DEC. 2015

Next Generation Security with Endpoint Detection and Response

WHITE PAPER

Table of Contents

Endpoint Compromise a Sad State of Reality 3

Traditional Endpoint Anti-virus Isn't Getting It Done 4

The Rise of the Sandbox 5

True Next Generation Endpoint Security with Hexis HawkEye G 6

About Hexis Cyber Solutions 7

Endpoint Compromise: A Sad State of Reality

It's fairly obvious to anyone these days that almost any business or organization, regardless of size, is a potential target of cyber attackers. Any organization that collects personal information, data or payments is now under attack from groups looking to steal that very same information. The headlines are riddled almost daily with tales of new victims, with groups as diverse as Sony Pictures, T-Mobile and JP Morgan Chase joining the ranks of the breached. That's just the tip of the iceberg. For every attack against a large enterprise that makes the news, there are hundreds that don't, and it's a near certainty that many organizations have their security breached right now and just have not detected the threat.

Five Stages of An Advanced Persistent Threat:

1) Recon
Hackers case the network and possible employee access.

2) Exploit
Based on reconnaissance, hackers attack weak access points, often a low-level endpoint.

3) Discover
Bad guys poke around to find targeted data.

4) Propagate
Malware steals the valuable data, exfiltrates to hacker command and control center.

5) Sustain
Attackers hide and wait to steal again.

Of the known attacks that were successful, many share the common theme that the initial breach of security arrived on a network through a compromised endpoint. Many advanced persistent threats (APTs), the tool of the modern attacker, are designed to first compromise a low-level endpoint within an organization, establish contact with command and control capability, move laterally deeper into the network to elevate privileges with the goal of slowly stealing targeted data or opening up holes for more advanced malware to enter.

As such, the current focus of many organizations is next generation endpoint protection. Gartner classifies next generation endpoint products as part of the Endpoint Detection and Response (EDR) category. This is an interesting categorization by Gartner because it emphasizes the ability for these products to actually respond to threats, something that not every so-called next generation endpoint protection solution is able to accomplish. Responding to and stopping APTs at the endpoint, before they can move to the core network, will eliminate threats before they become a real problem. It can also reduce the burden on overloaded perimeter defenses like Next Generation Firewalls and Intrusion Prevention Systems, especially if attackers specifically seek to overwhelm them to make it easier for malware to slip past.

But not all endpoint protection is created equally. A true next generation solution needs to easily integrate with existing security controls. It also needs to achieve three main goals to ensure APTs don't sneak inside.

Specifically, advanced next generation endpoint protection needs to:

1. **Detect** all threats, especially previously unknown ones, based on several factors including the analysis of endpoint behavior
2. **Verify** that detected threats are actually malicious, leveraging security analytics to correlate endpoint and network activity, and leverage threat intelligence feeds and other threat indicators for verification.
3. **Respond** to threats at machine speed before they do damage. True next generation endpoint protection must have the ability to automatically respond to threats using countermeasures to surgically remove and/or contain threats before they do damage. Countermeasures like killing processes and restoring registry keys can eliminate threats without any impact on the user – and without requiring a full system restore or downtime.

Traditional Endpoint Anti-virus Isn't Getting It Done

In its most primitive form, endpoint protection took the form of anti-virus (AV) software installed on endpoints throughout networks. Many corporations have rules in place that restrict any endpoint from joining their networks unless anti-virus protection is present and up to date.

For an individual user, there is nothing wrong with the signature-based protection that anti-virus offers, but it does take up valuable system resources with the need to run constant scans, and requires a budget for continual support. However, for an endpoint that is part of a network, especially one that faces constant attacks, traditional AV protection simply isn't good enough.

For one, AV is nearly worthless against the unknown nature of the threats presented by many APTs. There have even been some recent studies that show that anti-virus is even doing a less-than-perfect job against known threats. Anything less than catching 100 percent of all threats on an endpoint means that it can become the launching point for an APT to get inside a network. And attackers are very good at finding that low-hanging fruit. In fact, most advanced hacker groups write their APTs to specifically get around the most popular versions of anti-virus protection.

Anti-virus is also poor at integrating with the existing security offered by Security Operations Centers (SOC). Most endpoint anti-virus solutions treat each endpoint as its own entity. It might send back reports to SOC teams if it detects a virus, but that too can be exploited by clever attackers by purposefully triggering alerts on some machines while slipping the APT quietly into others. This distraction technique sometimes actually works better for the attackers if known anti-virus programs exist on endpoints.

One interesting point about anti-virus is that most government agencies, and many heavily-regulated organizations within certain industries, still use anti-virus due to compliance regulations. But compliance does not equal security. It's worth noting that quite a few organizations are switching over their anti-virus programs to free versions, which still allows for compliance within most industries. However, the money saved by migrating to a free program can then be spent on true next generation endpoint protection for a perfect marriage of compliance and actual security.

The Rise of the Sandbox

To bolster endpoint defenses, some companies began to rely on sandboxing. In sandboxing, endpoint environments are emulated on the network as virtual machines. Programs are executed on the sandbox and behavior is observed. Once a program is deemed to be bad, a signature is created blocking potential infections from that point. This protection is behavior based, as opposed to the signature protection offered by anti-virus, and is more effective at detecting unknown threats.

When sandboxing first came out, it was seen as the silver bullet for advanced threat protection. But, very advanced threats are now being programmed to detect if they are inside a sandbox or an actual endpoint environment, and behave differently depending on the environment. For the most part, they behave as normally as possible while being observed in the sandbox, only revealing their true nature after being placed into a real environment. Some threats are also being programmed with exceptionally long call functions, where they simply wait for a very long time, sometimes an hour or more, before trying to laterally move within a network or call back to command and control servers. In many cases, this can circumvent sandboxing which might have already approved the program and granted it some level of access.

Problems also arise because the sandbox doesn't always completely mirror the actual client environment, so it's possible that the sandbox is not accurately simulating the endpoints it is supposed to be protecting. That means that it might not catch every threat, even if attackers aren't specifically exploiting this increasingly known vulnerability.

Another problem is "ghost alerts" or false positives which can easily overwhelm even large teams of people monitoring the endpoints. This happens when the sandbox issues an alert based on the virtual environment, but then the human responder doesn't find anything wrong with the physical client. This alert chasing can waste a lot of time, and allow the real threats to slip past unnoticed.

True Next Generation Endpoint Security with Hexis HawkEye G

Only HawkEye G® offers the three capabilities that make up true next generation endpoint protection, while also seamlessly integrating into your existing security infrastructure. HawkEye G can detect, verify and respond to any threat against endpoints, even previously unknown ones, and can kill processes, restore registry keys and surgically remediate an endpoint without disrupting user activity, and without the need for a full system restore.

HawkEye G is easy to deploy in organizations of any size, even very large ones geographically distributed at multiple locations. Lightweight HawkEye G Host Sensors are easily pushed out to endpoints, which can also be located at multiple dispersed locations. The Host Sensors are seamless and invisible to users, and don't tax either the system resources of the endpoints, or the network connections that link them.

Host Sensors leverage behavior-based detection through heuristics – currently 175 static and dynamic indicators related to files and processes. The HawkEye G Host Sensor's real-time eventing capability collects an incredible amount of information about activities on the endpoints it's protecting, including the processes, changes and connections. It works perfectly against all types of attacks, because HawkEye G doesn't care how threats originate. An attacker physically plugging in a USB device will have no more success than someone outside attempting to send a weaponized document through e-mail. As soon as any program attempts to change a .dll, write code to the drive, set up an unauthorized program in memory, or take any unauthorized action, HawkEye G will instantly detect the attack.

The Host Sensors are complemented by HawkEye G Network Sensors that provide deep packet inspection focused on identifying infected endpoints calling out to command and control servers. Network Sensors are placed at key network ingress and egress points.

HawkEye G Host and Network Sensors are managed centrally by the HawkEye G Manager, which is deployed on a 1U G appliance. Customers can even elect to deploy multiple G managers if needed, for example with one controlling U.S. endpoints and another operating in Europe. HawkEye G can thus scale easily from a single building or office to multiple locations to protecting a global operation.

At this point, the analysis part of HawkEye G comes into play. Customers have total policy control over how they deploy automated and machine-guided responses. The ThreatSync™ analytics program fuses indicators from HawkEye G host and network sensors, threat feeds, a cloud malware verification service, and supported third-party solutions (currently Palo Alto Networks™ and FireEye®) if a customer already has those inside their environment. Information relating to the processes, registry files, .dlls and network connections being activated or attempting to activate on a monitored endpoint are recorded, ranked by severity and reported to administrators.

But HawkEye G goes beyond just detection and verification. The true measure of next generation endpoint protection is its ability to respond to threats, mitigating and eliminating them in nearly real-time before they can do damage. Only Hexis HawkEye G can consistently offer this level of protection. In fact, HawkEye G can be set to automatically mitigate any damage to an endpoint, remediating registry entries and system processes to eliminate malware - all without hampering operations.

HawkEye G easily integrates into popular SIEMs like Splunk so that customers can view it through their SIEM interface.

Everything that HawkEye G does on each protected endpoint is recorded and reported to the G Manager for possible analysis and auditing. This allows even smaller security teams to evaluate and deal with the most advanced problems trying to harm or compromise a network. While full automation is possible, HawkEye G also supports the ability to perform ad hoc manual investigations, enabling users to decide which response they want to take and then make it happen with the single click of a button.

Not every endpoint protection solution is created equally, and it's clear that traditional endpoint protection solutions no longer provide the degree of security necessary in today's environment of advanced persistent threats. Hexis HawkEye G is the only platform that is truly able to claim next generation status, with its ability to detect, verify and respond to all endpoint dangers. Even the most advanced and previously unknown threats are no match for HawkEye G.

Find out More About How HawkEye G Offers True Next Generation Endpoint Protection

Hexis HawkEye G is the only cybersecurity solution that can effectively protect the endpoints of organizations of any size against today's advanced persistent threats. It can automatically eliminate threats regardless of their origins across an entire network without disrupting operations, and can easily be managed by a small IT team or even a single administrator. To learn more about how HawkEye G can protect your network with true next generation endpoint protection, visit Hexis Cyber Solutions at www.hexiscyber.com or contact us at 443-733-1900 or sales@hexiscyber.com.

About Hexis Cyber Solutions

Hexis Cyber Solutions Inc. is a team of cybersecurity experts delivering solutions that enable organizations to defend against and remove cyber threats at machine speeds before they do damage. Hexis' advanced security solutions use real-time endpoint sensors, network detection, and threat analytics to provide organizations with an intelligent and automated threat detection and response solution. Hexis solutions deliver improved visibility into the network and endpoints, threat verification, and automated threat removal capabilities for organizations of all sizes. Hexis Cyber Solutions, Inc. is a wholly-owned subsidiary of The KEYW Holding Corporation (KEYW), based in Hanover, Maryland with engineering offices in Columbia, Maryland and San Mateo, California. Hexis' solutions were developed leveraging KEYW's expertise in supporting our nation's cybersecurity missions.

Hexis™
CYBER SOLUTIONS
a KEYW company