Beyond Prevention: Why You Need Next-Generation Endpoint Security

Evolve your security strategy to keep up with changing threats

Threats have changed. It's time for your endpoint security strategy to do the same.

For decades, organizations have relied on antivirus products to defend against malware. The traditional approach was designed to secure the perimeter of an organization's network, fully focused on keeping known malware out. An antivirus product scanned files as they attempted to enter the network, determined whether they were clean or malicious, then decided whether to block them or let them through based on that analysis. These tools were effective and served their purpose at the time, but as the threat landscape and cybersecurity teams have evolved, preventative measures simply haven't kept up.

More sophisticated evasion techniques

While organizations have had decades to understand how traditional malware prevention tools operate, so have adversaries. As a result, malware authors have become very skilled at designing malware that can mask itself and evade detection. When the success rate of a specific type of malware declines, attackers create new variants. Their approach is dynamic and changes at a pace that static point-in-time tools can't keep up with. To build solutions that can overcome such dynamic adversaries, we have to understand how these attacks work and what evasion techniques are making them successful.

Contents

Some of today's common evasion techniques include:

Environmentally-aware malware

This technique looks for signs that the malware is being run within a virtual machine or sandbox environment, and changes its behavior to evade analysis. This includes delay tactics where files wait until they are scanned to execute malicious behavior. Another tactic requires user interaction; the files wait until after a certain number of mouse clicks, mouse movements, or the launching of a specific program by the end user to exhibit malicious behavior.

Lure documents

Lure documents are technically benign, but often hold enticing URLs linking to documents with malicious macros or embedded malware. An end user typically receives these documents through highly convincing, targeted phishing emails.

Domain Generation Algorithms (DGAs)

To keep malware fresh and effective, adversaries use algorithms to create a variety of domain names that conceal their traffic and evade detection. The goal is to generate so many domain names that it becomes impossible to block all of them. DGAs have typically been short-lived, but the average life span has expanded significantly—up to about 40 days.

Fileless malware

This type of malware runs completely in memory without writing any artifacts to the file system or registry. That is, unless the attacker wants to put persistent mechanisms in place, such as storing a command to re-infect a victim in a registry. The command is automatically executed when a system is booted. Fileless malware is harder to detect, and makes forensic investigations and incident response more challenging because permanent system changes are kept to a minimum or avoided altogether.

Polymorphism

With this technique, a malware sample can change itself to evade systems looking for specific files or patterns within a file. The malware can accomplish this in a variety of ways, including rearranging where certain parts of the code are stored within itself, encoding or encrypting portions of itself in various ways, or modifying noncritical portions of itself, either by changing certain values, or adding and removing portions.

Piggybacking

This is a way for malware creators to install additional, usually unwanted software along with a desired piece of software. While the ability to bundle software may be legitimate and intentional on the part of the software authors, malicious actors can deliver their malware to users through what is known as a supply chain attack. In this scenario, attackers gain control of a portion of the legitimate software's development or release process, which allows them to bundle their malicious code within it, unbeknownst to the software's authors and users.

How the industry responds

As soon as the industry discovers a new threat type or evasion technique, it sees an opportunity to promote a shiny new product. The product works for a while, until the next new threat pops up and creates the need for yet another tool. As a result, organizations have fallen into the cycle of implementing products that focus completely on the latest method of protection instead of investing in comprehensive solutions. Fast forward a few years: organizations are finding themselves drowning in endpoint security tools that don't speak to one another, require management by a large number of skilled IT personnel who can be hard find, and demand ever-increasing funding that can be even harder to come by.

What's needed: a complete transformation

So how can organizations get out of this cycle and start defending themselves from advanced threats more effectively and efficiently? What's needed is a truly transformational change in how we detect malicious activity. Defenders need integrated solutions that go beyond the limitations of traditional point-in-time technologies. They need the next-generation of endpoint security.

Next-Generation Endpoint Security (NGES) is essentially the convergence of multiple technologies providing protection, detection, and response capabilities in an integrated solution. In this model, detection and response are no longer separate disciplines or processes, but extensions of a cohesive, continuous approach. When these components are brought together into one integrated system, organizations start to experience greater endpoint security efficiency and effectiveness.

Next-generation endpoint security capabilities and features include:

Continuous detection and visibility

While prevention still plays an important role in eliminating a majority of potential threats, the key is seeing prevention capabilities as a piece of the solution, rather than relying on them alone. By applying continuous detection technologies after the initial prevention phase, efforts to stop advanced malware become more effective and efficient. A continuous approach is foundational to the next-generation endpoint model and spurs a spectrum of additional innovations.

Next-generation innovations	
Retrospective detection	Detect and remediate malicious activity that evades initial detection through continuous tracking and monitoring of files after point-of-entry.
File trajectory	Identify patient zero and see file propagation over time throughout the environment to improve visibility and reduce the time required to scope a malware breach.
Elastic search	Quickly understand the context and scope of exposure to indicators of compromise or malicious applications using an unbounded search across file telemetry and collective security intelligence data.
Device trajectory	Quickly understand the history of events leading up to and following a compromise, and identify vulnerable applications.

Next-generation innovations	
Prevalence	Uncover previously undetected threats seen by a small number of users by identifying executables that exist on only a few hosts. This uncovers targeted, advanced, persistent threats that could otherwise gain access to the broader network.
Outbreak control	Gain control over suspicious files or outbreaks, and remediate an infection without waiting for a content update.

Advanced analytics

To detect attacks as they move laterally through the network and across endpoints, defenders need solutions that automatically look for Indicators of Compromise (IoCs). These solutions must also find more subtle and advanced behaviors that are indicative of an incident. With big data analytics and the use of continuous capabilities, security teams can identify patterns and IoCs as they emerge and focus efforts on the threats with the greatest potential for damage.

Informed investigations

Without the context and capabilities of a continuous approach, investigations often involve painstaking attempts to track down breaches with little contextual evidence. Often the hardest questions to answer is where to start. With next-generation solutions, investigations become faster, more targeted, and more productive. Security teams are armed with a better understanding of the point of entry, scope, and root causes of infection, so they can begin tightly focused investigations into breaches based on actual events.

Efficient containment

Containing malware can be overwhelming if it means having to reimage every potentially infected endpoint. Point-in-time technologies are blind to the chain of events and contextual information that goes along with it, and the ability to surgically contain malware isn't even within the realm of possibility. When increased visibility is coupled with the ability to target specific root causes, stopping an outbreak becomes fast and easy. By preserving detection and telemetry data, threats can be contained at many different points along the attack pathway, and the initial infection gateway can be closed to prevent future attacks.

Relevant reporting

As security increasingly becomes a boardroom discussion, reports should fuel these conversations by including actionable dashboards and trends that highlight business relevance and possible risks. Although point-in-time technologies can provide dashboards and risk relevance, they typically require additional product integrations to sift through and correlate the large amounts of event data. Next-generation reporting uses data to provide context and prioritization when and where organizations need it most.

The importance of an integrated security architecture

As important as each of these innovations are on their own, combining them in an integrated workflow magnifies their real impact across malware detection, monitoring, analysis, investigation, and containment.

Endpoint solutions capable of sharing and correlating threat intelligence with other security tools across the network create a force multiplier for security teams. Integrating endpoint tools with routers, network IPS, firewalls, web proxies, and email gateways creates a security ecosystem that can respond systemically. A fully integrated security architecture has faster, more comprehensive protection capabilities.

Conclusion

To effectively combat today's advanced threats, organizations need a solution that provides deep visibility, context, and control to prevent breaches. Moreover, if malware gets in, this solution has to quickly detect, contain, and remediate it. A continuous approach to endpoint security helps to enable key areas of innovation that can battle advanced threats that target the endpoint. This includes:

Continuous monitoring and analysis

With a continuous approach, detection becomes more effective, efficient, and comprehensive. This approach optimizes behavioral detection methods like sandboxing, captures activity as it unfolds, and shares intelligence across detection engines and control points.

Automated advanced analytics that looks at behaviors over time

When your security uses advanced analytics and continuous capabilities to identify patterns and IoCs as they emerge, you can focus your efforts on the threats that matter most.

Investigation that turns the hunted into the hunter

Transforming investigations into focused hunts for threats based on actual events and IoCs gives security teams a fast and effective way to understand and scope an attack.

Truly simple containment

Breaking the attack chain is fast and effective with the level of visibility that the continuous approach provides, combined with the ability to target specific root causes.

Actionable, contextual dashboards

These dashboards base reports on the comprehensive collection and advanced analytics of file and telemetry data across control points. The dashboards then overlay these with contextual information, highlighting trends, business relevance, and the impacts on risk.

Cisco® Advanced Malware Protection (AMP) for Endpoints provides next-generation endpoint security that empowers organizations to protect themselves from today's advanced threats.

Ready to see next generation endpoint security in action? Get started now with our 2 to 4-week trial at no cost to you.

C11-740006-00 12/17