

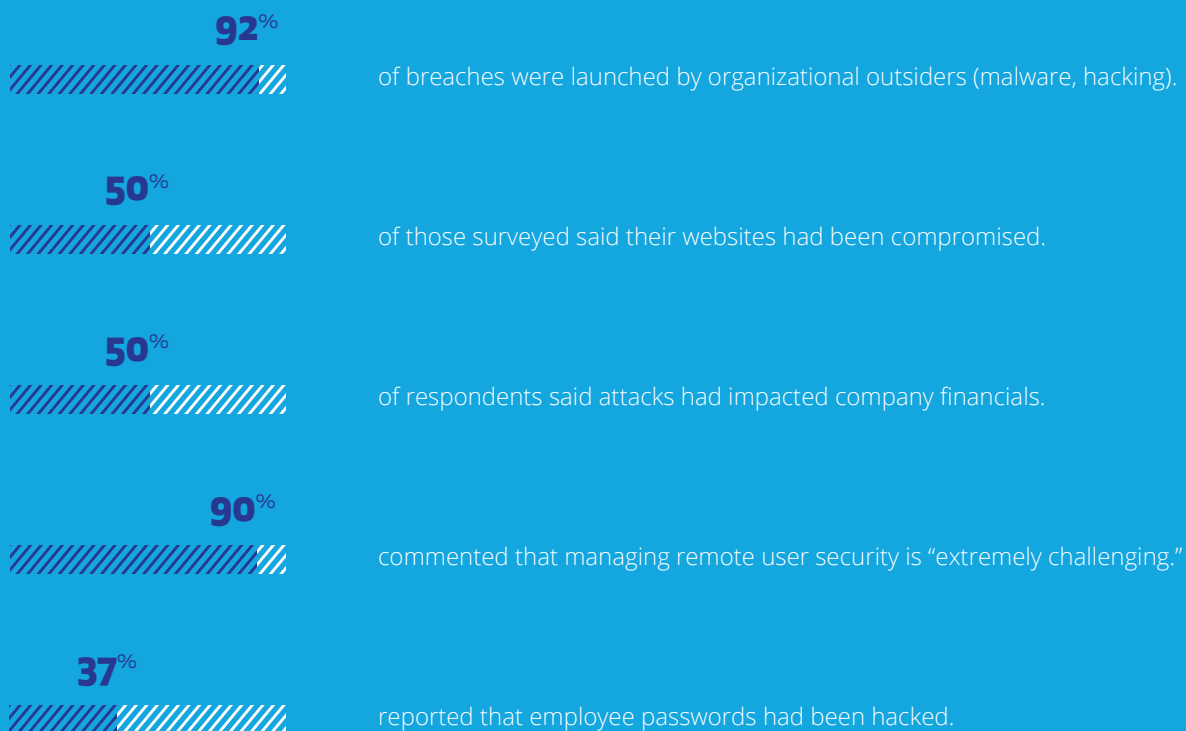
ADVANCED **THREAT DETECTION**

SECURING YOUR NETWORK
IN THE AGE OF THE REMOTE USER

Remote users

can introduce significant threats to your network. As employees, vendors and other business partners increasingly work from the road and remote offices—often using their own devices—the potential for disaster has grown exponentially. Banks and financial service institutions, defense contractors, government agencies, healthcare systems, multinational corporations and small businesses have all been all targeted.

Consider these statistics from the Verizon 2013 *Data Breach Investigations Report* and a recent Webroot survey of 500 web-security professionals:



Not only has the number of incursions soared, but also the nature of attacks has changed. In a January 2012 report, *Best Practices for Mitigating Advanced Persistent Threats*, Gartner notes that conventional signature-based security solutions cannot control advanced persistent threats (APTs), which typically establish an undetected and long-lasting base of operations on a network. The bottom line? Traditional solutions hit the wall quickly when filtering out problems, and neither proactive nor reactive approaches such as SIEM can see your remote users.

“ the nature of attacks has changed ”

To secure remote users, advanced threat detection (ATD) solutions are needed. Security software installed on endpoint devices is not enough to provide a reasonable assurance that they are malware free. ATD solutions should provide defense in depth through multiple detection methods—signature-based, heuristics, behavioral—and by utilizing multiple anti-malware engines to supplement the antivirus software installed on the endpoint. In addition, ATD solutions should report when a threat cannot be remediated or cleaned by the endpoint security solution.

The challenges you face

In securing remote users and your network, you face four challenges:

1

EFFECTIVELY DETECTING THREATS

The primary goal in securing your network against remote users is to ensure that a remote device is free of malware before allowing access to it. As a rule, it is possible to detect whether or not antivirus software is installed and activated on an endpoint, but there are two caveats. First, detection of installed antivirus software is generally performed through your secure remote access solution, such as SSL VPN, VPN or network access control (NAC), and integration with these solutions can be difficult to maintain. In order for newly released antivirus products to be detected on endpoint devices and properly reported to the secure remote access solution, firmware updates are required.

Second, no single antivirus scan engine is perfect. Virus signatures may be missing. Heuristics may miss a new virus, increasing vulnerability to a targeted attack. Behavioral analysis may fail to detect a problem. This means that detecting whether antivirus software is installed and enabled on the endpoint is not enough to indicate whether the device is malware free. The key to protecting your network against the constantly changing malware landscape is to scan endpoints with multiple antivirus engines.



2 DEALING WITH TIME CONSTRAINTS

Simply put, endpoint risk decisions must be made fast. Running a full system scan on endpoints at the time of connection is not an acceptable option. A reasonable assurance of device health must be obtained within seconds in order to preserve productivity.



3 PROVIDING NEEDED FLEXIBILITY

Many existing security solutions address specific use cases and user bases, which limits their usefulness in many contexts. A platform that provides near-real-time analysis is critical when managing a mobile workforce.



4 REDUCING SOLUTION FOOTPRINT

Remote device use is incompatible with downloading and installing a heavyweight endpoint security application. A lightweight client that utilizes cloud-based analysis, on the other hand, reduces the burden on endpoints, frees up memory and eliminates maintenance requirements.

Requirements of Advanced Threat Detection

Traditional signature-based antivirus engines and network-based security solutions are falling short. Critical threats that are not effectively detected by these solutions include:



Rootkits

Malware that activates at system boot-up—often before the boot-up process is complete—and make it possible to install hidden files, user accounts, and processes. Rootkits permit access to a PC or network and use the operating system to avoid detection and removal.

With increasingly sophisticated threats, rootkits must be deactivated completely before they can begin their work; otherwise it becomes almost impossible to remove them.

While many endpoint security applications can detect rootkit activity on the computer, they have difficulty remediating the threat. While they will continue to report detection, it may be unclear that the threat persists. Advanced threat detection solutions can help identify rootkits by looking at the detection logs of the installed antivirus to find repeated detections of the same threat, indicating that it persists and has not been remediated.


Keyloggers

A surveillance tool that detects every keystroke—including log files, email and IM—and sends it to a specified receiver. Often used to monitor employees' use of company equipment, keyloggers can also be embedded in spyware.

Individual antivirus engines have unreliable detection of the multitude of keyloggers in the wild. The value of an ATD's defense-in-depth is that it harnesses multiple antivirus engines, with each one likely to detect keyloggers that the others have missed.

	multi-scanning	AV Engine 1	AV Engine 2	AV Engine 3	AV Engine 4	AV Engine 5	AV Engine 6	AV Engine 7	AV Engine 8	AV Engine 9
ActualSpy	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗
FamilyKeyLogger	✓	✗	✗	✗	✗	✓	✓	✗	✓	✗
REFOG KeyLogger	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗
No Name KeyLogger 1	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗
Ardamax KeyLogger	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗
No Name KeyLogger 2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
No Name KeyLogger 3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
No Name KeyLogger 4	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗
Revealer KeyLogger	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓

Figure 1. Multiple antivirus engine scan capabilities enable identification of keyloggers that individual antivirus engines have missed.



Targeted attacks

Incursions targeted at a specific user, company or organization. Targeted attacks are designed to evade the existing security software and settle in, long-term, on a network. Examples include “social engineering” attacks that focus on user targeting as well as Zero Day threats that exploit undressed application vulnerabilities.

Advanced threat detection solutions should help mitigate the risk of targeted attacks by supplementing the installed antivirus software that may be evaded by the threat, as well as by identifying users that may need additional training for avoiding social engineering attacks.

Using multiple antivirus engines to supplement the installed antivirus software can detect threats that the single security product misses. Identifying threats that appear repeatedly on a user’s computer can signal that the user is repeatedly downloading malware.


ATD uses a defense-in-depth approach, including both static and dynamic analysis, to identify threats, and can detect potential infections that typical antivirus and security solutions miss. The ATD solution should provide detection for both threats that the existing security solution cannot detect, as well as for persistent threats that the solution cannot remediate.

Threats **missed** by installed antivirus software

No antivirus engine is perfect. While an endpoint should have installed antivirus software to catch most threats, ATD solutions provide additional protection against threats that the installed security solution misses. Using multiple anti-malware engines to scan files significantly increases the likelihood of detecting malware that the installed solution has missed, including targeted attacks that specifically intend to evade the installed software.

Threats the installed antivirus software **cannot remediate**

Further, an ATD can identify specific threats that are logged but not remediated by the existing security solution. In Figure 2, for example, an installed antivirus solution detects a particular malicious file repeatedly, indicating that the solution is not able to resolve the infection. This may be as a result of the user repeatedly downloading the malware (indicating that security and malware related training is needed), or it may be an indication that the antivirus solution is unable to fully remove the malware from the machine. The ATD solution can identify these scenarios and alert the administrator that additional manual actions may need to be taken to remediate the infection.



ANTI-MALWARE MONITORING

Endpoint Antivirus

VERSION 3.6.3.549

Real time protection is on

Virus definitions were updated within the last 3 days

The last full system scan time is not available

68 threats detected within the last week

Hide threat details ▲

THREAT NAME	Deal Slider
LOCATION	C:\Program Files (x89)\Bench\Updater\updater.exe
TIME FOUND	01/14/2014 14:01:05
TYPE	Virus
ACTION TAKEN	Couldn't determine what action was taken. File may still be dangerous!
THREAT NAME	Deal Slider
LOCATION	C:\Program Files (x89)\Bench\Updater\updater.exe
TIME FOUND	01/14/2014 17:53:28
TYPE	Virus
ACTION TAKEN	Couldn't determine what action was taken. File may still be dangerous!
THREAT NAME	Deal Slider
LOCATION	C:\Program Files (x89)\Bench\Updater\updater.exe
TIME FOUND	01/15/2014 11:44:10
TYPE	Virus
ACTION TAKEN	Couldn't determine what action was taken. File may still be dangerous!
THREAT NAME	Deal Slider
LOCATION	C:\Program Files (x89)\Bench\Updater\updater.exe
TIME FOUND	01/16/2014 08:01:59
TYPE	Virus
ACTION TAKEN	Couldn't determine what action was taken. File may still be dangerous!

Figure 2. Conventional antivirus product repeatedly detects the same threat—an indication that the antivirus solution has failed to remediate it or that the user needs security-awareness training.

GEARS

Advanced Network Security Management


As outlined above, an ideal ATD solution for remote users utilizes multiple methods to detect threats on endpoints and does so in a quick and efficient manner.

OPSWAT GEARS, a cloud-based network security management platform for IT and security professionals, incorporates all these features. GEARS utilizes cloud-based malware scanning with as many as 40 leading anti-malware engines to enhance threat detection on endpoints without needing to install a large application or perform virus definition updates before scanning. Further, to save time, GEARS scans only running processes on the endpoint rather than the entire system, providing an efficient and effective measure of the infection state of the machine.

GEARS also searches for repeated detection of the same virus by installed antivirus software to help identify unique persistent infection situations utilizing the existing security software. And with automatic updating capabilities, GEARS is able to analyze logs from newly released security software without requiring administrator maintenance.

In addition

to advanced threat detection for remote users and managed devices, GEARS



Identifies and monitors a variety of applications on [Windows](#) and [Mac](#) endpoints, including antivirus, hard disk encryption and public file sharing



[Automatically disables](#) public file sharing, [updates](#) virus definitions and [enables](#) firewall protection



Uninstalls non-compliant applications



Provides a [single pane view](#) into an organization's security and compliance status

GEARS offers significant visibility and control over network endpoints, devices and applications. This is particularly important for regulatory compliance such as HIPAA and PCI. The GEARS web-based management console makes it possible to quickly identify issues and to prioritize remediation tasks. And you can streamline and enhance compliance checks by integrating GEARS with network access control (NAC), IPSEC VPN, and SSL VPN solutions.

CASE STUDY

GEARS Integrated to Juniper Networks at a Large Global Bank

Because infected endpoints can unwittingly spread malware, an important part of any system administrator's network defense strategy is to ensure that all endpoints are healthy and protected before they can access the network.

Juniper Networks Junos Pulse SSL VPN and UAC assess endpoints that connect to Juniper Networks network security and access control gateways and appliances. The company's Host Checker includes predefined policies and rules that check for endpoint security software such as antivirus, anti-malware and personal firewalls running on Windows, Mac and Linux computers. Though this product is exceedingly robust, some customers require another layer of security—because of specific security restrictions or to provide a secondary check of endpoints without installed security applications. Integrated with Host Checker, OPSWAT GEARS rapidly scans endpoints, running multiple cloud-hosted antivirus engines to deliver defense in depth.

At a large global bank that employs 100,000+ people in more than 3,000 locations, hundreds of employees and partners are likely to remotely access its network at any one time. When users are denied access, GEARS runs as a custom solution integrated into Juniper Host Checker. If a device passes its scrutiny, the Juniper secure remote access gateway provides the necessary network access.

"Our organization has thousands of end users that rely upon our Juniper Networks SSL VPN infrastructure for secure remote network and resource access. We understand that it is challenging to maintain 100 percent detection of every antivirus product in the market from the moment a new antivirus product is released to the market. The extensibility and flexibility of Juniper's Host Checker to add custom checks like OPSWAT's GEARS enables us to provide our many users with increased usability, and secure network and resources access, while maintaining a high level of security for the bank's network."

-IT Director at the large global banking enterprise