tripwire

WHITE PAPER

Threat Prevention is Foundational

How proper foundational controls help block today's advanced threats

FOUNDATIONAL CONTROLS FOR SECURITY, COMPLIANCE & IT OPS

With the growing number of successful security breaches in recent years, the effectiveness of traditional threat prevention has gotten a bad rap. Clearly, if bad actors are getting through, prevention simply isn't working… right? Not necessarily.

As a result of that assumption, the conversation has started to shift, with some voices in security declaring that "detection is the new prevention." Why? Simply put, this emerging opinion states: Because the industry can't prevent attackers from getting in, it should instead focus on real-time detection and incident response. With so many recent instances, the probability of attack seems to be approaching 100%, fueling new technologies designed to detect and quickly remediate malware.

It's not surprising. Most signature-based malware solutions were developed in response to a very different threat landscape, one in which threats moved much more slowly and were much less sophisticated. With these defensive technologies, the security industry needs to know something about an attack and then write a signature or rule to protect against it.

In today's threat landscape, attacks are constantly mutating to evade security solutions and companies face an increasing number of zero-day threats.

But make no mistake, prevention is a necessary part of your security arsenal to ensure cyber integrity. So, to increase its effectiveness, a "back to basics" focus can help you assess and reduce the susceptibility of attack. This foundational approach to prevention no longer needs to understand the attack. It focuses on behavior, rather than indicators of compromise, so that it can protect against zero-day threats. Foundational prevention also reframes the challenge—focusing not only on keeping the bad guys out, but also on limiting their subsequent actions, including any damage they might cause.

It's a subtle, but critical shift. The benefit to foundational prevention over threat identification is that it goes beyond simply trying to stop cybercriminals from accessing corporate networks and systems; it also focuses on disrupting criminal activities. So, even if attackers do get in, this "new-school" prevention works to make sure they leave empty handed.

The landscape has changed and new tools are available to help you keep pace with these changes. In *Malware Is Already Inside Your Organization; Deal With It*, Gartner analysts state that "preventive controls to 'harden' the endpoint are highly effective and should be revisited by security organizations."[1]

In this white paper, you'll learn:

- Why threat identification and remediation alone is no longer effective in today's threat landscape
- How foundational prevention can help protect your organization against unknown threats
- And what you should look for when considering foundational prevention solutions

Why Threat Detection Alone Doesn't Work In Today's Threat Landscape

In public health circles, there's a parable that is frequently told to emphasize the importance of prevention in addition to merely treating problems. In the story, villagers are fishing when they see a person coming down the river, struggling to survive. They help the person, and soon another comes down river, and another. The villagers get overwhelmed spending the rest of the day rescuing people from the river.

Eventually, the villagers decide to head upstream to find out why so many people are falling into the river. What they find is a treacherous overlook without any protection to keep people from falling in. Ultimately, the village leaders decide to build a protective barrier at the overlook. Some people may still fall in, but there are many fewer victims to rescue.

So, what does this have to do with your cybersecurity stance?

Threat detection alone is a "downstream" approach to security—very reactive. But as this parable shows, an "upstream" approach is also needed to address the root cause—and that is foundational prevention.

Applying this example to security, a narrow threat identification approach would require that the villagers know exactly why people are falling in the river before they can venture upstream. This means interviewing survivors, cataloging their injuries and then developing an action plan…in advance. Because of the speed, specificity and stealthy nature of attacks in today's threat landscape, detection and remediation alone isn't a model that works.

Much like the fishing villagers, your team can quickly become overwhelmed if they're responding to attacks as they come – even the best-trained team. Preventing people from "falling into the river" in the first place is a smarter approach from both a security and resource management standpoint.

The Speed Of Attacks

More than a decade ago, the e-mail based ILOVEYOU virus represented a game-changing moment for the security industry. It moved like lightning across the Internet, infecting tens of millions of computers through users' files and address books before security experts could respond. At the time, it spread faster than any other e-mail worm, since only a few users had to open the attachment to generate millions more messages that eventually crippled servers and overwrote millions of files on

computers in each successive network. Today, the speed and number of attacks continues to challenge enterprises (see examples in "Attack Pivots" below).

As new software vulnerabilities are discovered, the criminal underground is organized to respond quickly. For example, in the week following news of the Heartbleed vulnerability, IBM Managed Security Services witnessed more than 300,000 successful attacks against its customer base in a single 24-hour period.[2] Old-school prevention technologies that use blacklisting and other pattern-based techniques simply can't respond quickly enough in today's threat landscape.

Attack Pivots

Old-school prevention approaches also struggle when confronted with today's advanced persistent threats. The challenge is that there must be a "patient zero," the first victim of an attack. Once patient zero is identified, new protections can be developed and released to help stop similar patterns of attack. However, advanced persistent threats often leverage highly customized malware designed to infiltrate a specific target. In essence, there is only a patient zero—a single victim—making traditional blacklisting and pattern-based approaches irrelevant.

Additionally, many attacks that result in successful data breaches simply exploit known (and still unpatched) vulnerabilities in order to gain a foothold. Attackers rely on well-known, tried-and-true methods. In fact, the Verizon DBIR has reported for many years that upwards of 90% of attacks were successfully executed because of known vulnerabilities or misconfigured systems. The latest attacks solidify that point:

» WannaCry—Ransomware attack via unpatched vulnerabilities

» Verizon—Misconfigured server

» Equifax—Unpatched vulnerability

» Dow Jones—Misconfigured server

In each case, the attacker broke into their target, then pivoted to the data theft, ransom, or destruction they are came for.

The Stealthy Nature Of Attacks

Cybercriminals now have arsenals of sophisticated tools to draw from as they work to bypass security technologies and penetrate their targets. Malware typically comprises a comprehensive suite of capabilities that enable attackers to remotely control systems, steal corporate data and evade detection.

As a result, it's become a game of chess—while organizations have deployed multiple layers of security designed to keep cybercriminals out of their networks, cybercriminals continually find ways to circumvent many old school prevention solutions:

» Zero-day threats can easily bypass antivirus/antimalware solutions

» Malicious activity embedded within legitimate application processes enables attackers to sidestep host-based prevention systems

» Social engineering paired with sophisticated malware has enabled cybercriminals to circumvent most authentication systems, including two-factor and step-up authentication solutions

Once inside, cybercriminals often hide in plain sight, obscured by the "noise" of millions of alerts as they conduct reconnaissance and work to escalate their privileges. In fact, following one major security breach, researchers found that the security team received alerts at all key junctions of the attack: when criminals had infiltrated the network, when malware was installed, when credit card numbers were moved to another server within the organization, and finally, when credit card numbers were exfiltrated.[3] However, those warnings were lost among the noise of thousands of security events. This isn't uncommon—IBM Security X-Force researchers have found that the loss of intellectual property often happens in the first two hours of an attack; however, enterprises typically don't detect the attack until days or months later.

Why are these holes left open? There are several prevailing theories:

1. That many cyber-protectors are focused on chasing the next malware threat, rather than nailing down the basics. As explained above, threat actors often take the path of least resistance right through the open door of an unpatched vulnerability (the upside being, if they run into much resistance, they'll frequently move along to find an easier victim).
2. That there are simply too many holes to plug; the tools designed to warn us of danger overwhelm the protectors with unprioritized security data.
3. That organizations are facing a skills gap, and struggling to find staff with the training needed to analyze the latest threats. Without these necessary skills, some staff are left wondering what to do, or believe that the "easy basics" can be done later or aren't "cutting edge" enough to bother with.

These bad actors are furtive, fast and focused, effective at throwing numerous victims "into the river." The situation calls for a systematic, dynamic, preventive defense at the front end of your cybersecurity strategy.

> *Research found that dwell time—the amount of time attackers may go undetected inside a network—can be as much as 225 days.*[4]

How Foundational Prevention Is Different

If you're like most security professionals, you probably feel positively inundated with the volumes of material made available to you about the challenges of enterprise cybersecurity and the serious consequences of malicious hacking to business, governments and society. Quite frankly, the variety of tech tools and security options are dizzying—it's hard to know where to start. You need a simplified guide to the numerous frameworks and security regulations out there to cut through the noise and hype

around securing today's modern enterprise—a foundation to build on.

So, the solution rests simply in making sure that your security practice is built on a solid foundation of controls. Surprisingly, these controls are not rocket science, nor are they cutting-edge, hot new technology from a single security vendor. They're simply the basics that all enterprises must deploy to answer these three questions:

1. How do I know which systems are on my network?
2. Can I harden them to reduce my attack surface?
3. How do I know when something has changed on them?

> *This is why it's called "foundational" prevention—it's literally the base tactics you should be building your cyber defense on.*

But, what are these foundational controls? They include:

1. Asset Discovery
2. Security Configuration Management
3. File Integrity Monitoring
4. Vulnerability Management
5. Log Management

With foundational prevention provided by these controls, the villagers don't need to understand why people are falling into the river before racing upstream to try to stop them. But, what makes foundational controls different from all the others available? Three significant strategies:

1. A focus on reducing the attack surface

The "attack surface" refers to all the ways that an unauthorized user can get into your systems—the more entry points you have, the larger your surface. You can reduce your attack surface with the following foundational controls:

Inventory of Authorized & Unauthorized Devices
Make sure you know which devices you have

This straightforward control level-sets your operating environment, and helps to differentiate between authorized and unauthorized (often BYO) devices in the inventory.

Inventory of Authorized & Unauthorized Software
Make sure you know what software you have

Understanding software inventory sounds easier than it is in actual practice. License agreements can be complex, and the ease with which software can be downloaded from the Internet (whether illegal, compromised copies or well-meaning employees installing/updating software on their own) makes a software inventory generally quite challenging. For the sake of efficiency this should be tackled in concert with hardware inventory as described above.

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Configure your systems properly

The systems in scope with this control include mobile devices, laptops, workstations, servers and other devices. The reference to proper configuration focuses on security properties such as making certain that good decisions are made to turn off unnecessary services and properly change defaults, from administrative privileges to camera and microphone access.

By focusing on the foundational controls rather than the attack, new-school prevention solutions are poised to more effectively protect endpoints, prevent infection and disrupt data exfiltration. But even with a reduced attack surface, you must also administer the other preventable factors that leave you susceptible to a breach, like balancing an overwhelming amount of data with limited time, resources, talent or skill.

2. Dynamic and active intelligence

Implementing foundational controls is meant to complement, not replace, threat detection and remediation. As an integral element of the security lifecycle, foundational solutions are also closely integrated with detection technologies to help improve their effectiveness. By sharing endpoint telemetry and attack forensic data with security information and event management (SIEM) solutions, these solutions can help reveal key indicators of both vulnerability risk and compromise, and help security teams more quickly and accurately respond.

Continuous Vulnerability Assessment
Check for and fix vulnerabilities continually

Every cybersecurity professional agrees that a major challenge in the industry involves keeping up with all the vulnerabilities identified in real time across the globe. Sadly, no shortcut exists to constantly maintaining vigilance around such vulnerabilities, and for taking steps to mitigate relevant ones quickly.

Maintenance, Monitoring, and Analysis of Audit Logs
Pay attention to your audit logs

Most systems in the enterprise generate useful log output that contains useful information about potential security attack indicators. Security teams must pay attention to these logs and use them in conjunction with tools that are designed to analyze log information, to provide relevant, actionable guidance to management teams.

3. A multi-layered approach

With old-school prevention, enterprises had to implement multiple layers of overhead to search for possible malware at every juncture—within e-mail, in downloads, and on websites. However, foundational prevention offers an integrated, multi-layered approach that seeks out potentially malicious behavior wherever it is. As a result, enterprises can easily extend this protection to new types of attacks without additional overhead.

Email and Web Browser Protections
Implement a program to protect email and web browsing

Since e-mail and web browsing are the two most service fundamental components in modern IT environments, it stands to reason that a good cybersecurity program would have explicit focus and attention on these activities. Web browsers in particular must be kept up-to-date with the latest bug fixes.

Malware Defenses
Make sure you run anti-malware software

This seems obvious, but it is surprising how many organizations do not have uniform anti-malware defenses across their inventory of systems. Certainly, anti-malware software has taken reputational hits with the success of variants from malicious actors. Nevertheless, the control still plays an essential role in cyber defense.

Limitation and Control of Network Ports, Protocols, and Services
Limit what's allowed on your network

The establishment of security policy rules that prohibit unnecessary services is one of the oldest concepts in information security. Such minimization of services at the network level makes it harder for hackers with scanners to find open ports and listening services through which to gain entry to the enterprise.

The Benefits Of Foundational Prevention

Foundational prevention makes sense, as it empowers your business to get upstream on threats instead and minimize the number of victims "falling into the river." The approach takes you back to basics—monitoring devices, software, and users—to ensure that even if attackers get in, it's not because you left a door or window open.

Foundational prevention is like repairing footbridges and adding sturdy guardrails to the river bank.

So, what's in it for your organization? Peace of mind. The adage "an ounce of prevention is worth a pound of cure" has been a guiding principle for everything from preventive maintenance to preventive healthcare. And across industries, organizations have found that it's usually less expensive to implement preventive measures than it is to recover from an event. And cybersecurity is no exception.

The point is this: While detection is critical, even the most rapid response usually occurs well after the criminal has already stolen significant assets or caused irreparable harm. And even if an incident is detected early, the costs required to address any losses can still add up. In its 2014 Cost of Data Breach Study, the Ponemon Institute estimated the average cost of a data breach reached $3.5 million.7 This includes investigation, remediation and legal costs, along with fines.

This is where foundational prevention solutions shine. They can:

» Leverage existing resources and skill sets in many cases, making your existing investments more efficient and effective

» Contribute to a holistic threat stance, covering the blind spots left by old-school prevention or detection-only based systems

» Deliver the flexibility to adapt and change as the threat landscape does

» Ensure that you have greater awareness of your systems, including changes to them

» Provide intelligence regarding unusual behavior, and vital insight that can be used to help improve detection analysis and streamline remediation processes

» Assist in hardening your system to reduce your attack surface

» Help minimize the damage and reduce the associated costs by aiding to block the exfiltration of data even when attackers find a way to evade other security layers

Conclusion

It's not surprising that many enterprises have grown skeptical of the value of prevention given the surge in security breaches. On the surface, it would appear that prevention simply doesn't work. The issue, however, isn't with prevention. It's with the old-school approach.

There is still value and purpose to threat prevention. What must change is how your enterprise approaches it.

Instead of focusing on stopping the bad guys from getting in, relying on known threat patterns, and finding a patient zero in order to identity threats, foundational prevention recognizes that today's and tomorrow's threat landscape is dynamic. It reframes the challenge to not only keep the cybercriminals out, but also to limit the damage if they do get in. By recognizing that the greatest danger—and greatest loss—comes from unknown threats, foundational prevention offers a multi-layered approach that focuses on the root causes of a breach, rather than the attack itself.

Lastly, foundational prevention supports and enhances other security measures. It understands its role as an integral part of a strong security ecosystem, providing critical intelligence that bolsters detection and remediation–while increasing efficiency and saving your enterprise money.

Is there a single vaccine or silver bullet that can protect your enterprise? As much as one wishes, that will never exist. But prevention remains a critical component in the security lifecycle, and new-school foundational prevention offers a host of benefits and capabilities that help companies preempt attacks and safeguard their data.

References

1 Peter Firstbrook, Neil MacDonald, "Malware Is Already Inside Your Organization; Deal With It," Gartner [Research Report], February 12, 2014, retrieved from: https://www.gartner.com/doc/2665320/malware-inside-organization-deal-it

2 IBM (September 2014), IBM X-Force Threat Intelligence Quarterly, 3Q 2014 [Trend Report], retrieved from: https://media.scmagazine.com/documents/90/ibm_x-force_quarterly_report_22415.pdf

3 The Ponemon Institute (December 2013), The State of Advanced Persistent Threats [Research Report], retrieved from: http://informationsecurity.report/Resources/Whitepapers/b92cfb99-1e2b-4c3d-9803-4720b7bb0d36_state-advanced-persistent-threats-pdf-6-w-1053.pdf

4 The Ponemon Institute (May 2014), 2014 Cost of Data Breach Study: Global Analysis [Research Report], retrieved from: https://www.ibm.com/security/data-breach

WPTPF1j 201712