



Network security redefined: Cybersecurity thinking machines detect and anticipate attacks in real time

TABLE OF CONTENTS

Introduction	3
Prevention is not enough	3
Four reasons to shift your security mindset	3
Security that listens, thinks, remembers and anticipates	4
Vectra watches, learns and remembers behaviors over time	5
Detections that matter	5
Intuitive, adaptive reporting	5
Vectra is operationally effective	6
Security that thinks™	6

Introduction

All organizations have infected hosts inside their networks. Prevention-centric security solutions deployed at the network perimeter provide one imperfect chance to stop an attack. Once attackers gain a foothold inside the network, they are free to begin their exploitation and perimeter defenses are blind.

Today, the top priority for security professionals is to implement automated real-time detection and reporting capabilities that provide multiple opportunities to stop an attack. Security technologies must continuously listen, think, remember and automatically analyze data to anticipate the attacker's next move.

The Vectra X-series platform is the first to bring that level of intelligence and automation, instantly identifying a cyberattack as it is happening as well as what the attacker is doing. With patent-pending technology, the Vectra platform learns the typical network traffic patterns and behaviors, and it remembers and correlates anomalous behaviors seen over hours, days and weeks.

The Vectra platform automatically prioritizes attacks that pose the greatest risk, enabling organizations to quickly focus their time and resources.

“The threat of advanced targeted attacks, also known as advanced persistent threats or APTs, has spawned a wave of innovation in the security market.”

Gartner⁴

Cyberattacks are a fact of life for organizations of every size and across every industry. A glance at the news each day reveals yet another massive theft of credit card numbers or other personally identifiable information or an exposé into the shadowy world of cybercriminals.

They have sophisticated business models, with some specialists spreading infections, others operating botnets and the “sales force” selling stolen data. Once attackers take over an organization's hosts, they are effectively selling a cloud services platform to the highest bidder at that organization's expense.

“Concerns about cyberattacks are starting to have measurable negative business implications in some areas,” according to a report from World Economic Forum and McKinsey & Company.¹

The research notes that 80 percent of organizations said that attackers' capabilities were improving faster than their ability to defend against them, and escalating security concerns could slow the progress of cloud computing and mobility.

The damage to a company's brand or loss of an organization's intellectual property or trade secrets can have a devastating impact. Yet stealing payment-card information or intellectual property is practically petty theft compared to the stakes of cyber-espionage and cyber-warfare.

Prevention is not enough

The effectiveness of preventing advanced attacks and malware from entering the network in the first place has eroded dramatically over the past three years.

Historically, the best practice was a layered defense with prevention-centric products such as firewalls, intrusion prevention systems (IPS), web security proxies, payload analysis tools and antivirus software.

“Prevention is futile in 2020. Advanced targeted attacks make prevention-centric strategies obsolete,” declared Gartner in 2013.²

What has happened since the report was published has only heightened the issue.

“Enterprises are overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks,” Gartner writes in a 2014 report.³

“Comprehensive protection requires an adaptive protection process integrating predictive, preventive, detective and response capabilities.” Gartner recommends that information security architects “shift your mindset from incident response to continuous response, wherein systems are assumed to be compromised and require continuous monitor and remediation.”

Four reasons to shift your security mindset

Once an attacker has gained a foothold inside the network, they are free to begin their job. The perimeter defenses are blind to any further activities.

1. Organizations are increasingly connected, extending their network's perimeter and making it porous. The explosion of mobile workers and the shift to cloud services means that corporate applications and data extend far beyond an organization's highly secure data center.

Workers' laptops and mobile devices may get infected at a coffee shop, and that infection will be carried right in through the company's front door. Add bring-your-own-device (BYOD) into the mix, and companies cannot effectively set and enforce guidelines regarding the security software that should be on the device.

The infections on all these devices can spread when they connect to the corporate network, ultimately exposing other applications, databases and users to threats that can further the goals of an attack.

2. Advanced threats are defeating current security controls and attempts to add more controls are failing. Organizations must defend against both high-volume, opportunistic threats and less-prevalent targeted attacks.

The most worrisome threats are stealthy and persistent, often unfolding in stages over days, weeks or even months. Attackers remotely direct the initial compromise, spreading laterally and shape-shifting to achieve their end goal.

3. Each prevention-centric product has only one imperfect chance to identify a threat before its slips past the perimeter into the network.

A firewall or IPS watches individual communication sessions between devices and tries to spot an attack in the traffic based on having seen such an attack before or by assessing an outside system's reputation. But malware and the places it communicates to mutate rapidly to evade these defenses.

More attackers use encryption and other means of obfuscation, often making it impossible for preventive products to create a signature which describes the attack pattern—and no patterns are available for zero-day attacks.

Once an attacker has gained a foothold inside the network, they are free to begin their exploitation. The perimeter defenses are blind to any further activities.

4. A security strategy based on prevention continues to drain IT resources. Most IT departments have limited resources to support the growing needs of the business. An experienced security analyst or consultant may need weeks to properly tune a firewall or IPS so that it is operationally effective.

Isolating a newly discovered suspected threat can mean a very long day of sifting through innumerable alerts.

Network security has always been a complex affair, but now it is so convoluted that big-data analytics companies are getting into the security business. And there simply aren't enough highly skilled (and highly compensated) security analysts to meet the demand.

A fresh approach is needed. Vectra is advancing network security to enable organizations to fully embrace mobility and cloud services and to connect confidently with partners and customers without security getting in the way of doing business.

Security that listens, thinks, remembers and anticipates

A cybersecurity thinking machine, Vectra is the brain within your network. It continuously listens, thinks, remembers and anticipates the next move of an attack in real time.

Providing multiple opportunities to stop the attack makes Vectra the perfect complement to existing prevention-centric security.

Vectra provides real-time insight into advanced persistent attacks through a combination of security research, data science and machine learning. This insight is fully automated with clear, intuitive reports so organizations can take immediate decisive action to stop an attack or mitigate its impact.

Real-time insights into advanced persistent attacks. Machine learning and data science enable Vectra to detect advanced persistent attacks at multiple stages and across the entire attack lifecycle (see Figure 1).

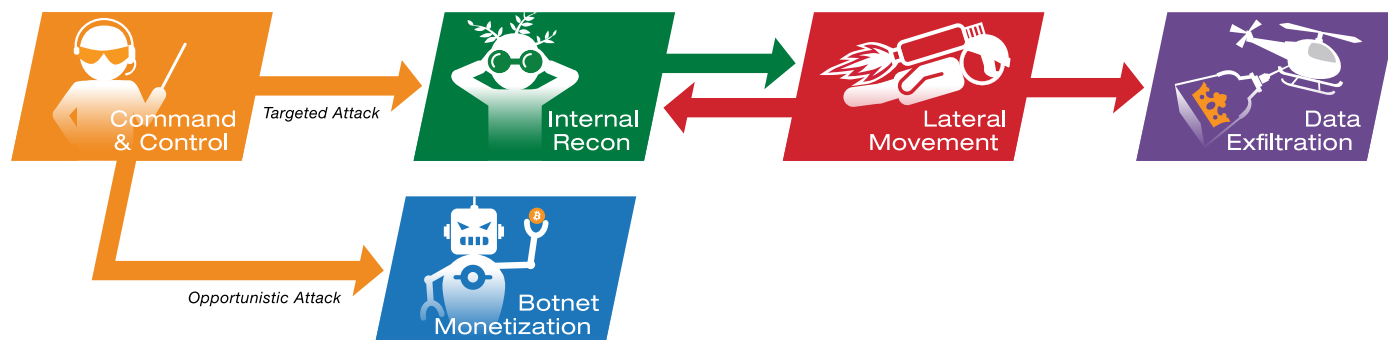


Figure 1: Vectra gives security teams a big advantage over cyber threats by providing visibility into every phase of an active cyberattack.

Providing multiple opportunities to stop the attack makes Vectra the perfect complement to existing prevention-centric security. Disrupting an in-progress attack at any point can prevent or significantly mitigate potential losses.

A device may be compromised by an opportunistic attack or a targeted attack. Once the device has been compromised, the attacker can establish a base camp in the network.

The compromised device may perform reconnaissance to determine where it is and what it might exploit. The attack may move laterally, looking for internal servers with high-value data or probing web servers to find application vulnerabilities.

As devices are exploited, Vectra identifies the signs of automated forms of monetization— sending spam, advertising click fraud, mining bitcoins or an outbound denial-of-service attack—behavior that uses one organization's devices to attack another's or Internet services.

If attackers successfully acquire high-value data, they need to get it out of the organization. Exfiltration is typically done through a series of benign intermediaries before it reaches its final destination.

The data might, for example, be sent to a previously compromised server at a hosting provider, and then later retrieved by the attacker. Vectra will look for the exfiltration, rather than focusing on where the data is being sent as it leaves the company's network.

Vectra watches, learns and remembers behaviors over time

Vectra is always listening, rather than periodically scanning. That means it knows when an attack starts, changes or subsides. And because it's deployed inside the network perimeter, Vectra can listen to users' traffic to and from both the Internet and the data center to identify anomalous behavior.

Vectra learns the traffic patterns and behaviors that are typical to a network, and remembers and correlates anomalous behaviors it detected hours, days or weeks before.

Additionally, Vectra identifies attacks on all operating systems, applications, devices and browsers. It learns the traffic patterns and behaviors that are typical to a network, and it remembers and correlates anomalous behaviors it has seen hours, days or even weeks before.

For example, a laptop that's sending emails is unremarkable, but if the email volume spikes suddenly or if the laptop begins mapping out the inside of the network, it may indicate a broader problem.

Detections that matter

Vectra's innovative Threat Certainty Index™ automatically displays the more significant threats in real time, based on contextual scoring (see Figure 2).

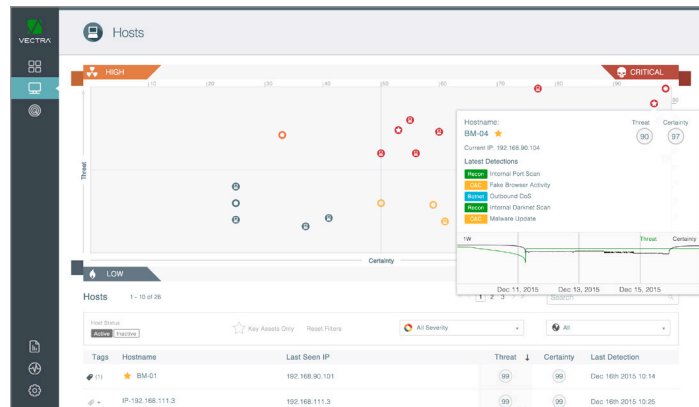


Figure 2: The Vectra Threat Certainty Index prioritizes hosts with the greatest security risk and reports contextual information about the threat.

As Vectra listens, learns and remembers, it may see a particular behavior repeat over time. Vectra distills the most important of these behaviors and analyzes them over days, weeks or even months.

With a longer-term memory than current-generation real-time products, Vectra can put an attack into context and better assess the risk for the organization. Administrators don't need to rummage through gigabytes of log files or wrestle with big-data analytic tools to determine if a threat is real.

Intuitive, adaptive reporting

With a real-time view of the most important threats, security teams can use the Vectra Threat Certainty Index to prioritize their remediation and mitigation efforts. This makes it easy to prioritize stopping a laptop an attacker is using to exfiltrate intellectual property over cleaning an infected machine being used for advertising click fraud.

Vectra's visual clarity comes without compromise. Security administrators can drill down into the threat details, including packet captures that enabled identification of the behavior (see Figure 3). Vectra's reporting can document the progression of a threat over time.

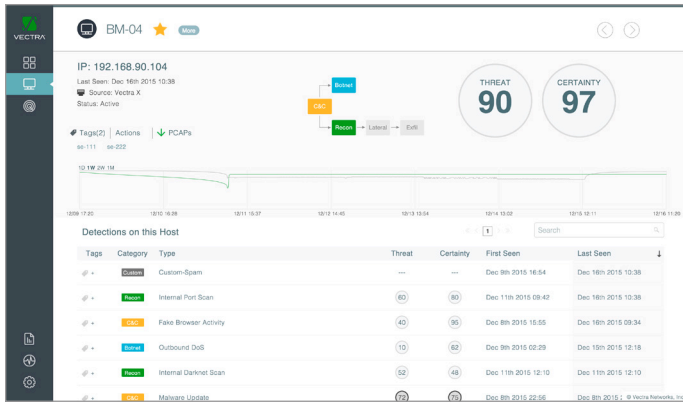


Figure 3

Vectra is operationally effective

Vectra does all the hard work of security and is designed to relieve the burden of real-time security monitoring from the operations team. Administrators don't need to perform a detailed, time-consuming configuration or spend weeks tuning the platform.

When the Vectra platform is plugged into the network, it automatically learns what it needs to know and establishes a baseline behavior of the devices connected to the network. Vectra updates automatically via a cloud service so protection is always up to date.

Security that thinks™

It's time for security to get smarter. Attackers are already in your network, looking for an opportunity to steal high-value data or further their goals. Vectra's cybersecurity thinking machine does the hard work by recognizing an attack amid the normal chatter in your network and anticipating the next move in real time so the attack can be stopped.

See how Vectra works at www.vectranetworks.com/demo

¹ "Risk and Responsibility in a Hyperconnected World," World Economic Forum in collaboration with McKinsey & Company, January 2014, http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

² "Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence," by Neil MacDonald, Gartner, 30 May 2013, ID G00252476, <http://www.gartner.com/document/2500416>

³ "Designing an Adaptive Security Architecture for Protection From Advanced Attacks," by Neil MacDonald and Peter Firstbrook, 12 February 2014, ID G00259490, <https://www.gartner.com/doc/2665515/designing-adaptive-security-architecture-protection>

⁴ "Five Styles of Advanced Threat Defense," by Lawrence Orans and Jeremy D'Hoinne, Gartner, 20 August 2013, ID G00253559