VECTRA®

The Vectra Networks cybersecurity platform

HIGHLIGHTS

- Finds active attackers inside your network
- Automates security investigations with conclusive answers
- Persistently tracks threats across all phases of attack
- Monitors all traffic – internal and Internet
- Covers all devices – Any operating system, BYOD and IoT
- Secures all infrastructure – physical and virtual
- Integrates with leading SIEMs, firewalls, NAC, and endpoint solutions

The Vectra® Networks cybersecurity platform provides the fastest, most efficient way to find and stop attackers in your network by delivering real-time attack visibility and putting attack details at your fingertips to empower immediate action.

Machine learning software from Vectra performs non-stop, automated hunting with always-learning behavioral models to quickly and efficiently find hidden and unknown attackers before they do damage.

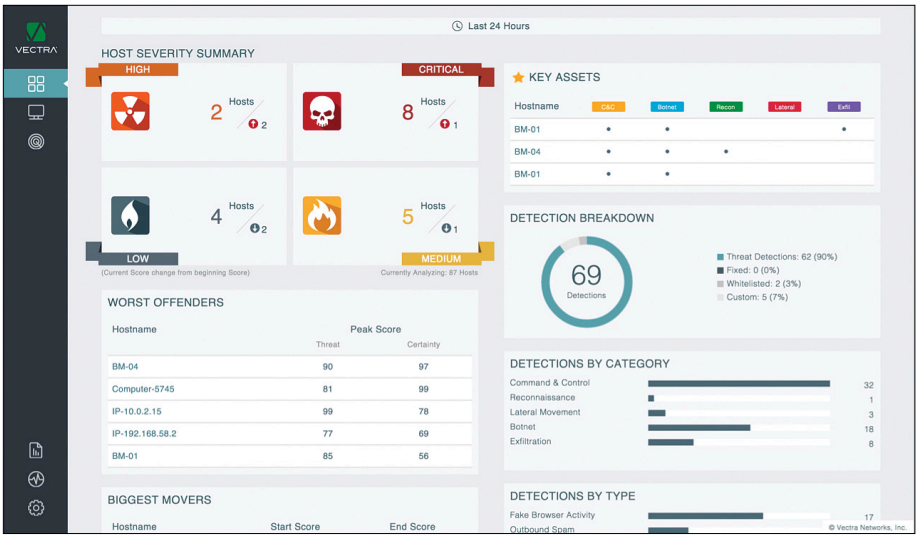
Vectra also delivers blind-spot-free coverage by directly analyzing all network traffic to gain high-fidelity visibility into the actions of all devices—including IoT—from campus to datacenter to cloud, leaving attackers with nowhere to hide.

By providing continuous, automated threat surveillance throughout the enterprise network, Vectra proactively exposes hidden and unknown cyber attackers as they spy, spread and steal.

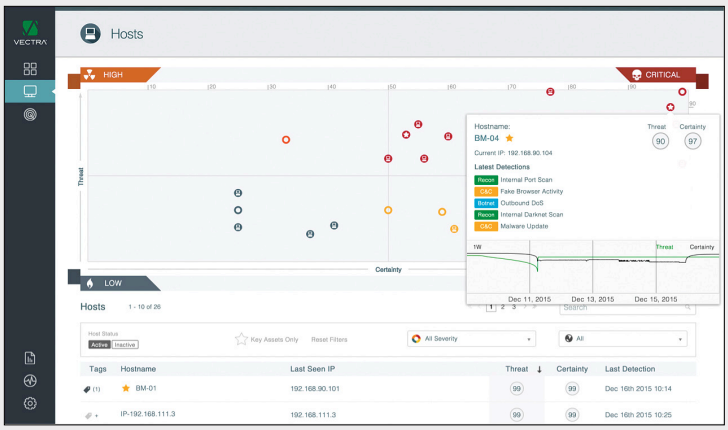
Vectra is based on a simple principle for finding hidden threats: Go to an authoritative source of data and seek out the fundamental threat behaviors that attackers simply can't avoid.

To do this, Vectra goes to the only source of truth that is independent and trusted during a cyber attack – network traffic. Logs only provide low-fidelity summaries of events that have already been seen, not what has been missed. Likewise, endpoint security is easy to compromise during an active intrusion. Only the traffic on the wire reveals the truth with full fidelity and independence.

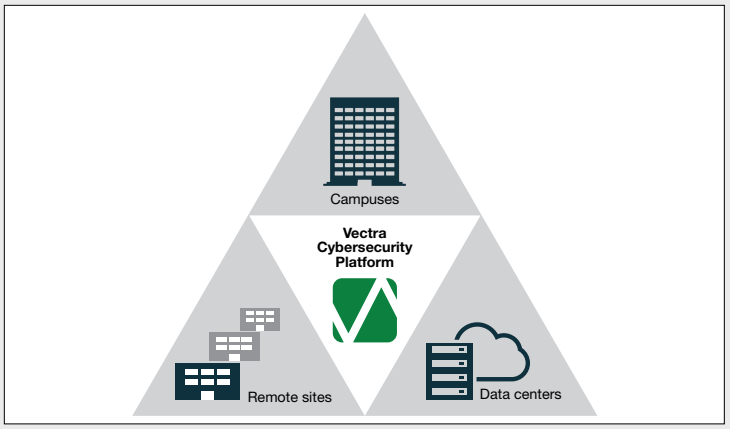
The Vectra core innovation is based on a new way of analyzing network traffic. Instead of traditional payload inspection, Vectra has developed groundbreaking behavioral traffic analysis that exposes the fundamental behaviors of attackers who are inside the network.



Vectra dashboard



Vectra Threat Certainty Index™



Threat detection coverage across the entire enterprise

The platform persistently tracks threats over time and across all phases of an attack, automatically delivers conclusive detections, and eliminates the need for security analysts to endlessly hunt and investigate.

Vectra covers the entire enterprise equally, leaving attackers with nowhere to hide. Every physical or virtual host with an IP address are persistently tracked, regardless of operating system, including laptops, servers, printers, personal smart-devices, and IoT devices.

In addition to the physical infrastructure, Vectra brings native visibility and attack detection to your virtualized data center and private cloud operations. By leveraging behavioral detection models instead of payload-based analysis, Vectra is able to detect threats within SSL/TLS encrypted traffic without the need for decryption.

Security that Thinks®

Real-time attack visibility

Vectra continuously and automatically hunts for hidden and unknown attackers inside your network perimeter. Unique behavioral-detection algorithms constantly learn from your local environment and from global trends to reveal the fundamental behaviors at the root of a cyber attack. By focusing on the inherent actions of attackers, Vectra lets you to stay ahead of attackers and stop them before they do damage.

The intelligence to reveal all phases of attack

Vectra brings together security research and cutting-edge data science to identify the behavior of malware as well as external and internal human attackers inside your network.

Unlike solutions that only look for abnormal or outlier behavior, Vectra threat intelligence deterministically identifies the fundamental techniques of a cyber attack, such as the use of remote access tools, hidden tunnels, botnet behaviors, and reconnaissance tools.

Vectra also constantly learns your local environment and persistently tracks all hosts, both physical and virtual. This allows Vectra to recognize if a host has been compromised and if it is enabling an attacker to move laterally in the network or steal data. The combination of deterministic and anomaly-based detections ensures that Vectra retains a complete view of any active attack.

Blind-spot-free detection coverage

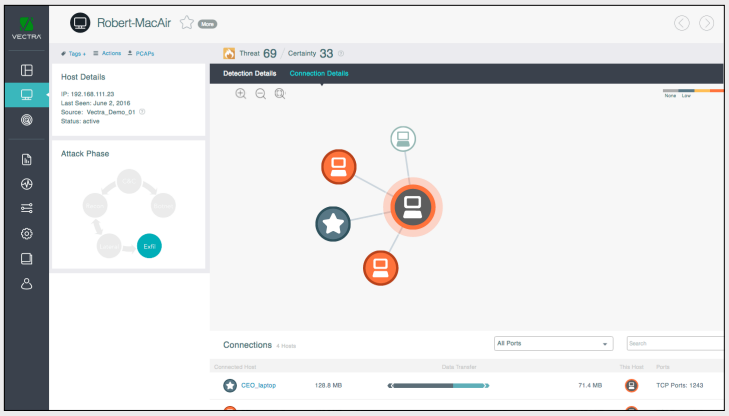
Vectra monitors all of your network traffic, including Internet traffic, internal traffic between hosts, and traffic between workloads in your private-cloud data center.

By focusing on monitoring the real-world actions of devices, Vectra provides equal coverage for all hosts, including BYOD devices, IoT devices, laptops, servers, virtual assets, as well as the physical infrastructure of your network, such as routers, switches and firewalls.

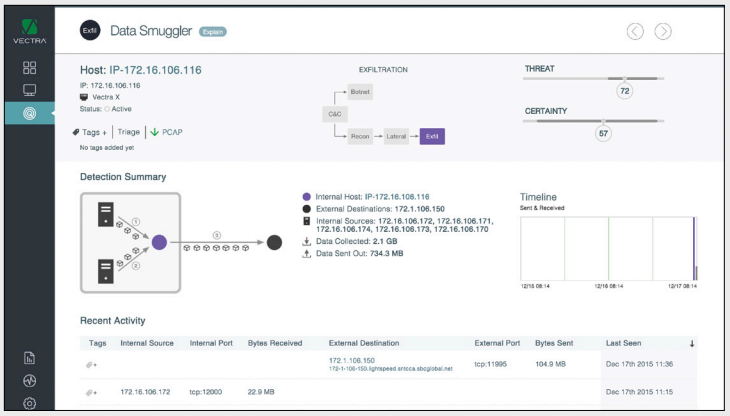
Vectra extends this level of visibility to all parts of your enterprise network infrastructure. From campuses, to remote offices, to data centers, to the cloud, Vectra leaves attackers with nowhere to hide.

Find the greatest threat with certainty

The Vectra Threat Certainty Index™ consolidates thousands of low-level events and network history to pinpoint the individual hosts that pose the greatest threat to your network. Scores take into account historical context of the host over time as well as the progression through the attack lifecycle.



Host connectivity details



Real-time detection of data exfiltration in progress

Threat and certainty scores can be used to trigger notifications to your security team, trigger a response from existing enforcement solutions, or provide a precorrelated starting point for investigations within a SIEM or forensic tools. Vectra ensures that action is taken quickly and without the need for manual analysis.

Security context that saves staff time

Vectra unburdens and empowers your most limited resources – the time and skill of your security team. Vectra automates the time-consuming Tier 1 analysis of security events and eliminates the need for security teams to endlessly hunt and search for threats.

Each detection is explained in detail, along with the underlying event and historical context that led to the detection. Security analysts can instantly view a connection map of any host to see other hosts the device is communicating with and how.

Vectra also provides on-demand access to packet captures for further forensic analysis. This enables security teams to quickly get to the point that matters with proof, so they can take immediate, decisive action.

Strengthen your existing security infrastructure

Whether providing the intelligence to block a new class of threat with existing enforcement points such as firewalls, endpoint security and NAC, or providing a clear starting point for a more extensive search with SIEMs and forensic tools, Vectra helps you get more value out of your existing security technologies and teams.

Vectra integrates with leading endpoint security solutions to automatically add enriched context to investigations and enables IT security teams to isolate compromised host devices.

A robust API enables automated response and enforcement with virtually any security solution. Vectra also generates syslog messages and CEF logs for all detections as well as precorrelated host scores. This makes Vectra much more than just another source of logs and provides an ideal trigger for investigations and workflows from your SIEM.

Full lifecycle detection of ransomware

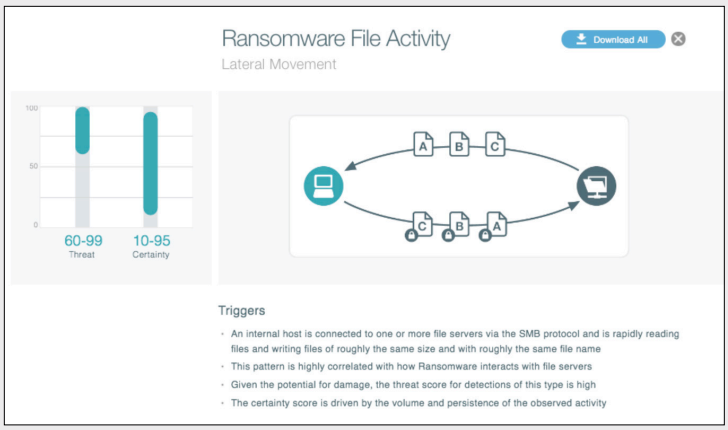
Vectra detects ransomware campaigns against enterprises and other organizations across all phases of an attack. By monitoring all internal network traffic, Vectra identifies in seconds the fundamental behaviors of a ransomware attack as it attempts to take critical assets hostage.

In addition to detecting ransomware directly, Vectra detects command-and-control traffic used by ransomware, as well as the network scans and spreading behavior that malware relies on to find and seize critical assets.

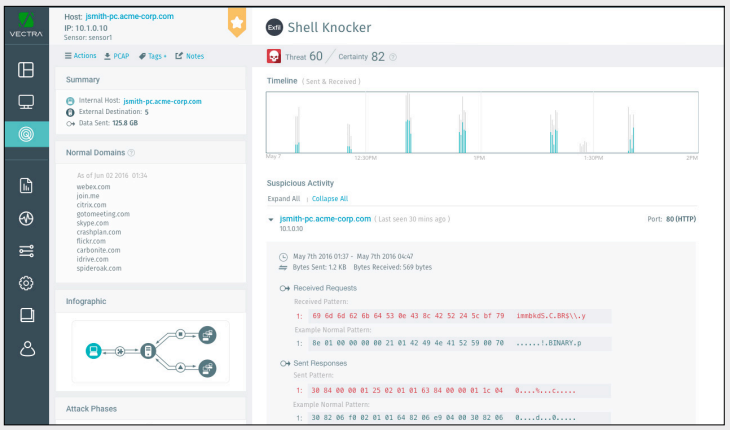
Watching the watchers

While attackers may initially compromise an end-user device, the real prize involves commandeering administrator or system credentials. Vectra goes beyond simple user-behavior monitoring to detect signs of compromised administrators.

Vectra tracks administrative protocols and learns the specific machines or jump systems that are used to manage specific assets. This vigilance quickly reveals when a cybercriminal attempts to use administrative privileges to escalate an attack on the network.



Vectra ransomware detection



Vectra Shell Knocker detection

Native security for your private cloud

The private-cloud data center has become the heart and soul of many organizations, yet often remains a blind spot for security teams. Vectra persistently monitors critical data center applications, data, and infrastructure with the ability to detect even the most sophisticated attacks.

Some 80% of data center traffic never leaves the data center and is not monitored by traditional perimeter-based security. Vectra's virtual sensors (vSensors) connect to any VMware vSwitch to ensure visibility into all traffic and detect threats passing between workloads in the virtual environment.

Vectra also integrates with VMware vCenter to provide an authoritative, always up-to-date view of your virtual environment. Vectra is the first vendor to bring together the required visibility, context and intelligence to find advanced attacks inside the data center.

Security from hardware to workload

Data center security goes beyond virtualization and includes the physical server hardware and low-level tools used to manage the data center. Vectra provides unprecedented threat detection that extends from the application layer down to the underlying hardware.

For example, the Vectra Port Knocking detection reveals servers that are compromised by a rootkit, which could reside below the physical operating system itself. In addition, Vectra monitors and detects the improper use of low-level management protocols such as IPMI and iDRAC.

Normally used by administrators for lights-out management of server hardware, these protocols are increasingly targeted by attackers because they give an always-on backdoor into the virtual environment yet are not logged and are rarely monitored by security.

Unifying data center operations

Modern data centers require constant coordination between networking, application development, virtualization teams, and of course, the security team. Vectra makes it easy for all groups to remain in sync and retain full visibility into the virtual environment, even when workloads are constantly on the move.

Vectra visually displays the connections between all workloads and the type of traffic flowing between them. With full VMware vCenter integration, Vectra provides an always up-to-date view of the environment and alerts about any assets that are not monitored for threats.

VECTRA®

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