VECTRA™

White Paper

# Reinventing Network Security

## Vectra's cyber-security thinking machine delivers a new experience in network security

**Executive Overview**

Organizations are under constant attack from high-volume opportunistic threats and the less-frequent, but highly targeted attacks. Damage ranges from a nuisance to operational disruption to the theft of high-value information. For decades, prevention-centric security has been the answer, but its efficacy has fizzled in the face of more advanced attacks. The reality is that adversaries are already inside most organizations' networks, and security operations teams are often blind to these incursions.

Vectra's platform delivers real-time detections of advanced cyberattacks by continuously monitoring the network. Vectra reports real-time insights into each stage of a cyber attack, providing multiple opportunities to prevent or mitigate loss, with next-to-zero operational cost. Vectra achieves this differentiation by leveraging inflection points in data analytics, machine learning and next-generation computing technology. The platform can detect attacks on any operating system, application, device and browser.

Read this whitepaper to learn how Vectra's cyber-security thinking machine continuously listens, thinks, remembers and anticipates the next move of an attack in real time, giving IT the insight to stop attacks, even while they are happening.

# Reinventing Network Security

## Vectra's cyber-security thinking machine delivers a new experience in network security

VECTRA™

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

—Gartner[4]

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.

### Relying on Prevention is Not Enough

The effectiveness of preventing advanced attacks and malware from entering the network in the first place has eroded rather 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."

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

# Reinventing Network Security

Vectra's cyber-security thinking machine delivers a new experience in network security

VECTRA™

## Four reasons to shift your security mindset

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 control 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 game.

3. **Each prevention-centric product has only one 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 the attack has gained a foothold inside the network, it is free to begin its job. 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 the 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.

# Reinventing Network Security

Vectra's cyber-security thinking machine delivers a new experience in network security

VECTRA™

## Security that Listens, Thinks, Remembers and Anticipates

Vectra is a cyber-security thinking machine—a brain within your network. Vectra continuously listens, thinks, remembers and anticipates the next move of an attack in real time. 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 impact 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 lifecyle (see Figure 1). 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.

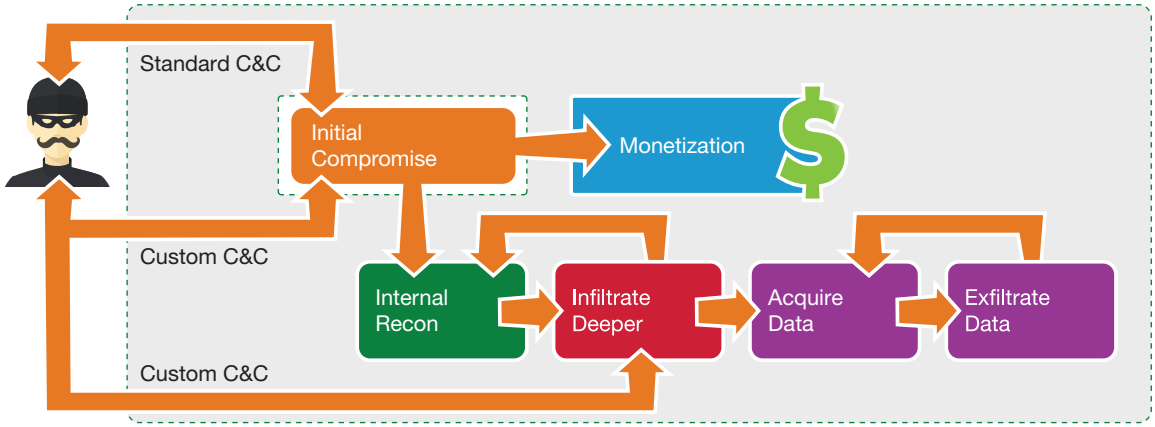


*Figure 1: Vectra gives security administrators an unfair advantage over cyberattacks. Vectra has visibility into every attack stage, from the initial infection to the exfiltration of the stolen information. Disrupting an attack at any point can prevent or significantly reduce potential losses.*

# Reinventing Network Security

## Vectra's cyber-security thinking machine delivers a new experience in network security

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

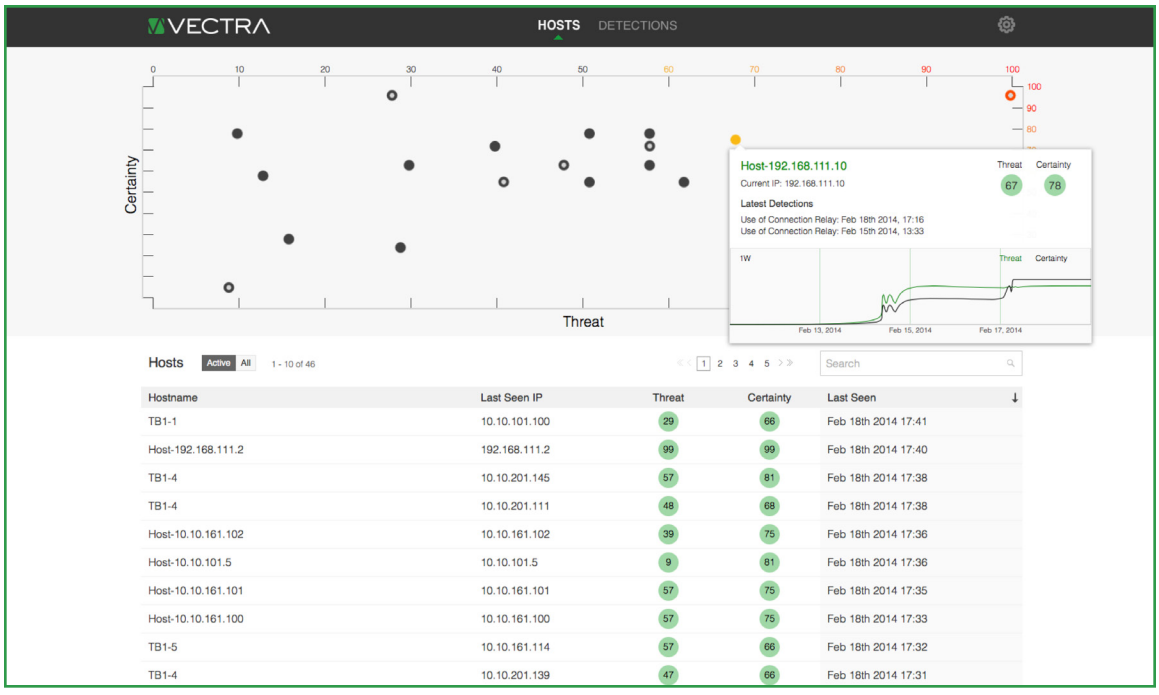


*Figure 2: Administrators can see the most important threats in their network at a glance with Vectra's innovative Threat-Certainty Index.*

# Reinventing Network Security

## Vectra's cyber-security thinking machine delivers a new experience in network security

Vectra is a cyber-security thinking machine. Vectra continuously listens, thinks, remembers and anticipates the next move of an attack in real time.

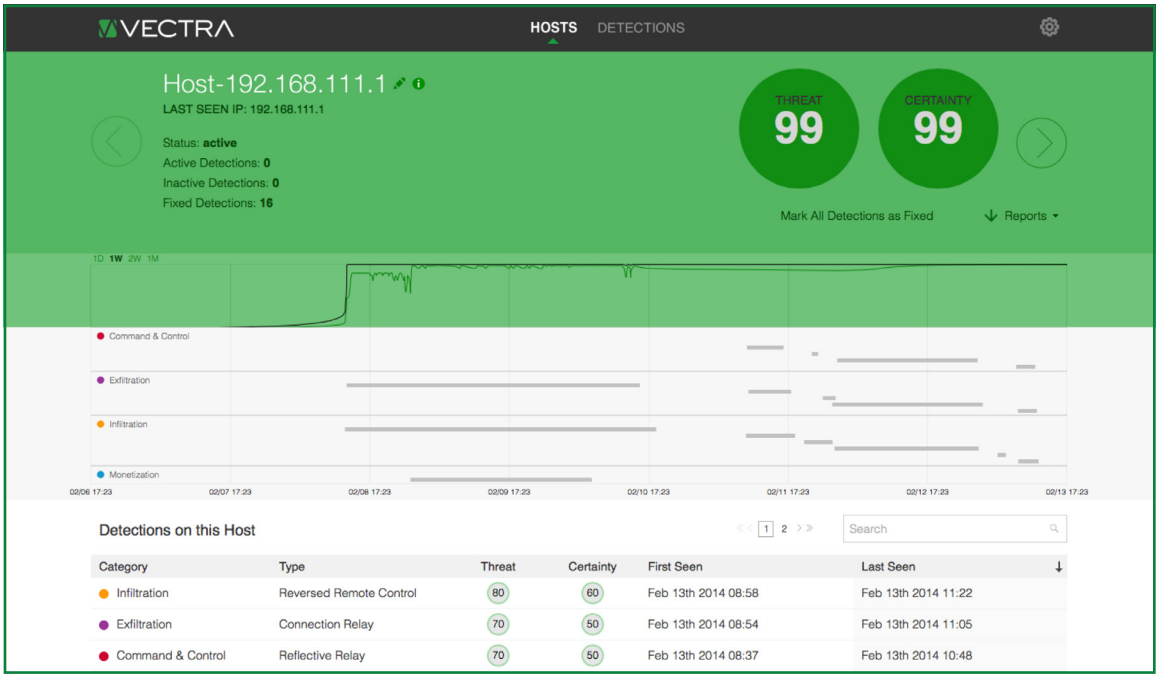


*Figure 3: Administrators can drill into details, such as the threats detected on a particular device.*

**Intuitive, adaptive reporting.** With a real-time view of the most important threats, security managers can use the Vectra Threat-Certainty Index to prioritize their remediation and mitigation efforts. That makes it easy for IT 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.

**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 cyber-security 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](www.vectranetworks.com/demo).**