VECTRA®

Vectra Networks company backgrounder

VECTRA

TABLE OF CONTENTS

Introduction

A brief history of Vectra

Vectra® Networks is the leader in artificial intelligence software that automates the hunt for hidden cyber attackers inside networks and enables cybersecurity teams to respond to threats with exceptional speed and precision.

In 2015, Vectra was recognized by Gartner as a cool vendor in security intelligence, the RSA Conference as a finalist in its annual innovation sandbox competition, and the American Business Awards as the top tech startup of the year. At the conclusion of 2015, Vectra sales bookings grew nearly 400% year over year.

In 2016, Vectra was recognized by Forbes as one of the top five hottest security startups, CRN as one of the 10 emerging security vendors you need to know about, and received the Best of Black Hat Award for most innovative emerging company.

The Vectra Threat Labs™ has published breakthrough research, including a zero-day threat in Microsoft Internet Explorer 11, how attackers can easily turn a Web cam into a network backdoor and a critical Microsoft Windows zero-day vulnerability in versions as far back as Windows 95.

In the third edition of the Post-Intrusion Report, published in April 2016, the Vectra Threat Labs provided data and trends of attacker behaviors detected in over 150 product deployments of organizations that opted to participate in the study.

Key company takeaways

Vectra artificial intelligence software offers the fastest, most efficient way to detect and stop cyber attackers inside your network – from the campus to the data center to the cloud.

Real-time cyber-attack visibility

Vectra delivers real-time attack visibility and non-stop automated threat hunting powered by always-learning behavior models. This enables Vectra to quickly find elusive cyber attackers in your network before they cause irreparable damage.

Blind-spot-free threat detection

Vectra analyzes all network traffic to gain high-fidelity visibility into the actions of all devices – including BYOD and IoT devices – from the campus to the data center to the cloud, leaving attackers with nowhere to hide.

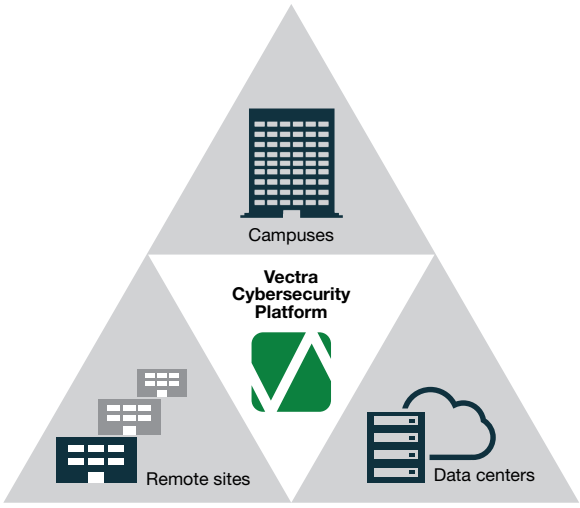
The right context, right now

Vectra 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. We automatically prioritize, score and correlate detected threats with compromised hosts and key assets that are the targets of an attack.

Strengthen your security infrastructure

Vectra works with firewalls, endpoint security, network access control, and other enforcement points to automate the blocking of hidden and customized attacks. We also give SIEMs and forensic tools a clear starting point to perform faster and more efficient threat investigations.

All this enables cybersecurity teams to make quick, better-informed decisions about where to focus their time and deploy countermeasures to quickly mitigate active threats and prevent loss.



Vectra detects active cyber attacks that can spread inside networks – from campuses to remote sites to data centers and the cloud

Why cyber attackers succeed

Challenges in campus networks

Despite having next-generation firewalls, IDS/IPS and malware sandboxes, cyber attackers can evade the strongest perimeter security and spread inside networks. That's because perimeter defense systems only keep out known threats.

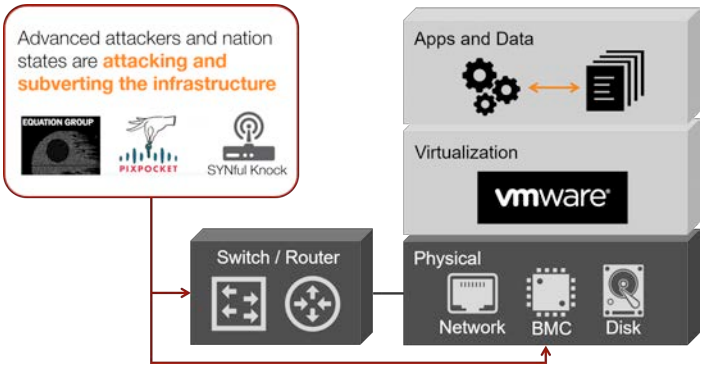
Perimeter defenses rely on signatures and reputation lists of known threats and must be continually updated. This approach cannot keep up with today's organized cyber criminals, who constantly change their attack methods to elude detection.

In fact, according to the 2015 Verizon Data Breach Investigations Report, a majority of malware used in attacks are unique to targeted organizations and are therefore unknown. It's also quite 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 in data centers

For years, data center security has largely focused on segmentation, access management policies and anti-virus in the virtual space to detect an initial infection. Today, 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 data center's physical infrastructure of equipment – the routers, firewalls, switches and systems below the operating system.



Data center attacks focus on the most vulnerable point – underlying physical infrastructure

Instead of launching exploits or malicious payloads at data center resources, cyber attackers 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 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 across the entire infrastructure

Security analysts today are overwhelmed by a never-ending succession of alerts and logs about potential network cyber attacks. 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 security 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.

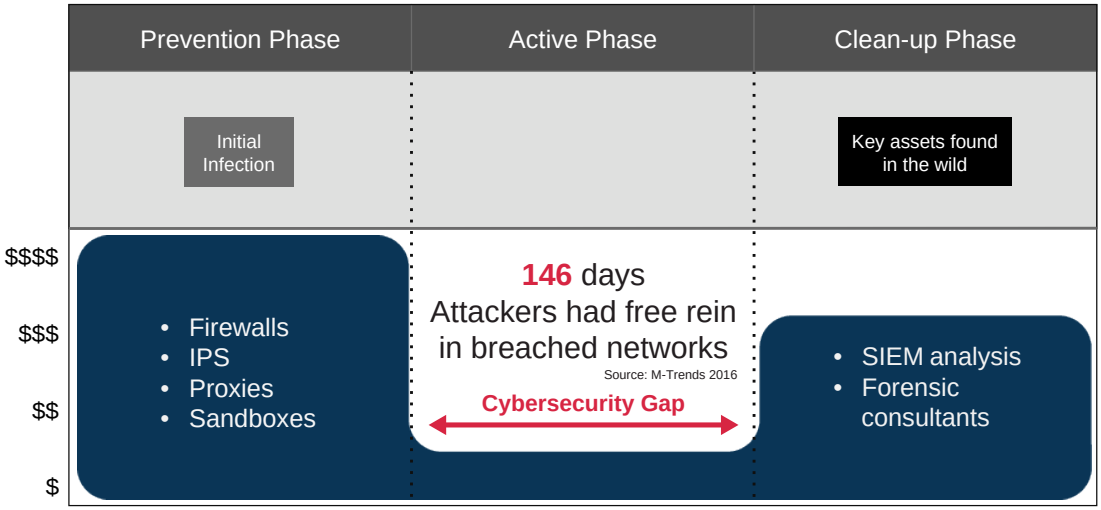
The Vectra difference

From campuses to data centers to private clouds, Vectra provides continuous, automated threat surveillance to proactively expose hidden and unknown cyber attackers that are actively spreading in your network.

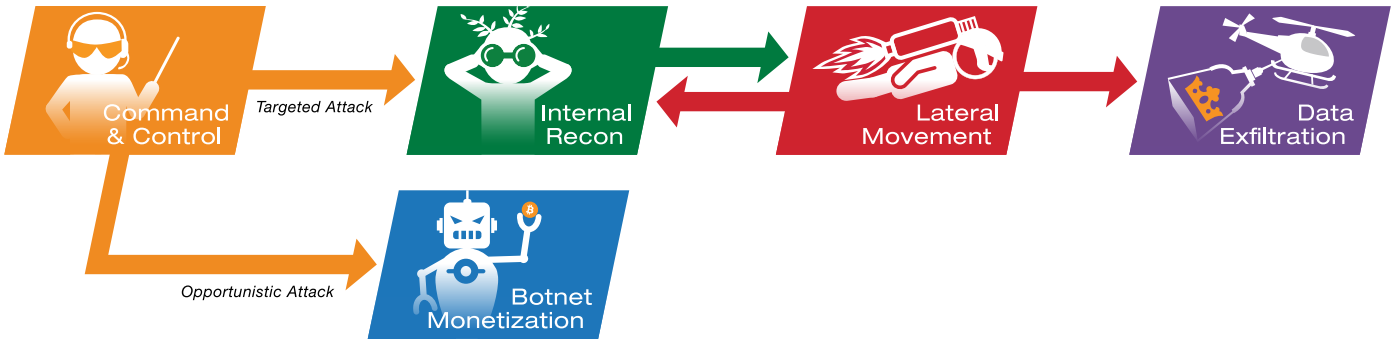
The Vectra cybersecurity platform is based on a simple principle for finding hidden threats: Use an authoritative source of data and seek out the fundamental threat behaviors that attackers simply can't avoid.

To do this, Vectra relies on the only source of truth during a cyber attack – 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.

Vectra delivers a new, automated way of analyzing network traffic at scale. Instead of traditional payload inspection, Vectra 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.



There's a dangerous cybersecurity gap between prevention security at the network perimeter and post-forensic analysis that occurs after an attack



Vectra detects active threats across all phases of a cyber attack

The intelligence to reveal all phases of attack

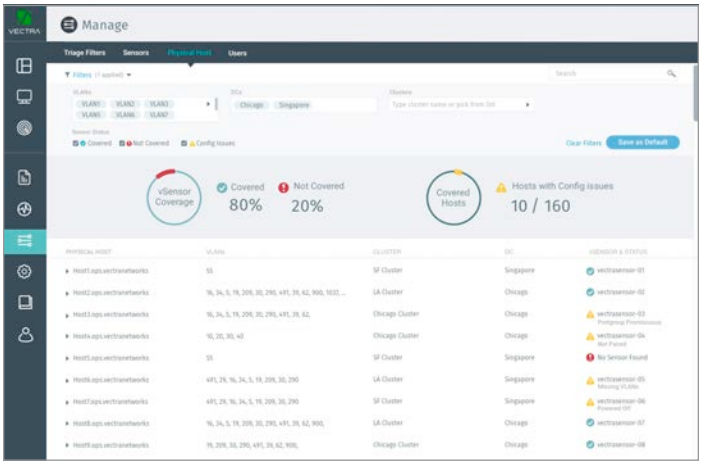
Vectra automatically exposes fundamental attack behaviors in network traffic, including:

- Remote access tools
- Hidden tunnels
- Backdoors and rootkits
- Credential abuse
- Command-and-control communication
- Internal reconnaissance
- Lateral movement
- Data exfiltration
- Botnet monetization

Vectra 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

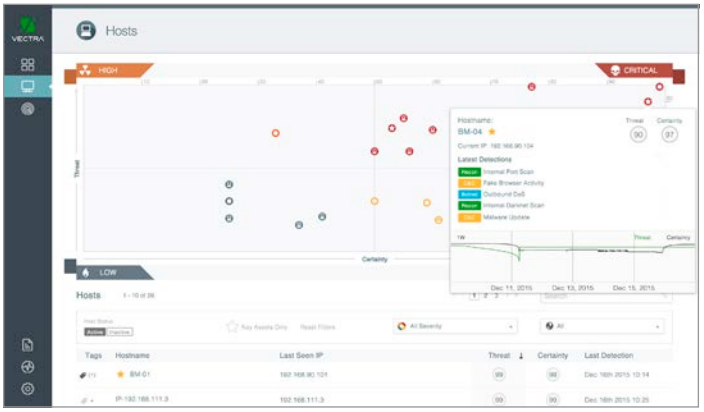
Vectra monitors all enterprise network traffic – Internet bound (north/south), internal (east/west), and inside the data center, including traffic between virtual workloads. All host devices are monitored, including servers, workloads, laptops, BYOD, IoT, as well as routers, switches and firewalls in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



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

Find the biggest threats with certainty

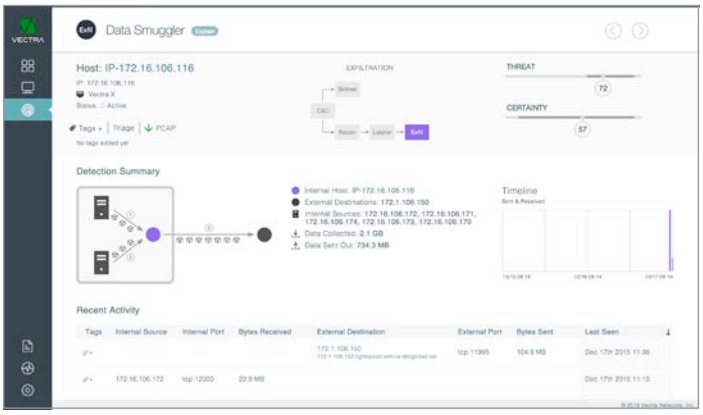
The Vectra Threat Certainty Index™ consolidates thousands of events and historical context to pinpoint hosts that pose the biggest threat. We boil down mountains of data to pinpoint the threats that matter. Threat and certainty scores trigger notifications to security teams, a response from other enforcement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



Thousands of events and historical context are automatically consolidated to identify compromised hosts that pose the biggest threat

Automation for faster incident response

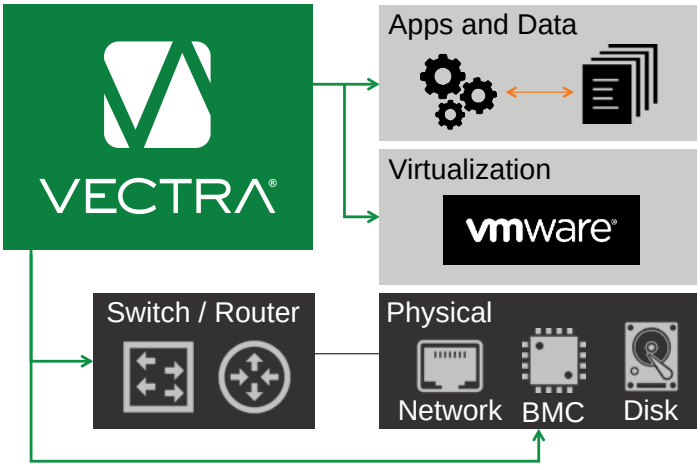
Vectra automates the time-consuming Tier-1 analysis of individual security events and eliminates the manual hunt and search for threats. Security analysts can instantly see who compromised hosts are communicating with. In addition, on-demand access to packet captures speeds-up forensic analysis to enable 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

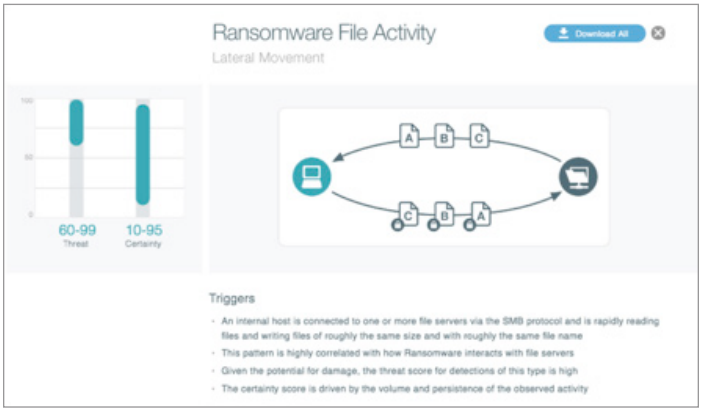
Vectra monitors the virtualized layer of the data center and its underlying infrastructure to detect complex attacks. Vectra virtual sensors (vSensors) provide visibility into all traffic passing between virtual workloads, while native integration with VMware vCenter offers an always up-to-date view 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, Vectra identifies the 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.



Vectra identifies ransomware behaviors, including command-and-control, network scans and lateral movement

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 cyber attacks, 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 Vectra cybersecurity platform.

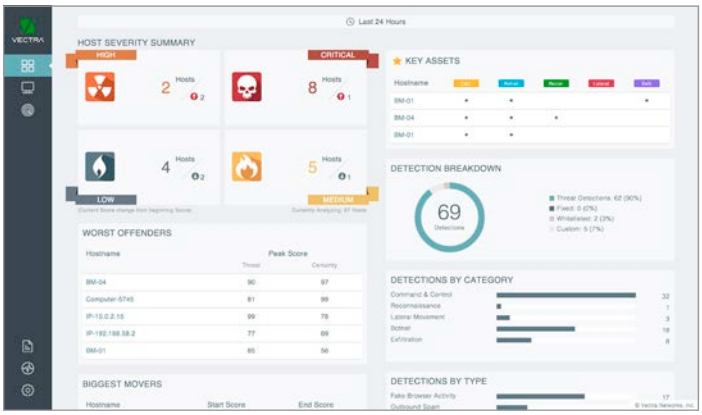
Reports, bulletins and blogs issued by the Vectra Threat Labs zero-in on attackers' goals, place them in the context of the broader campaign that attackers wage, and provide insights into durable ways in which threats can be rapidly detected and mitigated.

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 won't be a constant race against time.

Products

The Vectra cybersecurity platform is based on a flexible, scalable architecture that ensures full visibility into cyber attack behaviors across enterprise networks. Regardless of size or geographic spread, this distributed architecture provides unified threat detection coverage of all network traffic in campuses, remote offices, virtualized data centers and the data center's physical infrastructure.

The Vectra architecture enables customers to deploy X-series software 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.



Metadata collected by physical and virtual sensors is processed by the central Brain and presented in a dashboard that enables security teams to respond quickly and accurately to detected threats

X-series software

Vectra X-series software 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.

Physical S-series sensors

Vectra S-series sensors are easily deployed at remote sites or at access switches on internal network segments to extend the reach of a Vectra deployment. 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 model 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

Vectra vSensors run in VMware ESXi 5.0 or later, making 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. Vectra also integrates with VMware vCenter for an authoritative, always up-to-date view of the virtual environment.

Leadership

Executives

Hitesh Sheth
President and CEO of Vectra

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.

Günter Ollmann
Chief Security Officer

Günter Ollmann is chief security officer at Vectra. He has nearly 30 years of information security experience and cybersecurity consulting and research. Before Vectra, Ollmann was CTO of domain services at NCC Group, where he led the company's generic Top Level Domain (gTLD) program. He was also CTO at IOActive, CTO and vice president of research at Damballa, and chief security strategist at IBM.

Oliver Tavakoli
Chief Technology Officer

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
Chief Financial Officer

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.

Jason Kehl
Vice President of Engineering

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.

Kevin Moore
Senior Vice President of Worldwide Sales

Kevin Moore is senior vice president of worldwide sales at Vectra. 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.

Kevin Kennedy
Vice President of Product Management

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 cyber attacks. 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.

Rick Geehan
Vice President of Sales for North America

Rick Geehan is vice president of sales for North America at Vectra, where he brings more than 20 years of sales and sales management experience. Prior to joining Vectra, he was director of Western Region sales in the United States and Canada at Riverbed Technologies. Geehan joined Riverbed from Silver Peak Systems, where he was the director of Western region sales.

Mike Banic
Vice President of Marketing

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.

Gerard Bauer
Vice President of EMEA

Gerard Bauer is vice president of EMEA at Vectra. Before Vectra, he held key sales leadership roles at Riverbed Technologies, 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. Messina is the chairman of Organizing for Action, an advocacy group that promotes the president's policies, 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

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 the Center for Internet Security. 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 day-to-day management efforts, including 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.

Email info@vectranetworks.com **Phone** +1 408-326-2020
www.vectranetworks.com

© 2017 Vectra Networks, Inc. All rights reserved. Vectra, the Vectra Networks logo and Security that thinks are registered trademarks and the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra Networks. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.