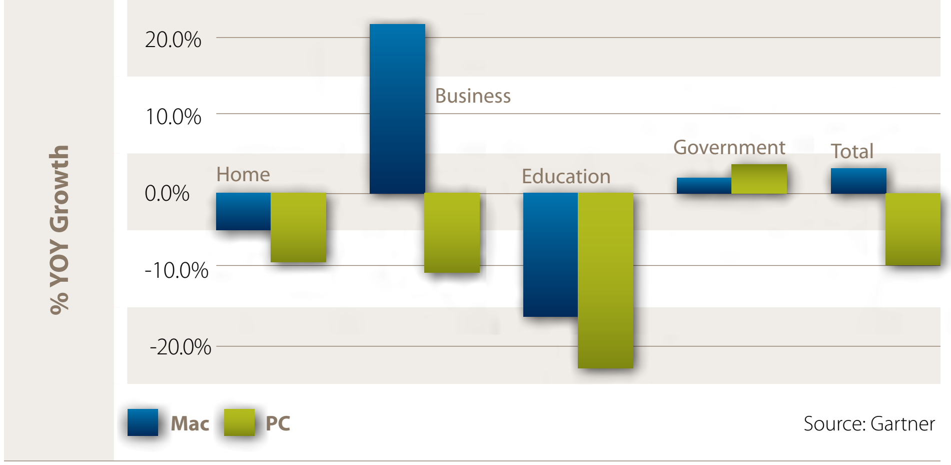
This increased use of Macs, and the evolving threat landscape, presents additional challenges for enterprise security teams.

According to MacInsiders' most recent report, Mac usage in business environments continues to grow. Sales of Mac hardware to U.S. businesses are experiencing 49.4 percent year-over-year growth.[3]

What's Driving this Growth?

The trend of giving people a choice in the platform they use (BYOD), most commonly thought of in terms of mobile devices, extends to desktops as well. Apple's success with iOS devices has made the Apple brand more familiar to enterprise users. The halo effect of BYOD is driving consumer demand to use Macs in business.

Mac's Growth vs. PC Market Growth, September 2012



Source: Gartner

Some interesting facts: According to Forrester Research, managers and execs are more than twice as likely to use Apple products—and businesses in countries outside North America and Europe are more likely to use Apple products for work.[4]

Advanced attackers are always looking for enterprise infrastructure vulnerabilities, and their knowledge of how to exploit Mac endpoints has grown.

This eBook will give you an understanding of the nature of malware exploiting Macs — and how to adopt a security posture that works for your entire enterprise infrastructure.

LEARN MORE Bit9 Blog
First Next-Gen Endpoint and Server Security Solution for Mac

LEARN MORE Video
The Future of Cyber Security with Bit9's CTO Harry Sverdlove

[3] Hughes, Neil. *Mac Sales to US Businesses Grow Nearly 50%.* AppleInsider, November 12, 2012.

[4] Gillette, Frank, et al. *Apple Infiltrates the Enterprise and Reshapes the Markets for Personal Devices at Work.* Gartner, January 26, 2012.

No More "Security through Obscurity"

Greater Incentive to Crack OS X

The development of security solutions for OS X has lagged behind those for protecting Windows environments. Mac advocates claimed "nobody hacks Macs" and touted their "security through obscurity."

With Windows' security improving, and with the growing use of Macs in the enterprise, there's now more incentive for perpetrators of advanced attacks to invest in Mac malware. Mac OS X vulnerabilities have become the weaker link in the enterprise security chain.

- 35.5 percent of all Mac users are running versions of OS X that are officially unsupported by Apple — and are at higher risk of contracting malware delivered through flaws in the Java browser plug-in, which was shipped with every version of OS X until Snow Leopard.[5]
- Earlier this year, exploitation of this vulnerability in the Java browser plug-in affected OS X systems at Apple and Facebook,[6] as well as at Microsoft and Twitter.[7]

Exfiltrating Data Directly from Macs

OS X malware has become more adept at finding and exfiltrating data than the more heavily defended Windows.

Senior executives using Macs represent "bigger fish," aka high-value targets. Identified through social engineering, like phishing, these users might have valuable data like intellectual property, financials and strategic plans on their machines. And, of course, they can also lead to additional lucrative targets.

Exploiting the Gaps in Windows-based Security

Security solutions tuned for Windows won't pick up on unusual file-name variants or atypical locations for OS X environments that would normally send up red flags.

Nor will network security solutions easily recognize, as legitimate or not, anomalous traffic or user behaviors associated with the Apple® Safari® Web browser, such as pre-caching or network-discovery broadcasts generated by the Apple® Bonjour® services.

Bottom line:
Advanced threats exploiting Macs mean big headaches for IT and security staff.

LEARN MORE Datasheet
Bit9-for-Mac-Web-FNL

[5] Bott, Ed. *Latest OS Share Data Shows Windows Still Dominating in PCs.* ZDNet, April 1, 2013.
[6] Finkle, Jim, and Menn, Joseph. *Apple Computers Were Hacked by Same Hackers who Targeted Facebook.* Reuters, February 19, 2013.
[7] Schwartz, Matthew. *Microsoft Hacked: Joins Apple, Facebook, Twitter.* InformationWeek Security, February 25, 2013.

Mac Attacks Catching Up to Windows Malware

The malware designed to exploit OS X architecture, capabilities and vulnerabilities has become increasingly sophisticated.

- **MacDefender,** fake antivirus malware, appeared in 2011 as a pop-up prompting the user to download a program to remove viruses — which, if installed, provides the users' personal information to perpetrators.
- **Flashback Trojan** attacked more than 600,000 Macs in 2012 by targeting a Java vulnerability on OS X to download and run malicious code from a remote location.
- **OSX/NetWeirdRC** is an inexpensive malware kit allowing Mac malware designers to embed backdoor techniques.
- **Mal/KeyGen-M** performs file system changes, memory modifications, registry value changes, and registry key changes.
- **Sabpab** is a backdoor Trojan with remote control capability.
- **Morcut/Crisis** is spyware that infiltrates through a Java Archive file (JAR) that enables perpetrators to track IM transactions, location, keystrokes and mouse movement; contents of the clipboard; running processes; etc., a variant of Morcut, Win32 and Swizzor, that attack Windows.
- **OSX/KitM.A** allows hackers to access a compromised system by establishing a backdoor and uploads screen shots to a remote command-and-control server.

The evolution of OS X malware is similar to that of Advanced Persistent Threats (APTs) that target Windows environments.

Advanced attackers build on experience and return to try again and again using slightly different tactics. They may embed backdoors for stealthy return and later exfiltration of data. OS X malware is demonstrating remote Command and Control (C&C) capabilities that enable the attacker to perform reconnaissance and adjust tactics depending on what they encounter.

Bottom line:
OS X malware now poses a serious threat to protecting Personal Identity Information (PII), enterprise intellectual property, and trade secrets and business operations.

Apple: On the Right Track but Stops Short

> "It's no mystery that antivirus (AV) technologies are fighting a losing battle against an increasingly sophisticated malware threat landscape."
>
> - Forrester, 2012

Apple's Scan-based Blacklisting

After realizing that security through obscurity was not viable, Apple introduced limited malware scanning (LSQuarantine and XProtect technology).

But even with features such as an update service to detect and clean up files identified as malicious added, this approach has a fundamental flaw confronting advanced attacks.

Apple's Gatekeeper: Better, but…

In mid 2012, Apple took a step in the right direction when they introduced Gatekeeper. The Gatekeeper paradigm is based on "whitelisting"; it is designed to keep malicious software off of your Mac by giving you more control over what you install. Gatekeeper only allows you to run:

- Applications downloaded from the Mac App Store
- Applications downloaded from the Mac App Store and from identified developers
- Any downloaded application

While a step in the right direction, Gatekeeper still has significant limitations. Recently, backdoor malware (OSX/KitM.A) successfully bypassed Gatekeeper, having been signed by what appeared to be a valid Apple developer.[8]

Gatekeeper does not cover software already on the machine, physical transfer like USB sticks, software copied directly between machines, or transferred by nonstandard file- transfer systems such as Dropbox

Gatekeeper is not designed as an enterprise solution. For example, users with administrative credentials can change Gatekeeper's default settings without any alert.

But, most significantly, a separate security solution for Macs forces IT to use another, separate tool to learn, manage and stay updated.

[8] Clover, Juli. *Newly Discovered Mac Malware Captures and Stores Screenshots*. MacRumors, May 16, 2013.

Advanced Persistent Threats: A Mac Scenario

APT Penetration via Mac

At the request of senior executives in a large enterprise, IT purchases and installs several Macs on one network. For some time, and unknown to the enterprise, a cybercriminal group has been unsuccessful at infiltrating their malware by sending customized emails with attached malformed documents. But they try a new tack, targeting senior executives who are Mac users.

The email's attachment (an innocuous-looking Apple® Pages® file) contains an executable that's a new variant, built from a kit, of Mac backdoor malware.

When opened, the malware executes undetected and connects through the Mac to its C&C server.

The Advanced Persistent Threat (APT) is now in place. The C&C operator can access the cached credentials of the IT administrator who built the Mac. The perpetrator gains "legitimate" access to anything on the network: domain controllers, email servers, etc.

The perpetrators can begin to exfiltrate data out through the Mac, cleaning up their tracks along the way.

Why Wasn't the APT Detected?

If built with a runtime interpreter preauthorized by Apple (OS X shell scripts, Java, Flash), the backdoor malware would have passed Gatekeeper without notice.

Antivirus wouldn't catch it because this new malware wasn't in its signature library — nor was the behavior picked up by network security solutions designed only for Windows.

Remediation is Difficult

Unfortunately, without having recorded relevant activity from the initial attack, it is very difficult to trace all potential paths and remediate.

You may have two different IT teams involved — one that manages Macs and the other Windows. Neither has the capability to look across what's happening on Windows and OS X machines simultaneously.

Finding all the components of the malware, backdoors and the damage caused will take weeks — if it's possible at all.

The Bit9 Security Platform: Protecting Windows *and* OS X

LEARN MORE eBook
Detecting and Stopping Advanced Attacks

LEARN MORE White Paper
Advanced Threat Landscape: What Organizations Need to Know

What if there was one comprehensive solution that protected both Windows and OS X endpoints and servers?

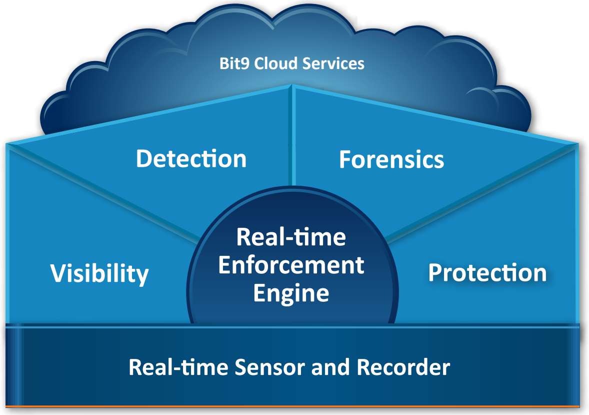
Bit9 for Mac is the only next-generation endpoint and server security solution that continuously monitors and records all activity on Mac endpoints and servers to provide real-time protection against cyber threats that evade traditional security defenses. Bit9 for Mac defends teams in four key areas:

1. Visibility: Know What's Running on Every Computer

From a single console, Bit9 provides immediate visibility into the files, executables and critical system resources on every machine protected — whether Windows or OS X. Macs are no longer vulnerable to blind spots in the enterprise infrastructure.

2. Detection: Real-Time Protection against Advanced Threats

Get real-time, signatureless detection of advanced threats and zero-day attacks that evade traditional Mac antivirus tools. Bit9 combines real-time sensors, Advanced Threat Indicators (ATI), and the Bit9 Software Reputation Service to immediately detect malware. No waiting for signature file updates. No testing and updating .dat files.



3. Protection: Stop All Untrusted Software from Executing

Bit9 Security Platform lets you define policies for the software that you trust in your enterprise. Everything else is denied by default. This stops advanced threats and malware — including customized attacks targeted specifically at your organization.

4. Forensics: Full Audit Trail Accelerates Analysis and Response

The same continuous monitoring and recording that gives you real-time visibility into what's happening on each OS X or Windows machine also allows you to "go back in time" when needed.

This helps you see what happened in the past, understand what is happening right now, isolate untrusted software, and determine the trust rating for any file.

Bit9: Closing the Endpoint Security Gap

> "It's a big mistake for enterprise security teams to underestimate the potential risks their Mac deployments represent. Bit9 has delivered a version of its platform for Mac that addresses this growing problem with a true enterprise-class security solution that offers real-time monitoring and recording and the same level of protection against untrusted software it offers for Windows."
>
> - Fran Howarth,
> *Security Practice Leader for*
> *Bloor Research*

Next-generation endpoint and security solutions, such as Bit9's, close the endpoint security gap in enterprises.

IT has One View into all Machines: Windows and OS X.

Imagine having visibility into every machine on the network — whether running Windows or OS X: one console, one view, the same tools managing both operating systems. There are no endpoint blind spots.

Support employees' demand for Macs in businesses while maintaining the level of security required in today's enterprise computing environment:

- Immediate visibility into everything running on your Mac endpoints and servers for immediate identification of untrusted software
- Superior protection against today's advanced threats and zero-day attacks that target the Mac platform
- Complete recorded history of all Mac endpoint and server activity for deep forensics
- Strengthened compliance to include Mac endpoints and servers

LEARN MORE Video
Bit9 for Mac: Closing the Mac Security Gap in your Enterprise

About Bit9

About Bit9 for Mac:

Bit9 is the first next-generation endpoint and server security solution provider to offer a comprehensive solution for securing both Macs and Windows endpoints and servers.

About Bit9:

The **Bit9 Security Platform** is the only next-generation endpoint and server security solution that continuously monitors and records all activity on endpoints and **servers** and stops cyber threats that evade traditional security defenses. Bit9's real-time sensor and recorder, **cloud-based services** and real-time enforcement engine, give organizations immediate **visibility** into everything running on their endpoints and servers; real-time signatureless **detection** of and **protection** against advanced threats; and a recorded history of all endpoint and server activity for deep **forensics**.

Follow us online: