

# *Whitepaper*

## **A Cybersecurity Solution for Mortgage Companies**

**By**  
***Access Business Technologies***



***February, 2017***

# A Cybersecurity Solution for Mortgage Companies

## I. Executive Summary

Cybersecurity is a hot topic for every business today, no matter its size or market. In recent years, we've seen cybercrime spread like wildfire throughout the financial marketplace, leaving many mortgage companies wondering, "Are we next?"

Mortgage companies and financial institutions are at an especially high risk of becoming the target of a cybersecurity attack. Even small mortgage companies face data breaches from viruses and worms that infiltrate security measures via infected emails or fake social media ads. No business is immune from hackers intent on stealing sensitive financial and personal information—just ask the government agencies and department stores that have suffered heists of massive consumer information.

No longer can small businesses count on their size as a protection against attack. The question today for CEOs and small business owners is not *if* cyber hackers will attack their businesses but *when*.

Exacerbating this issue is that cyber criminals seem to evolve and become more sophisticated in their attack methods every day. They delight in thwarting the latest security systems with new hacks. They bypass security protocols to hide evidence of malware in victim networks, making it harder to recognize when an attack is imminent. Worms wait for opportunities to self-execute, and trojans lay concealed until an unsuspecting person unintentionally triggers the fatal execution command. Cyber criminals no longer seem satisfied with causing interruptions of the work stream and disruptions of service. Now, they extort money.

In this report, we will discuss in depth the scope of today's cybersecurity problem. The truth is that mortgage businesses need a comprehensive and streamlined approach to cybersecurity—one that protects vulnerable endpoints throughout your entire network. As mobile devices become increasingly common in the workplace, those too must be secured from attacks.

DeviceGuardian™ is a unique tool that has been developed to meet the specific needs of mortgage professionals and help them fight back against cybercrime. In a highly connected and mobile world, what are you doing to keep your customers and their private data safe?

## II. The Cybersecurity Problem

It's hard to overstate the size of the cybercrime problem when a conservative estimate places the number of breaches in 2015 at [half a billion](#) personal information records stolen or lost. Security experts estimate the number of reported identities affected in 2015 was 429 million. The problem may be even greater than that because companies often choose not to report the full extent of successful breaches.

Another problem is that administrators often leave the doors open to cyber criminals by failing to secure their websites from vulnerabilities. Symantec's security experts estimate that almost 75% of all legitimate websites have unpatched vulnerabilities.

Mobile devices, and the applications they run, are notoriously unsecure and present an even more pressing need for holistic cybersecurity strategies that protect every device at every level, wherever mortgage loan officers happen to be.

### **All Types of Attacks Are on the Rise**

Phishing campaigns have increased 55%, while ransomware has increased 35%. The targets are changing, too, as hackers carried out ransomware attacks against popular devices like smart phones, smartwatches, and smart TVs, as well as Mac and Linux operating systems that were once deemed impenetrable.

The more connected businesses become the more vulnerable they are and the more costs continue to escalate. The average cost of a corporate data breach increased to [\\$3.5 million in 2015](#). To put that another way, on a consolidated average basis, each lost/stolen record of sensitive and confidential information costs \$145.10. In the US, those costs are \$246 per lost/stolen record. That statistic makes it easy to understand why the losses incurred by the financial services sector from security breaches increased by 24% in 2015.

Security breaches are also costly in terms of lost time. Security incidents caused more than 8 hours of downtime for 31% of organizations. Can you afford that kind of downtime?

### **Some Good News**

The good news is that companies that report having a strong security protocol also report reducing the cost of breaches by as much as \$14 per record. Companies that maintain strong business continuity management policies reduced their data breach costs by an average of \$9 per record.

### **Mobility Costs**

As companies increase their dependence on mobile devices (and who isn't in today's digital marketplace), their vulnerability to attacks and stolen information increases. Symantec's report indicated the following eye-opening statistics:

- Thieves steal one laptop every 53 seconds.
- 70 million smartphones are lost each year, with only 7% recovered.
- 4.3% of company-issued smartphones are lost or stolen every year.
- 80% of a lost laptop's cost relates to data breach.
- Thieves steal 2% of mobile devices from the office/workplace but a whopping 24% from conferences. Implementing and enforcing strong security policies has shown it can reduce laptop theft by 85%.

### **Other Statistics Round out the Problem**

The Bit9 + Carbon Black Threat Research team undertook a ten-week study that found five times more operating system malware in 2015 than during the **previous five years combined**.

In 2015, the Internet Crime Complaint Center reported 2,500 cases of ransomware at a cost to victims of \$24 million in the US alone. In addition, researchers report tracking over 500 different types of malware used to bypass security detection. The average number of evasion techniques used per malware sample is 10. The math astoundes.

### **More Astounding Insights**

Ninety-seven percent of malware is unique to a specific endpoint, which means that signature-based security protocols become virtually useless. Malicious execution is possible in 15% of new files.

Microsoft Office-targeted threats use macros 98% of the time, and there was a 50% increase in email attacks where macros are the method of infection. Researchers found a more than 600% increase in attachment-based vs. URL-delivered malware attacks from the middle of 2014 to 2015. The AV Test Institute registers 390,000 malicious programs every day.

### **There Is Hope**

Businesses can realize a 19.2% potential increase in detecting malware simply by adding a second anti-virus program to existing email security, while cleansing or purging dangerous or hidden code in files can help eliminate macro malware threats.

## **III. Malware: A History & Background**

When it comes to managing cybersecurity, it is useful to understand the complex mechanisms with which hackers can launch attacks against networks.

Malicious software (known popularly as malware) is a broad term. In general, the term refers to any type of software that hackers use to disrupt computers, computer networks, or mobile devices. Malware can operate as simply as displaying pop-up ads or other unwanted programs that slow down computer systems.

On the other hand, more sophisticated malware often gathers financial or other sensitive personal information that it then passes on to third parties for more heinous purposes. In the most common occurrences, hackers use stolen authentication details to gain unauthorized access to networks.

Another factor to bear in mind: hackers deliver [66% of malware](#) via infected email systems.

Below, we'll discuss the various types of malware.

### **Computer Viruses**

Computer viruses work to infect digital files in much the same way that human viruses attack the human body. When a virus infects a machine's files, the virus can spread to other machines when the infected computer sends infected files through the email system or on a USB drive.

As one version tells it, the first virus [to thwart software piracy](#) came on the scene in 1986. Creators named the virus the "Brain" and infected the boot sector of floppy disks. When the thieves copied the disks, the virus disseminated to their computers.

The main thing to remember about viruses is that they need humans to spread and infect other machines or media.

### **Worms**

Worms operate in a fundamentally different way from viruses. They do not need humans to spread to other machines. Worms infect a computer once, then they use networks of computers to spread the infection to others—all without the help of human users.

Worms exploit weaknesses in email programs, networks, or software. Worms can send thousands of copies of themselves to infect new systems, and then the worm's life cycle begins again.

In the beginning, worms generally disrupted system resources and slowed the infected computer's performance. In today's increasingly digital world, however, worms consist of malicious code designed to steal files or delete them.

### **Adware**

As the name implies, most people recognize adware as the online nuisance that automatically delivers advertisements to computers. Adware includes the ubiquitous "pop-up" ads that disrupt access to web pages, as well as ads that come with "free" software.

Adware is mostly a harmless nuisance. However, some adware products contain tracking tools that can steal information from a consumer's browser history, including the consumer's geographic location, and then send targeted ads to his computer. Most recently, [security expert](#) Malwarebytes warned consumers that a new type of adware seeks to disable virus software.

Since users voluntarily install adware, it is not malware (which attacks without permission). Adware is a "potential unwanted program," or PUP.

### **Spyware**

Well-named, spyware does just what it says. Spyware collects data like keystrokes, browser habits, and login information, which it then turns over to cyber criminals. Spyware also changes security settings on infected computers or interferes with network connections. [TechEye](#) warns that newer spyware programs may track user behavior across multiple devices without consent.

### **Ransomware**

This malware is more vicious. When ransomware infects a computer, it encrypts the sensitive data it finds (personal documents, photos, financial information) and then demands payment of money in order to effect its release. Businesses or individuals who refuse to pay the ransom risk data deletion as punishment.

Some ransomware encrypts the data and locks the owner from all access to the computer or network. The ransomware known as [CryptoWall](#) caused users to report \$18 million in losses in 2015 to the FBI's [Internet Crime Complaint Center](#).



### **Bots**

Bots are malware that hackers program to execute specific operations automatically—without the user's approval or knowledge. Hackers who can infect multiple computers using the same bot create a "botnet" (derived from robot network).

Hackers can use botnets to remotely manage infected computers. Hackers use botnets to steal sensitive or personal data, spy on users' activities, disseminate spam, or launch distributed denial of service (DDoS) attacks via their managed networks.

### **Rootkits**

Rootkits allow IT professionals to remotely troubleshoot network issues, but they can also create big problems. By design, rootkits give third parties remote access to a computer or a network. Rootkits also actively hide their presence.

Once rootkits install on a computer, hackers can gain complete control over the computer and its networks. They can steal data or install malware. The only way to uncover this malicious code is by manually scrutinizing traffic for unusual behavior. Best practices also call for regularly patching the operating system and software to ward off potential infections.

### **Trojan Horses**

Trojan Horse malware has been around awhile. Like its namesake, these malware programs hide in plain sight by masking themselves so they appear as authorized files or software. Once installed on a system, Trojans can execute changes to the victim's computer and perform malicious code, all without the knowledge or consent of the user.


### **Bugs**

Bugs in software are not malware but, rather, programmer errors that can, nevertheless, have serious effects on a victim's computer. Typical effects involve freezing, crashing, or slowed performance.

On the other hand, bugs in security software are more lethal. They often provide hackers a pathway to avoid security defenses and infect the computer or network. This is why it's so important to update software patches that address specific programming bugs.

## **IV. About DeviceGuardian™**

Mobile devices have exploded into the workplace and are now widely used by mortgage industry professionals. In fact, many mortgage companies are now jumping on the BYOD trend and adopting IT policies that allow, and even encourage, employees to use their own personal devices for work production.



These factors combine to put pressure on mortgage companies to find a simple and streamlined way to secure borrower data on mobile devices. Ultimately, the most effective solutions require mortgage employees to manage and modify their personal devices in specific ways to ensure they are completely secure. This often involves installing device-level security software and/or standardizing the operating system to adhere to company policies and procedures.

### **That's where DeviceGuardian™ comes in.**

DeviceGuardian™ is a cybersecurity tool that provides real-time protection to mortgage companies and their computer networks. Once a mortgage company enrolls its computers and other devices into the program, DeviceGuardian™ provides the following services:

- Automatically scans for malware and virus threats
- Automatically removes or quarantines malware files
- Continuously monitors computers/devices for threats such as viruses and spyware trying to install themselves
- Alerts the administrator if real-time protection turns off. In such case, the computer's status changes to "at risk."

Whenever DeviceGuardian™ detects a potential threat, it alerts the mortgage company's administrator via email.

DeviceGuardian™ also helps mortgage companies manage system updates. The tool monitors and protects devices while it provides remote assistance.

DeviceGuardian™ tracks hardware and software inventory, and sets security policies such as device encryption. It does all this from a portal within the MortgageWorkSpace® platform, specifically designed for mortgage companies.

With respect to the banking industry's requirements for advanced password settings, all DeviceGuardian™ security passwords contain:

- A minimum length
- Alpha-numeric strands
- A minimum number of minutes of activity before it requires password input
- A maximum number of days after which passwords expire

DeviceGuardian™ also creates a system restore point before fixing malware issues. The system scans all downloads and attachments before downloading them from the internet and scans for application updates daily.

In addition, DeviceGuardian™ does the following:

- Schedules automatic updates at 3:00am
- Monitors user behavior
- Scans scripts
- Protects Windows, Android, Mac, and iOS devices
- Manages security patches
- Comes with an easy to use portal

When DeviceGuardian™ scans all downloads, it includes files that are automatically downloaded via Windows Internet Explorer and Microsoft Outlook® Express, such as ActiveX® controls and software installation programs. These types of files the browser itself can download, install, or run without human intervention. As a result, malicious software, including viruses, spyware, and other potentially unwanted programs, can download within these files and install without the user's knowledge.

DeviceGuardian™ also protects mortgage companies by monitoring all files and programs that start running on the company's computers, and then it alerts the administrator about any actions they perform and any actions taken on them. These tasks are important because malicious software takes advantage of the vulnerabilities in programs that the IT staff has installed. It uses the software installed to run malicious or unwanted programs without the user's knowledge.

For example, when a user starts a program that he frequently uses, he also may unintentionally start a spyware program at the same time. That spyware can run in the background without further assistance from the user and without the user's knowledge. DeviceGuardian™ monitors all programs and alerts the administrator if it detects suspicious activity.

DeviceGuardian™'s design meets the rigorous standards mandated by the Federal Financial Institutions Examination Council (FFIEC), the organization in charge of regulating mortgage companies, banks, and credit unions. DeviceGuardian™ keeps mortgage companies compliant with the Consumer Financial Protection Bureau's rules. It keeps data safe and enables mortgage company staff to perform at the top of their game from any device, anywhere.

Any questions about cybersecurity, malware or DeviceGuardian, please feel free to [contact us](#).

**(888) 422-3400**

**[www.myabt.com](http://www.myabt.com)**

#### **References**

1. [Kaspersky. usa.kaspersky.com](http://usa.kaspersky.com) Retrieved 31 January 2017.
2. [Bit9 + Carbon Black research document. www.carbonblack.com](http://www.carbonblack.com) Retrieved 31 January 2017.
3. [AnomALI. www.anomali.com](http://www.anomali.com) Retrieved 31 January 2017.
4. [clearswift. www.clearswift.com](http://www.clearswift.com) Retrieved 31 January 2017.
5. [hackmageddon. www.hackmageddon.com](http://www.hackmageddon.com) Retrieved 31 January 2017.
6. [Symantec/threat-report. www.symantec.com](http://www.symantec.com) Retrieved 31 January 2017.
7. [Channel Pronet Work/article. www.channelpronetwork.com](http://www.channelpronetwork.com) Retrieved 31 January 2017.
8. [NetIQ Security Statistics. www.netiq.com](http://www.netiq.com). Retrieved 31 January 2017.