Vectra
company background
TABLE OF CONTENTS

Introduction .......................................................... 3
What makes Vectra unique ............................................ 3
Real-time threat hunting ............................................. 3
Blind-spot-free threat detection coverage ..................... 3
The right context, right now ......................................... 3
Fortify your security infrastructure .............................. 3
Why cyberattackers succeed ...................................... 3
Challenges in the cloud and data centers .................... 3
Challenges in enterprise networks ............................... 3
Challenges across the entire infrastructure .................... 4
How Cognito works .................................................. 4
The intelligence to reveal all phases of attack ............... 4
Monitor all traffic across the enterprise ....................... 5
Find the biggest threats with certainty ....................... 5
Automation for faster incident response ..................... 5
Native security for the private cloud ......................... 6
Full lifecycle detection of ransomware ....................... 6
Linking multiple attacks to a single campaign ............ 6
Cutting-edge threat research .................................... 6
Artificial intelligence products .................................. 7
  X-series appliance .................................................. 7
  S-series sensors .................................................... 7
  Virtual sensors ....................................................... 7
Leadership ............................................................ 8
  Executives ............................................................ 8
  Board of Directors ................................................ 10
  Investors ............................................................. 10
  Advisors ............................................................ 11
Introduction
Incorporated in 2011 and headquartered in San Jose, Calif. with other offices worldwide, Vectra® artificial intelligence automates the hunt for hidden cyberattackers inside networks. This enables security operations teams to detect and respond to cyber threats with exceptional speed and precision to prevent catastrophic damage.

The company’s innovative Cognito™ threat detection and response platform uses artificial intelligence to automate the manual, time-consuming analysis of security events, condensing days or weeks of investigation into minutes and reducing attack investigation workloads by up to 29x.

What makes Vectra unique
Cognito is the fastest, most efficient way to detect and stop cyberattackers inside global enterprise networks – from cloud and data center workloads to user and IoT devices.

With Cognito, security operations teams can make fast, intelligent decisions about where to focus their time and resources to stop the spread of in-progress cyberattacks and prevent loss.

Real-time threat hunting
Cognito performs non-stop automated threat hunting powered by always-learning behavior models based on artificial intelligence. This enables Cognito to quickly find hidden cyber attackers before they cause irreparable damage.

Blind-spot-free threat detection coverage
Cognito analyzes all network traffic – including cloud and data center workloads – to gain high-fidelity visibility into the actions of IoT, BYOD and all other connected devices, leaving attackers with nowhere to hide.

The right context, right now
Cognito eliminates manual threat hunting and lets security analysts respond quickly and decisively to attacks in progress by putting the most relevant information and context at your fingertips.

Fortify your security infrastructure
Cognito works with firewalls, endpoint security, network access control, and other enforcement points to automate the blocking of cyberattackers. It also gives SIEMs and forensic tools a clear starting point for threat investigations.

Why cyberattackers succeed
Challenges in the cloud and data centers
Cloud and data center security has largely focused on segmentation, access management policies and anti-virus in the virtual space to detect an initial infection. Today, cloud and data center security must extend beyond virtualization to include the underlying infrastructure and low-level management tools.

This is critical today because advanced adversaries and professional hacking groups recognize that the keys to the kingdom can be found in the physical infrastructure of equipment in the cloud and data center – the routers, firewalls, switches and systems below the operating system.

Cloud and data center attacks focus on the most vulnerable point – underlying physical infrastructure
Instead of launching exploits or malicious payloads against data center resources, cyberattackers prefer to use a position of trust to make their way closer to key assets. They covertly hijack administrative credentials, elevate their privileges, and plant rootkits and backdoors in the physical infrastructure.

Once they are in the cloud and data center, attackers will burrow beneath the operating system to gain complete administrative control over a firewall and then launch attacks against routers and servers in the same network. It is extremely difficult to detect these attacks using traditional methods because they occur well below the level of the operating system.

Challenges in enterprise networks
Despite having next-generation firewalls, IDS/IPS and malware sandboxes, cyberattackers can evade the strongest perimeter security and spread inside networks. That’s because perimeter defense systems only keep out known threats.
Perimeter defenses rely on signatures and reputation lists of known threats and must be continually updated. This approach cannot keep up with today’s organized cybercriminals, who constantly change their attack methods to elude detection.

In fact, most malware used in cyberattacks are unique to the organizations that are being targeted and have never been seen before. It’s also easy for attackers to mount an assault by using different IP addresses or by adding a few bits to a known malware file so it can slip by undetected.

**Challenges across the entire infrastructure**

Security analysts today are overwhelmed by a never-ending succession of alerts and logs about potential network cyberattacks. In many networking environments, it’s common to get 50 alerts per minute.

Faced with lean or understaffed security teams, it’s not humanly possible to manually sift through and interpret that much data, identify the most serious threats, and then mitigate attacks before they spread. Security teams often don’t know what to look for or where.

For post-breach forensic analysis, which occurs after an attack, many organizations rely on log managers and security information and event management (SIEM) systems. They are used to reconstruct a cybercrime in order to understand the extent of damage.

Despite all the security tools at your disposal, there remains a dangerous cybersecurity gap between the time attackers infiltrate and spread inside a network and the moment they exfiltrate with stolen assets. These attacks can go unnoticed for many months, giving the bad guys plenty of time to disappear into the wild.

**How Cognito works**

From cloud and data center workloads to user and IoT devices, Cognito provides continuous, automated threat surveillance to proactively expose hidden and unknown cyberattackers that actively spread inside networks.

The genesis of Cognito is based on a simple principle for finding hidden threats: Use an authoritative source of data and seek out the fundamental threat behaviors that cybercriminals can’t avoid when they carry out an attack.

To do this, Cognito relies on the only source of truth during a cyberattack – network traffic. Only traffic on the wire reveals the truth with complete fidelity and independence. Low-fidelity sources, such as analyzing logs, only show what you’ve already seen, not the hidden attacks that were missed.

Cognito delivers a new, automated way of analyzing network traffic at scale. Instead of traditional payload inspection, it uses artificial intelligence, machine learning, and behavioral traffic analysis to expose the fundamental behaviors of attackers as they spy, spread, and steal in the network – even in encrypted traffic.

**The intelligence to reveal all phases of attack**

Cognito automatically exposes fundamental attack behaviors in network traffic, including:

- Command-and-control and other hidden communications
- Internal reconnaissance
- Lateral movement
- Abuse of account credentials
- Data exfiltration
- Early indicators of ransomware activity
- Botnet monetization
- Attack campaigns, including the mapping of all hosts and their associated attack indicators

<table>
<thead>
<tr>
<th>Prevention Phase</th>
<th>Active Phase</th>
<th>Clean-up Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Infection</td>
<td>99 days</td>
<td>Key assets found in the wild</td>
</tr>
<tr>
<td>$$$$$</td>
<td>$99 days</td>
<td>$1212222</td>
</tr>
<tr>
<td>$$$$</td>
<td>Attackers had free rein in breached networks</td>
<td>$2222222</td>
</tr>
<tr>
<td>$$ $$</td>
<td>$555555555</td>
<td>$333333333</td>
</tr>
<tr>
<td>$</td>
<td>Cybersecurity Gap</td>
<td>$777777777</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Firewalls</th>
<th>IPS</th>
<th>Proxies</th>
<th>Sandboxes</th>
<th>SIEM analysis</th>
<th>Forensic consultants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source: M-Trends 2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There’s a dangerous cybersecurity gap between prevention security at the network perimeter and post-forensic analysis that occurs after an attack.
Cognito detects active threats in all phases of the cyberattack kill chain

Cognito continuously learns your local network environment and tracks all physical and virtual hosts to reveal signs of compromised devices as well as insider threats.

**Monitor all traffic across the enterprise**

Cognito monitors all enterprise network traffic – internet bound (north/south), internal (east/west), and inside the data center, including traffic between virtual workloads. All host devices are monitored, including servers, workloads, laptops, BYOD, IoT, as well as routers, switches and firewalls in the physical infrastructure.

Blind-spot-free threat detection coverage is provided across the entire enterprise network infrastructure

**Find the biggest threats with certainty**

The Vectra Threat Certainty Index™ consolidates thousands of events and historical context to pinpoint hosts that pose the biggest threat. We boil down mountains of data to pinpoint the threats that matter. Threat and certainty scores trigger notifications to security teams, a response from other enforcement points or automate SIEM workflows.

Events and historical context are automatically consolidated to identify compromised hosts that pose the biggest threat

**Automation for faster incident response**

Cognito automates the time-consuming Tier-1 analysis of individual security events and eliminates the manual hunt and search for threats. Security analysts can instantly see who compromised hosts are communicating with. In addition, on-demand access to metadata from captured data packets speeds-up forensic analysis to enable quick, decisive action.

The most relevant threat information and context is always at your fingertips so you can act quickly and decisively to mitigate attacks, such as data smuggling
Native security for the private cloud
Cognito monitors the virtualized layer of the data center and its underlying infrastructure to detect complex attacks. Virtual sensors (vSensors) provide visibility into all traffic passing between virtual workloads, while native integration with VMware vCenter offers an always up-to-date view of virtual and physical environments.

Complex attacks are detected in the virtualized layer of the data center and its underlying infrastructure.

Full lifecycle detection of ransomware
By monitoring all internal network traffic throughout the enterprise, Cognito identifies the early tell-tale behaviors of a ransomware threat across all phases of an attack – including command-and-control communications for key exchange, network scans for network drives, and lateral movement of file encryption across the network – before key assets can be taken hostage.

Linking multiple attacks to a single campaign
Cognito exposes the relationships between threat detections on separate workloads and devices to understand the activity and broader scope of orchestrated attack campaigns.

As an attacker controls devices remotely, performs reconnaissance and moves laterally in a network, Cognito presents a synthesized view of the entire attack campaign by connecting the dots of related attacker behavior detections across all involved hosts.

Cognito can also zoom in or pan the view of hosts or related campaign detections to analyze the campaign history and better understand the lifetime of the attack. By identifying connections across multiple machines that are part of a single attack campaign, an entire attack can be stopped at the earliest signs of detection.

Cutting-edge threat research
The Vectra Threat Labs™ operates at the precise intersection of security research and data science. Lab researchers take unexplained phenomena seen in customer networks and dig deeper to find the underlying reasons for the observed behavior.

Security industry experts in the Vectra Threat Labs each have over a decade of experience in reverse engineering, exploit development and incident response from security research organizations at IBM, eEye Digital Security, Juniper, ISS, and the U.S. Department of Defense.

 Vectra researchers identify, investigate and report on a wide range of cyberattacks, security vulnerabilities and threat behaviors that are largely unknown to the world. With data sets from the research team, data scientists develop the machine learning and behavioral analysis behind the artificial intelligence in the Cognito cybersecurity platform.

Reports, bulletins and blogs issued by the Vectra Threat Labs zero-in on attackers’ goals, place them in the context of the broader campaign that attackers wage, and provide insights into durable ways in which threats can be rapidly detected and mitigated.
Focusing on the underlying goals of attackers and thinking about the possible methods they use to achieve them lead to detection methods that are incredibly effective for extended periods of time. This ensures that the security posture of our customers is not a constant race against time.

**Artificial intelligence products**

Based on artificial intelligence, the Cognito automated threat detection and response platform features a flexible, scalable software architecture that ensures full visibility into cyberattack behaviors across enterprise networks.

Regardless of size or geographic spread, this distributed architecture provides unified threat detection coverage of all network traffic, from cloud and data center workloads to user and IoT devices.

This distributed architecture enables customers to deploy X-series appliances as a centralized Brain. A combination of physical S-series sensors and vSensors are deployed across multiple locations to collect and deliver information to the Brain for centralized analysis, detection and correlation of threats.

**X-series appliance**

Cognito runs on the X-series appliance, which can be deployed in three modes – Sensor, Brain or Mixed. In Sensor mode, the X-series ingests traffic, extracts metadata and forwards it to another Brain or Mixed-mode X-series for processing. In Brain mode, the X-series only receives metadata from one or more sensors. In Mixed mode, the X-series performs both Brain and Sensor functions.

**S-series sensors**

S-series sensors are easily deployed at remote sites or at access switches on internal network segments to extend the reach of Cognito deployments. Small, dedicated devices, S-series sensors passively monitor network traffic, extract critical metadata and forward it to the Brain for analysis and attack detection.

S-series sensors can be deployed in-line as a bump-in-the-wire that fails-open or on a SPAN port or network TAP. The small size and simple deployment of the S-series sensors ensure that there is comprehensive coverage across the entire network, especially at remote sites such as small offices, clinics and retail locations.

**Virtual sensors**

Running in VMware ESXi 5.0 or later, vSensors make it easy to extend threat detection coverage across the physical network and into virtualized data centers.

The vSensors can connect to any VMware vSwitch in the data center to provide visibility into all traffic and detect threats that pass between workloads in the virtual environment. Cognito also integrates with VMware vCenter for an authoritative, always up-to-date view of the virtual environment.
Leadership

Executives

Hitesh Sheth is the president and CEO of Vectra. Previously, he held the position of chief operating officer at Aruba Networks. Sheth was also executive vice president and general manager of the Juniper Networks switching business and senior vice president of Service Layer Technologies. Before Juniper, he held senior management roles at Cisco Systems, including running its metro Ethernet business.

Oliver Tavakoli is the chief technology officer at Vectra. Tavakoli is a technologist who has alternated between working for large and small companies throughout his 25-year career. Prior to joining Vectra, he spent more than seven years at Juniper Networks as the CTO for its security business. Tavakoli joined Juniper as a result of its acquisition of Funk Software, where he was also CTO.

Howie Shohet is the chief financial officer at Vectra. Previously, he was CFO at Lattice Engines and CFO at C3 Energy. Howie was also senior business unit controller at Juniper Networks, where he led finance for the enterprise switching, security and data center business groups, and was executive director at Siebel Systems, where he was responsible for worldwide financial planning and analysis.

Kevin Moore is senior vice president of worldwide field operations. He brings nearly two decades of sales and sales operations experience, having spent 13 successful years as a key sales executive at Proofpoint from its first product shipment to post-IPO. Kevin was vice president of sales at Proofpoint, where he was responsible for global strategic accounts and sales throughout Japan, Australia and New Zealand.
Mike Banic is vice president of marketing at Vectra. Previously, he was vice president of global marketing for networking at Hewlett-Packard. Banic joined HP from Juniper Networks, where he was vice president of enterprise marketing and vice president of marketing for Ethernet switching. He joined Juniper through its acquisition of Peribit Networks, where he was vice president of corporate marketing.

Kevin Kennedy is vice president of product management at Vectra. Before Vectra, he was vice president of product management at Agari Data, which builds security solutions that eliminate email as a channel for cyberattacks. Prior to Agari, Kennedy was senior director of security product management at Juniper, where he led the company’s continued innovation in data center security.

Jason Kehl is vice president of engineering at Vectra. Prior to joining Vectra, Kehl was vice president at Juniper Networks, where he led global R&D for network security and management products. Before that, he joined Cisco Systems via its acquisition of IronPort Systems and became a director, where he drove innovations in IPS global correlation and big data to power anti-malware technologies.

Gerard Bauer is vice president of EMEA at Vectra. Before Vectra, he held key sales leadership roles at Riverbed Technology, most recently as regional vice president of Southern Europe. Prior to Riverbed, Bauer also held sales leadership roles at NetApp, including director of Eastern Europe, where he established new markets that fueled revenue growth for the company.
Board of Directors

Hitesh Sheth is the president and CEO of Vectra. Prior to Vectra, he was the chief operating officer at Aruba Networks, which is now part of Hewlett-Packard Enterprise. He was also executive vice president and general manager of the Juniper Networks enterprise switching business and senior vice president of the company’s security products in the Service Layer Technologies group. Before Juniper, Sheth held senior management positions at Cisco Systems, including running the company’s metro Ethernet line of business.

Charles Giancarlo is a senior advisor to Silver Lake Partners and was a senior executive at Cisco Systems, where he was responsible for over 80 percent of revenue. Giancarlo is on the board of Accenture, Arista, Blue Jeans Network, Imperva, ItsOn, ServiceNow and Soraa, and is chairman of the board at Avaya. Giancarlo holds a bachelor’s degree in electrical engineering from Brown University, a master’s degree in electrical engineering from the University of California at Berkeley, and an MBA from the Harvard Business School.

Brad Gillespie, general partner at IA Ventures, has over 15 years of leadership experience in product, technology and management and held key roles at Microsoft, including technology advisor to the chief technical officer. He began his career at Lockheed-Martin, where he developed real-time classification systems and PDP-11 assembly programming. He holds a PhD in electrical engineering from the University of Washington and is an affiliate professor of electrical and computer engineering at the University of New Hampshire.

Jim Messina is founder and CEO of the Messina Group, a full-service strategic consulting firm. The architect of Barack Obama’s 2012 re-election campaign, he is recognized as one of the world’s top public affairs and communications strategists. In 2013, Messina was named the chairman of Organizing for Action, an advocacy group that promotes social policies from the community level, and co-chairman of Priorities USA Action, a progressive super PAC. His close, trusted relationships with key global figures add value and insight to the work of the Messina Group.

Eric Wolford from Accel Partners is on the board of directors at Riverbed Technology, BitTorrent, and Jut. He has held a variety of executive leadership roles, including products group president at Riverbed; senior vice president of products, marketing and business development at NetVMG, and vice president of product marketing and management at Inktomi and FastForward Networks. Wolford earned a bachelor’s degree in pre-medicine from Pepperdine University and an MBA from the New York University Stern School of Business.

Investors

khosla ventures

ACCEL

PARTNERS

IA VENTURES

AME CLOUD VENTURES

DAG VENTURES

Intel Capital

JUNOS INNOVATION FUND

wipro
Advisors

Thomas J. Bakewell is the former chief information officer and vice president of information technology at Infoblox in Santa Clara, Calif. Under his leadership, the IT organization achieved new levels of business agility, productivity, and customer service through innovative, adaptive technology solutions that accommodate Infoblox business priorities. Before Infoblox, Bakewell held executive IT leadership roles at Riverbed, Coherent, Brocade Systems and Sun Microsystems.

Alan Boehme provides leadership and oversight for several key areas within the Coca-Cola Global IT organization. He is responsible for establishing and managing process, data, applications, technology and infrastructure for all of Coca-Cola as well as evaluating new technologies and working closely with the business. Before joining Coca-Cola, Boehme was senior vice president of IT strategy and architecture and head of off-shore business process outsourcing operations for ING.

Mike Kourey is the chief financial officer at Medallia and a former partner at Khosla Ventures. He is currently a member of the board of directors at Riverbed Technology, AliveCor, Climate Corp., Metamarkets, Solum, Transonic, and Varentec. Kourey is also a board observer at eASIC and on the advisory boards of the University of California, Davis Graduate School of Management. Previously, Kourey was the CFO and a member of the board of directors at Polycom.

Jane Holl Lute is president and CEO of SICPA North America and special advisor to the United Nations secretary general. Previously, she served as deputy secretary for the U.S. Department of Homeland Security. As the department’s chief operating officer, she was responsible for ensuring the nation’s cybersecurity. Prior to that, Lute served as United Nations assistant secretary-general for Peacebuilding Support and assistant secretary general for Mission Support in the Department of Peacekeeping Operations.

RiceHadleyGates LLC is an international strategic consulting firm based in Silicon Valley and Washington, D.C. It offers advice based on extensive experience in the international arena. The consultancy works with companies to develop and implement international strategic plans and helps them expand in major markets, including Asia, the Middle East and the Americas. The principals at RiceHadleyGates are Condoleezza Rice, Stephen J. Hadley, Robert Gates and Anja Manuel.