WHITE PAPER

Eliminating the Blind Spot:

Rapidly detect and respond to the advanced and evasive threat

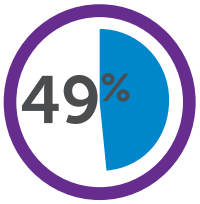
DELL SecureWorks

Executive Summary

Unfortunately, it's a foregone conclusion that no organization is 100 percent safe from intrusion. With today's threat actors continuing to evolve their tradecraft by employing more advanced and evasive techniques, it's all about mitigating risk and the potential reach of any intrusion. What options do concerned security leaders have to address this challenge? Security leaders should capitalize on opportunities to link network and endpoint visibility, and enhance detection while informing incident response – the endgame being reduced time to detect advanced threats and reduced effort required to respond.

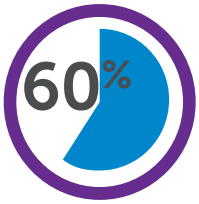
In this paper we will explore the benefits of combining advanced network and endpoint detection technology with the right people, process and intelligence for greater organizational visibility to detect, investigate and eradicate the threat.

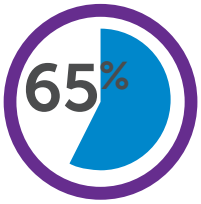
The Current Situation



Believe zero day attacks will be the most prevalent over the next three years[1]

Say the severity of malware infections have increased significantly[2]





Say attacks have evaded current preventive security controls[3]

SOURCES:
1: 2015 Global Megatrends in Cybersecurity: Ponemon Institute, Jan. 2015
2: The Cost of Malware Containment: Ponemon Institute, Jan. 2015
3: 2014: A Year of Mega Breaches: Ponemon Institute, Jan. 2015

Who Should Read This White Paper

- » CISO/CSOs
- » CIOs
- » CFOs
- » Directors of Security
- » Security Researchers
- » Security Architects

Why Traditional Security Fails to Stop Advanced and Evasive Malware

Some of today's most damaging cyberattacks utilize advanced and evasive malware used to target specific enterprises. These threats serve as beachheads for multiphase campaigns to collect and exfiltrate confidential data, including intellectual property, credit card and social security numbers, and protected personal information.

Advanced Threats

An Advanced Threat is:
A targeted threat. It may be 'off-the-shelf' and been seen before, or be a zero-day threat.

An Evasive Threat is:
A threat intentionally designed to evade existing security controls.

As preventative measures have become smarter, so too have the techniques used by threat actors to penetrate traditional cybersecurity defenses through use of:

- Morphing, encrypting and disguising existing malware files, so they cannot be detected by signature-based defenses.
- Developing custom malware for "zero-day" and targeted attacks that strike before signatures can be developed and widely distributed.
- Creating "evasive" malware that is intelligent enough to hide from some sandboxes and other second-line defenses.

Unfortunately, for security professionals, cybercriminals and hackers have time on their side. Even when security teams find an initial threat indicator, it often takes days, weeks or longer to trace the attack, analyze the threat, identify and quarantine all of the systems that have been compromised, and implement plans to remediate those systems. The longer that process takes, the greater the opportunity attackers have to achieve their goals, and the higher the cost of remediation.

46%[4] **55%**[4] **66%**[5]

SOURCES:
4: 2014: A year of Mega Breaches: Ponemon Institute, January 2015
5: The Cost of Malware Containment: Ponemon Institute, Jan. 2015

In a recent survey conducted by the Ponemon Institute, 46 percent of enterprises discovered breaches only by accident, while 55 percent were unable to determine the entry point of those breaches when they were discovered. Respondents conceded that 66 percent of the time they spend responding to malware alerts is wasted because they don't have the right threat intelligence to focus their incident response efforts.

These survey results tell us that most enterprises have one or more operational blind spots that lead to longer threat actor "dwell times."

The gaps in visibility are caused by a shortage of one or more of the following capabilities:

- Detection of advanced malware threats captured on the network, and accurate and timely forensic analysis of those threats.
- Rapid collection of security data from endpoints and the forensic analysis of that data.
- The application of up-to-date intelligence to accurately diagnose the threat and provide useful context to aid in forensic analysis.

While each of these capabilities serves a powerful purpose in its own right, combining capabilities amplifies an organization's ability to detect advanced threats sooner and reduce both the scope and effort required to respond.

Advanced Detection of Malware on Networks

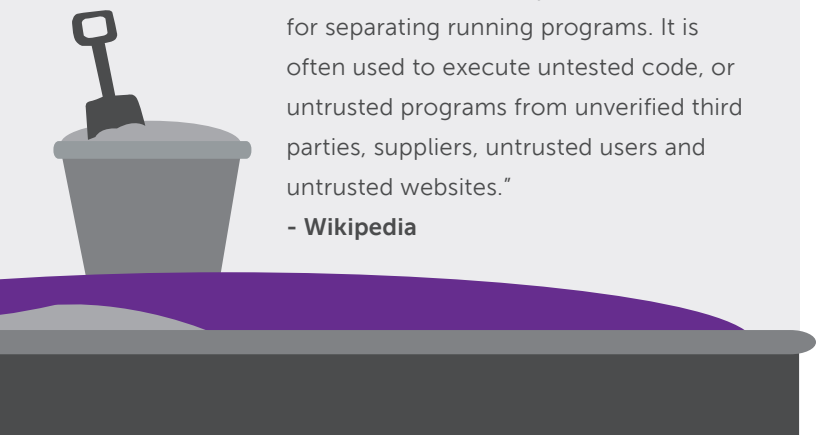
The Power of Advanced Malware Detection

Signature-based security measures such as antivirus software and intrusion detection/intrusion prevention systems (IDS/IPS) are useful for blocking threats that have previously known signatures to match or analyze against. However, detecting advanced, evasive and zero-day attacks at the network level does require adding an additional layer of security through technology into the environment.

This technology, generally referred to as Advanced Malware Protection, is advanced detection technology that typically utilizes sandboxing. With the right type of intelligence integrated into the sandbox technology, organizations can identify behaviors that indicate the tactics, techniques and procedures (TTPs) of known threat actors.

Utilizing integrated intelligence, sandboxing places isolated files (email attachments, web files, etc.) in simulated environments, allowing sandboxes to execute the files and observe for actions that suggest malicious intent (such as trying to change registry settings, access other systems on the corporate network or communicate with a "command and control" server outside the network).

What's in your sandbox?



"A **sandbox** is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third parties, suppliers, untrusted users and untrusted websites."
- Wikipedia

How Does This Eliminate a Blind Spot?

Advanced sandboxing technologies with embedded intelligence can:

- Increase threat visibility to the network.
- Act as an early warning system to detect advanced and evasive threats (including zero-days) that circumvent traditional signature-based defenses.
- Arm incident response and forensics teams with detailed information on the threat, its behavior and intent.

Limitations of Advanced Malware Protection

Not all sandboxes are created equal in design and effectiveness. Savvy threat actors have developed malware that tests for evidence of a sandbox, such as a virtual environment or a lack of human actions such as clicks and mouse movements. If the malware finds any of this evidence, it declines to perform any malicious actions. The malware remains idle until it is cleared by the sandbox, then "detonates" when it reaches its goal destination.

However, with next generation sandboxing technology, countermeasures are designed to detect these techniques with features such as full-system emulation. For example, the sandbox can generate clicks and mouse movements at the right time to simulate human interaction, thus tricking the malware into thinking it is on a live system.

Due to the changing nature of the threat, organizations should inquire as to the type of sandboxing technology employed and the efficacy of that technology against sandbox evasion tactics.

While advanced detection of malware on networks enhances detection capabilities and eliminates part of the blind spot, it does not address visibility into endpoints.

Advanced Detection of Malware on Endpoints

The Evolution of Endpoint Threat Detection

For many threat actors, endpoints such as servers, employee laptops and desktop computers, and mobile devices are the primary points of intrusion into enterprise networks.

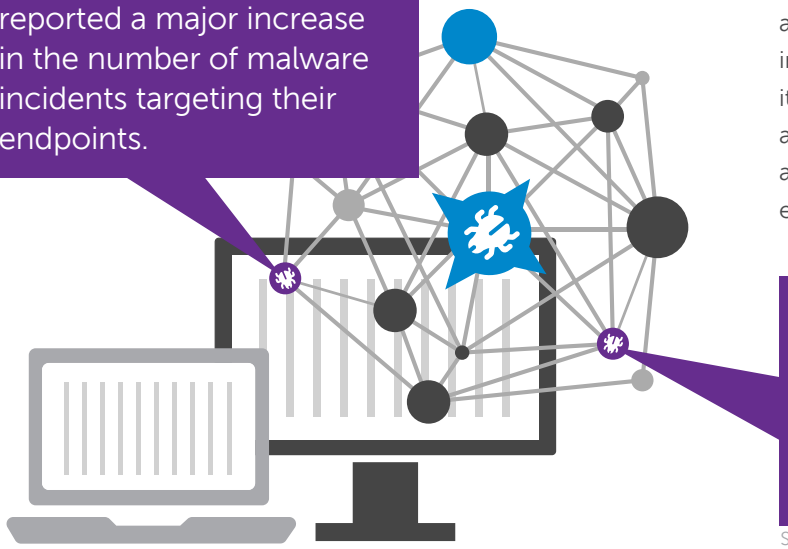
In a recent Ponemon Institute survey 40 percent of enterprises reported that endpoints had been the entry point for an advanced or targeted attack within the past year. The real figure is probably higher since it would include additional attacks that were never detected and, therefore, never reported.

Fortunately, endpoint threat detection technologies have rapidly evolved to monitor a wide range of actions on endpoints.

For example, they can track:

- Registry entries created, edited and deleted.
- Files created, opened, modified and deleted.
- Changes in process tables; for example, calls to processes frequently used by malware.
- Network connections — including connections to other systems on the corporate network and to unknown servers on the Internet.

44% of respondants reported a major increase in the number of malware incidents targeting their endpoints.



The real advantage of endpoint threat detection solutions is the ability to track and record the activities of malware that may have evaded or bypassed other network-based preventative measures. This includes encrypted and obfuscated malware, files transferred from USB devices, and malware that infected laptops and mobile devices when they were outside of corporate defenses (for example, on the home networks of employees). In this case, endpoint solutions go beyond detection to include forensic readiness and some response capabilities.

How Does This Eliminate a Blind Spot?

Acting like a "black box" flight recorder, endpoint threat detection collects comprehensive forensic data that empowers a capable analyst to accelerate incident response. Information, such as the original location of the breach, the attacker's lateral movement within the network, the specific systems that have been compromised and may be used to exfiltrate data to external servers, provides the building blocks of an accelerated response effort. With the specificity of information (the exact endpoint or endpoints affected, the nature of changes made on the endpoint, lateral movement, etc.) these endpoint technologies can provide, responders can more quickly respond to and eradicate the threat with much less effort required.

Limitations of Endpoint Threat Detection

Just like advanced malware detection for the network, not all solutions are equal. Endpoint technology is still developing in terms of detection, forensics and response capabilities as well as how the technology is deployed and managed in the environment. In addition, not all organizations are ready to deploy endpoint solutions because internal expertise is often lacking for their effective management.

40% said their endpoints had been the entry point for an Advanced Persistent Threat (APT) targeted attack in the last 12 months

SOURCE: 2014 State of Endpoint Risk, Ponemon Institue, Dec. 2013

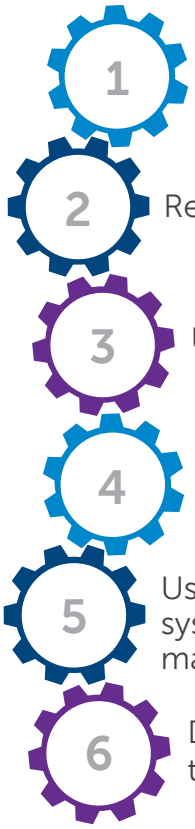
Considerations when implementing endpoint threat detection include:

- The endpoint threat detection solution should integrate easily with security processes; for example, solutions should allow security analysts to send unknown files automatically to an advanced threat detection (sandboxing) service for analysis.
- Endpoint data should be embedded with up-to-date threat intelligence based on the latest threat actor TTPs. This intelligence should allow for potential attribution to threat actors or threat actor groups.
- The organization should have analysts with the experience and skills to find critical clues contained in the vast quantities of data generated by endpoints. Paired up with intelligence, analysts can develop a much more complete picture of the threat, its operations and reach, which, in turn, fuels its effective remediation.

Unifying Advanced Malware Detection, Endpoint Threat Detection and Threat Intelligence

Advanced malware detection on the network and endpoint threat detection are powerful tools in themselves. When combined and layered with intelligence, they provide the type of end-to-end visibility that dramatically speeds up the detection of advance threats and the remediation of compromised systems.

Working together, they provide end-to-end visibility so an experienced analyst can:



1. Start with an initial threat indicator uncovered at the network or endpoint level, and determine if that indicator is associated with a known threat actor.
2. Research the tactics, techniques and procedures (TTPs) of that threat actor.
3. Use knowledge of the TTPs to find related threat indicators.
4. Construct a complete picture of how the attack was launched and carried out.
5. Use data collected to identify the systems affected and the changes made to those systems during the exploit in order to perform remediation quickly and in a focused manner.
6. Develop threat indicators and recommend changes in technology and processes that will protect against the attack in the future.

The Importance of People, Process, Technology and Intelligence

Advanced detection solutions are only one piece of the puzzle. As breaches over the last 18 months have stressed, security teams must aggressively integrate people, process and technology at every security defensive layer.

Carrying out investigations efficiently requires not only the right technologies and threat intelligence, but also the right people and processes. Note-- your capabilities are only as good as the threat intelligence you utilize. Threat intelligence is the catalyst that turns raw threat data into relevant, timely and actionable information that not only speeds up detection, but also improves incident response, forensics and remediation.

Additionally, analysts and incident responders need skills such as network analysis, endpoint forensics and malware reverse-engineering, as well as detailed knowledge of how threat actors construct and execute attacks. Processes need to be in place to collect, correlate, analyze and disseminate security data and threat intelligence.

To achieve inner security peace:

Conclusions

There is no shortage of threat actors out there that continue to evolve their tradecraft to evade traditional cybersecurity defenses. Consequently, enterprises not only face the challenge of implementing the right technologies for rapid detection, but must obtain the end-to-end visibility, detection and response capabilities required to quickly remediate.

Unifying advanced detection technologies for the network and endpoint with the right intelligence, people and processes empowers security teams to:

- **Reduce the time to detect.** Advanced detection capabilities at the network level and on endpoints allow organizations the opportunity to detect threats earlier.
- **Investigate alerts and diagnose attacks.** Combining alert reporting information with intelligence on threat actor tradecraft on the advanced malware with endpoint data provides a more complete picture of the threat and helps answer questions like: What was the entry point of the threat and when? Has the malware communicated with command-and-control servers outside the environment? What is it designed to do? What is the malware's purpose? How has the actor moved laterally within the environment? Were files and sensitive information exfiltrated to remote systems?
- **Identify true positives and reduce false positives.** Not all suspicious files detected on the network are dangerous or part of an attack. Network and endpoint threat detection can determine what files have actually performed malicious actions on systems and which can be ignored or investigated at leisure.
- **Isolate infected systems fast and focus remediation on systems and devices known to contain advanced malware.** Combining the analysis of malware with endpoint data makes it much easier to identify which specific systems were affected by an attack and the extent of changes on each affected system. Enterprises can quarantine infected systems quickly and apply the least disruptive forms of remediation consistent with eliminating the threat.

For more information, call (877) 838-7947 to speak to a Dell SecureWorks security specialist.
www.secureworks.com