Adaptive distributed architecture

Vectra® Networks automates the detection of cyber attacks in real time by detecting all active phases of an attack – including command and control, internal reconnaissance, lateral movement, and exfiltration – from campuses to remote sites to data center and the cloud.

Overview

Today's cyber security threat landscape is highly dynamic with attackers constantly morphing malware and attack vectors to evade detection, and persistently attacking your information assets. There are also many infections that will occur outside the perimeter – from mobile users with BYOD or IoT devices as well as from connected partners.

Recent breaches all follow the same blueprint of attackers gaining privileged access, extending the compromise across the network and stealing or destroying data. These cyber attacks are evading the perimeter security systems that are designed to stop an attacker from entering.

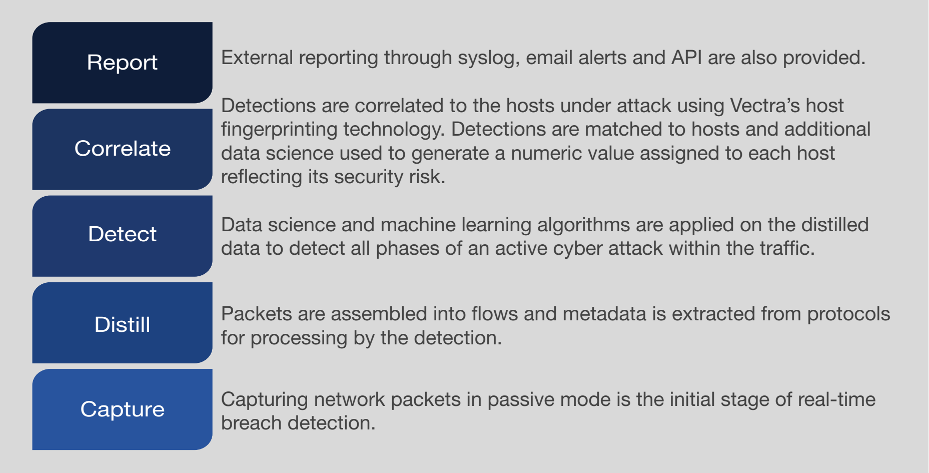
The breach at retailer Target began with keylogger malware installed on a computer at its business partner Fazio Mechanical. By infecting computers at Fazio Mechanical, the attackers used stolen credentials to gain access to the Target network, spread laterally, locate key assets, accumulate data and exfiltrate it.

Automating the detection of attacks in progress

To pinpoint cyber attacks that bypass the network perimeter, security professionals need a high-fidelity solution that automates real-time threat detection and reporting, while reducing false negatives and false positives.

That's what Vectra does. Combining data science, machine learning and behavioral analysis, Vectra monitors all network traffic and detects active threats in real time in every active phase of a cyber attack.

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



Report

External reporting through syslog, email alerts and API are also provided.

Correlate

Detections are correlated to the hosts under attack using Vectra's host fingerprinting technology. Detections are matched to hosts and additional data science used to generate a numeric value assigned to each host reflecting its security risk.

Detect

Data science and machine learning algorithms are applied on the distilled data to detect all phases of an active cyber attack within the traffic.

Distill

Packets are assembled into flows and metadata is extracted from protocols for processing by the detection.

Capture

Capturing network packets in passive mode is the initial stage of real-time breach detection.

The Vectra architecture

Why cyber attackers succeed

Efficacy increases when this solution has visibility into traffic across the entire attack surface – including campuses and internal neworks segments, remote sites, data centers, and the cloud – where key assets are located.

Challenges in campus networks

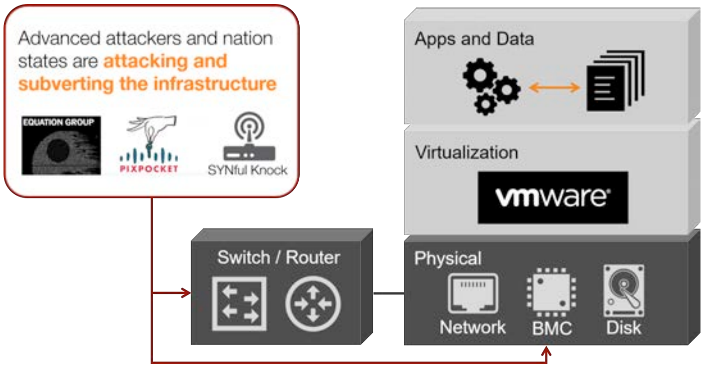
Despite having next-generation firewalls, IDS/IPS and malware sandboxes, cyber attackers can evade the strongest perimeter security and spread inside networks. That's because perimeter defense systems only keep out known threats.

Perimeter defenses rely on signatures and reputation lists of known threats and must be continually updated. 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 new bits of code 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 – the underlying physical infrastructure

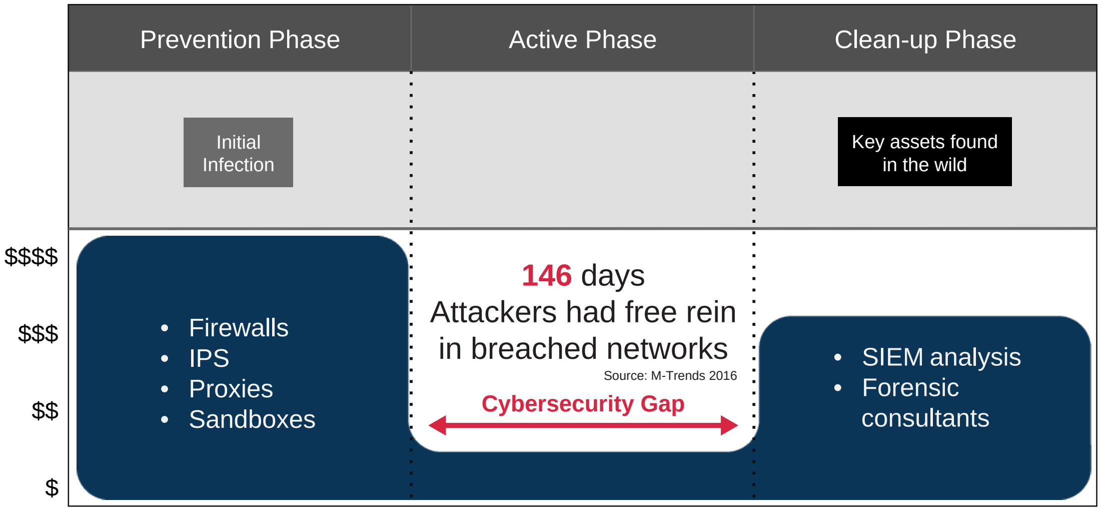
Instead of launching exploits or malicious payloads at data center resources, cyber attackers prefer to use a position of trust to make their way closer to key assets. They covertly hijack administrative credentials, elevate their privileges, and plant rootkits and backdoors in the physical infrastructure.

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 where no one is watching.

Challenges across the entire infrastructure

Security analysts today are also 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, hunt and search for the most serious threats, and then mitigate attacks before they spread. Security teams often don't know what to look for or where.



Source: M-Trends 2016

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

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 solution

From campuses to data centers to private clouds, Vectra provides continuous, automated threat surveillance throughout the organization 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.

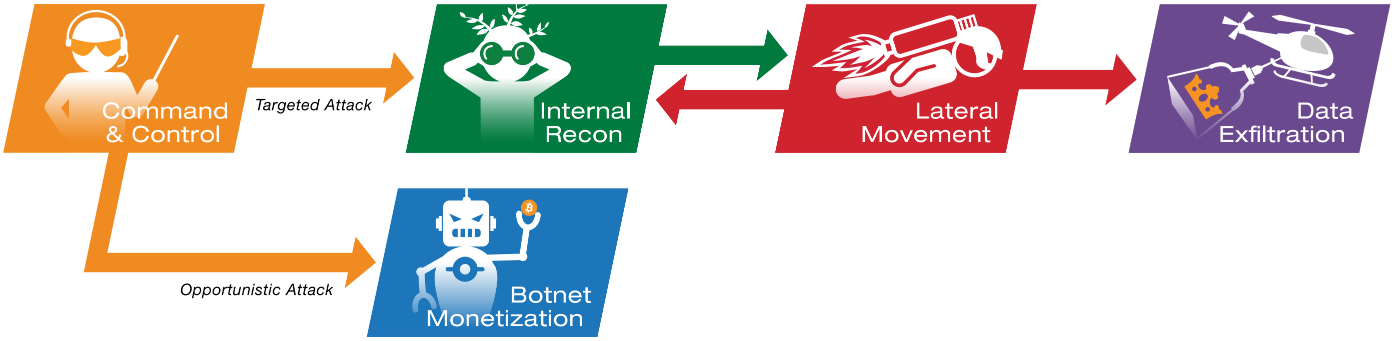
Vectra delivers a new, automated way of analyzing network traffic at scale. Instead of traditional payload inspection, Vectra uses artificial intelligence, machine learning and behavioral traffic analysis to expose the fundamental behaviors of attackers as they spy, spread, and steal in the network.

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

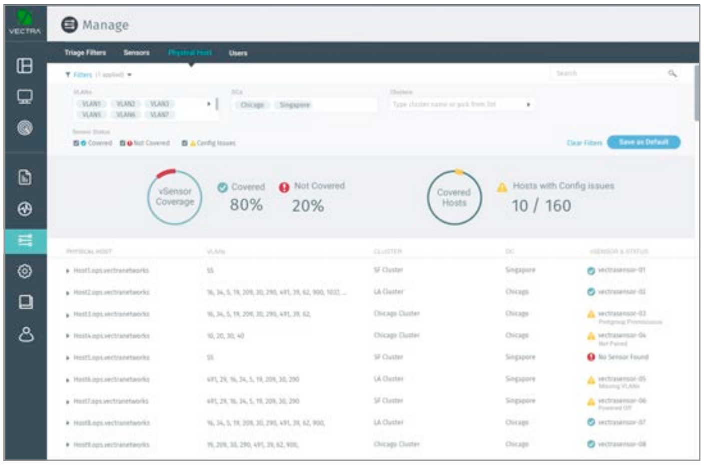
Vectra continuously learns the local network environment and tracks all physical and virtual hosts to reveal signs of compromised devices as well as insider threats.



Vectra detects active threats across all phases of a cyber attack

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.


Manage

Triage Filters | Sensors | Physical Host | Users

Filters (1 applied)

VLANs: VLAN1 VLAN2 VLAN3 VLAN5 VLAN6 VLAN7

DCs: Chicago Singapore

Clusters: Type cluster name or pick from list

Sensor Status: ☑ Covered ☑ Not Covered ☑ Config Issues

Clear Filters | Save as Default

vSensor Coverage: Covered 80% | Not Covered 20%

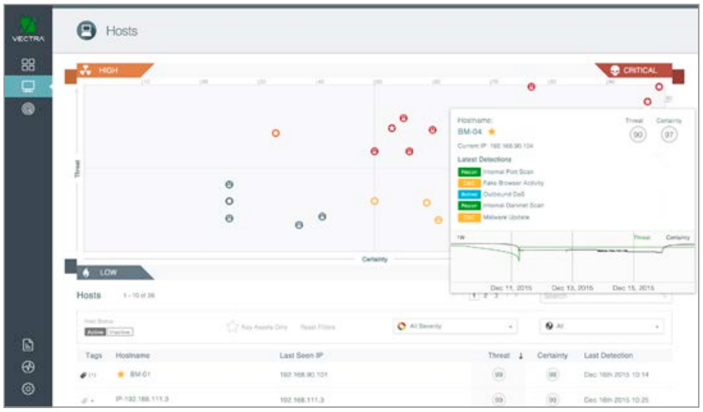
Covered Hosts: Hosts with Config issues 10 / 160

PHYSICAL HOST	VLANs	CLUSTER	DC	vSENSOR & STATUS
Host1.ops.vectranetworks	55	SF Cluster	Singapore	vectrasensor-01
Host2.ops.vectranetworks	16, 34, 5, 19, 209, 30, 290, 491, 39, 62, 900, 1032, ...	LA Cluster	Chicago	vectrasensor-02
Host3.ops.vectranetworks	16, 34, 5, 19, 209, 30, 290, 491, 39, 62,	Chicago Cluster	Chicago	vectrasensor-03 Portgroup Promiscuous
Host4.ops.vectranetworks	10, 20, 30, 40	Chicago Cluster	Chicago	vectrasensor-04 Not Paired
Host5.ops.vectranetworks	55	SF Cluster	Singapore	No Sensor Found
Host6.ops.vectranetworks	491, 29, 16, 34, 5, 19, 209, 30, 290	LA Cluster	Singapore	vectrasensor-05 Missing VLANs
Host7.ops.vectranetworks	491, 29, 16, 34, 5, 19, 209, 30, 290	SF Cluster	Singapore	vectrasensor-06 Powered Off
Host8.ops.vectranetworks	16, 34, 5, 19, 209, 30, 290, 491, 39, 62, 900,	LA Cluster	Chicago	vectrasensor-07
Host9.ops.vectranetworks	19, 209, 30, 290, 491, 39, 62, 900,	Chicago Cluster	Chicago	vectrasensor-08

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. Vectra boils 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 and automate SIEM workflows.



Hosts

Hostname: BM-04 ★ | Threat 90 | Certainty 97

Current IP: 192.168.90.104

Latest Detections
- Recon: Internal Port Scan
- C&C: Fake Browser Activity
- Botnet: Outbound DoS
- Recon: Internal Darknet Scan
- C&C: Malware Update

Hosts 1 - 10 of 36

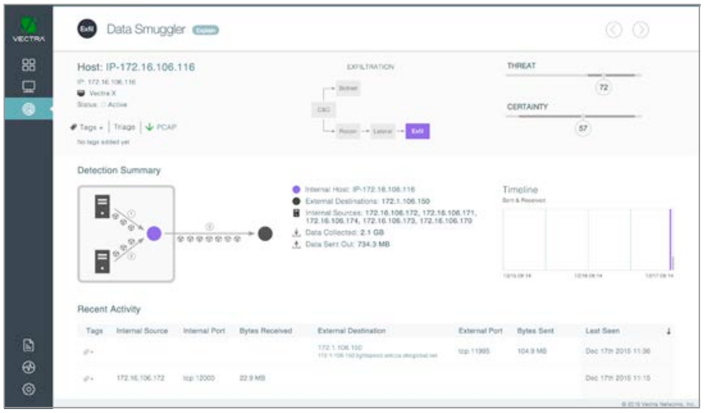
Host Status: Active | Inactive — Key Assets Only — Reset Filters — All Severity — All

Tags	Hostname	Last Seen IP	Threat	Certainty	Last Detection
(1)	★ BM-01	192.168.90.101	99	99	Dec 16th 2015 10:14
+	IP-192.168.111.3	192.168.111.3	99	99	Dec 16th 2015 10:25

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. And on-demand access to packet captures speeds-up forensic analysis to enable quick, decisive action.



Data Smuggler

Host: IP-172.16.106.116

IP: 172.16.106.116

Vectra X

Status: Active

Tags | Triage | PCAP

No tags added yet

THREAT 72

CERTAINTY 57

Detection Summary

- Internal Host: IP-172.16.106.116
- External Destinations: 172.1.106.150
- Internal Sources: 172.16.106.172, 172.16.106.171, 172.16.106.174, 172.16.106.173, 172.16.106.170
- Data Collected: 2.1 GB
- Data Sent Out: 734.3 MB

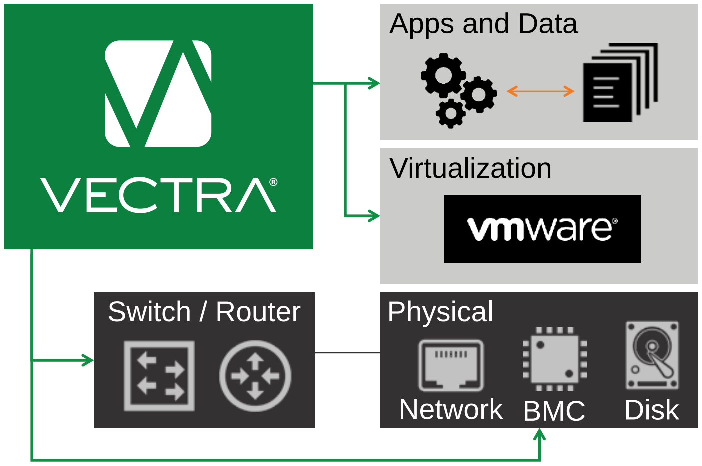
Recent Activity

Tags	Internal Source	Internal Port	Bytes Received	External Destination	External Port	Bytes Sent	Last Seen
+				172.1.106.150 172.1.106.150.lightspeed.wlcca.sbcglobal.net	tcp:11985	104.9 MB	Dec 17th 2015 11:36
+	172.16.106.172	tcp:12000	22.9 MB				Dec 17th 2015 11:15

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 your private cloud

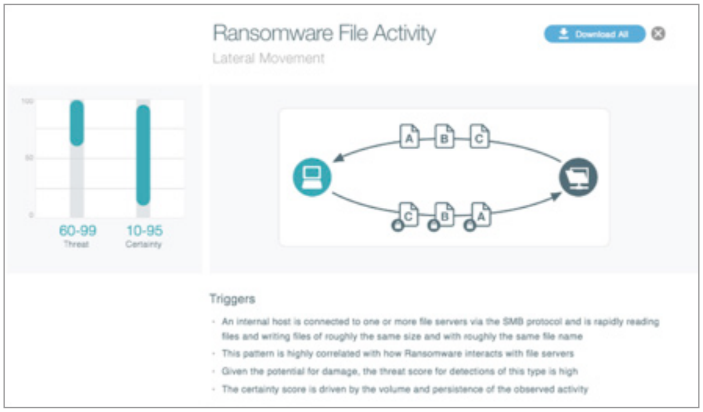
Vectra monitors the virtualized layer of the data center and its underlying infrastructure to detect complex attacks. Vectra vSensors provide visibility into all traffic passing between virtual workloads, while native integration with VMware vCenter offers an always up-to-date view of virtual and physical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



Ransomware File Activity

Lateral Movement

Triggers

- An internal host is connected to one or more file servers via the SMB protocol and is rapidly reading files and writing files of roughly the same size and with roughly the same file name
- This pattern is highly correlated with how Ransomware interacts with file servers
- Given the potential for damage, the threat score for detections of this type is high
- The certainty score is driven by the volume and persistence of the observed activity

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

Components of the Vectra architecture

The Vectra 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.

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.

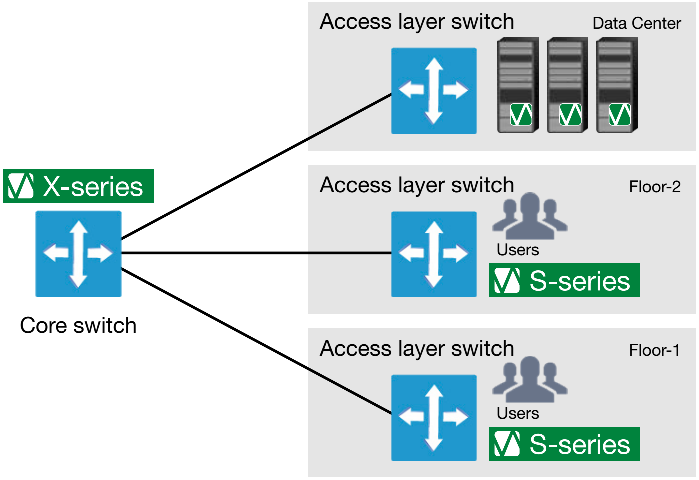
X-series appliances

The X-series is deployable 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.

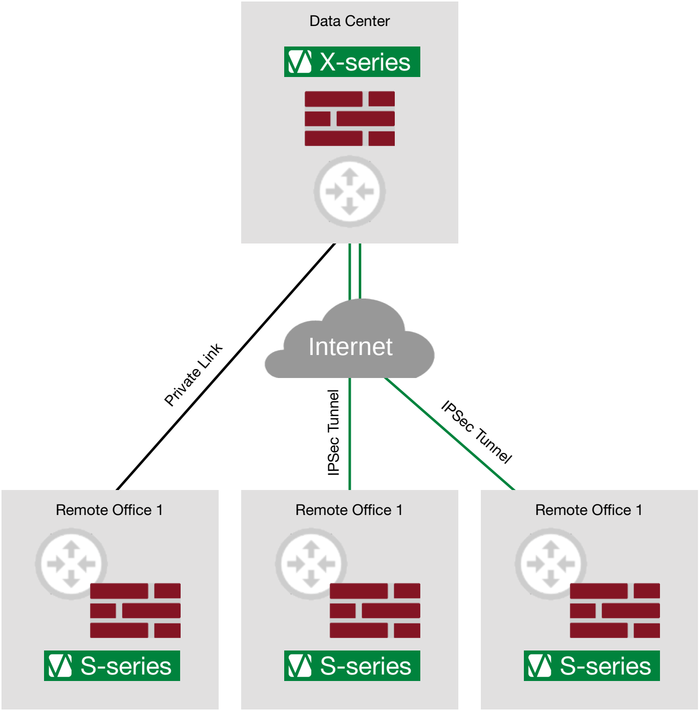
Deploying a distributed architecture

The scalable Vectra distributed architecture ensures that you have consistent cybersecurity protection across your entire organization, regardless of size or geographical distribution.

S-series sensors, vSensors and X-series appliances scale to accommodate any size network across geographically dispersed locations – campuses, remote sites, data centers, and the cloud – to deliver centralized analysis, detection and correlation of threats.



- Physical sensors deployed at the access layer switch provide visibility into user-to-user traffic
- vSensors in the data center can connect to any VMware vSwitch to provide visibility into all traffic and detect threats that pass between virtual workloads
- X-series deployed at the core/distribution layer provides visibility into traffic to and from users to Internet, and correlates detections from physical sensors and vSensors



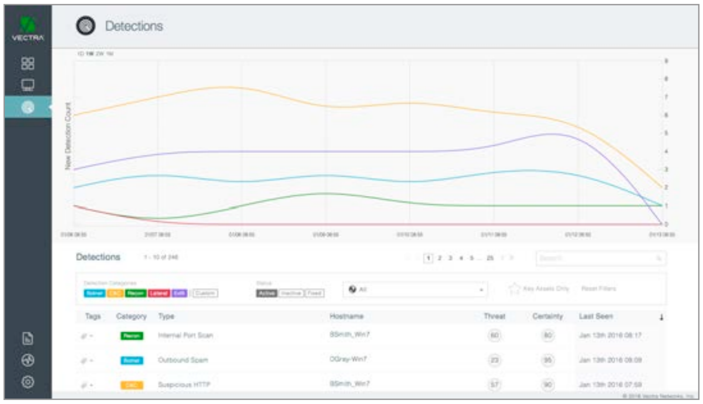
- Physical sensors deployed remotely provide visibility into traffic at remote sites
- X-series deployed at the data center provides centralized visibility into traffic and correlates detections from sensors

Benefits of a distributed architecture

The Vectra distributed architecture provides the following benefits:

- Plug-and-play deployment
  - Physical sensors are provisioned with customer information before shipment by Vectra
  - Sensors obtain their network configuration from a DHCP server in the network. This helps with deployments in remote sites with very little technical expertise
  - Sensors can be deployed in passive mode or in-line as a bump-in-the-wire with fail-open
  - vSensors are easily deployed as a virtual image
- Low bandwidth utilization
  - Physical sensors and vSensors distill metadata from traffic and send it to the X-series for threat analysis and reporting
  - The metadata from physical sensors and vSensors to the X-series is compressed to less than 1% of the received bandwidth to reduce overhead on low-bandwidth network links
- Extends full-fidelity traffic visibility
  - Remote sites are weak links in the attack surface. Sensors can be easily deployed at remote locations to strengthen network security at remote sites
  - Sensors are deployed on internal segments with key assets to detect lateral spread and data accumulation
  - Full visibility of intra-workload traffic within the data center
- Automatic centralized reporting
  - X-series appliances provide a unified view of an organization's risk profile by aggregating and correlating all detections
  - X-series appliances enable security operations team to filter threat detections based on sensor monitoring the suspect traffic
  - X-series appliances provide automatic real-time reporting, empowering organizations with the relevant data to rapidly respond to attacks, which saves time and manpower
- Automatic software updates
  - The Vectra cloud provides updates to the X-series
  - Updates are downloaded automatically to physical sensors and vSensors from the X-series

The user interface below shows detections viewed from the X-series deployed in a distributed architecture.



Detections 1 - 10 of 246

1 2 3 4 5 … 25

Detection Categories: Botnet C&C Recon Lateral Exfil Custom

Status: Active Inactive Fixed

All

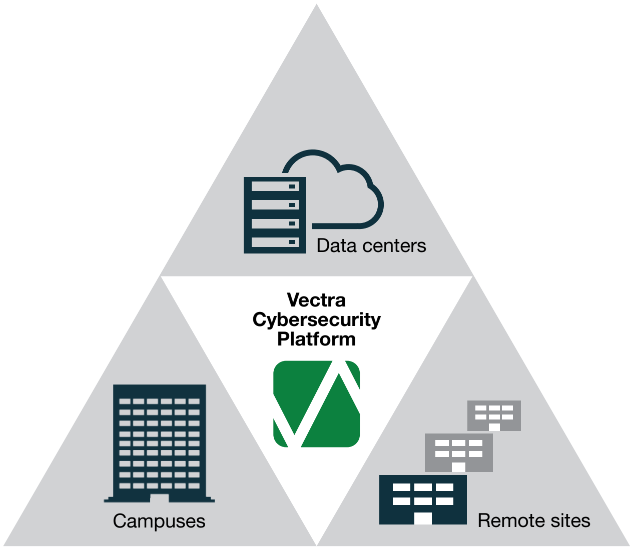
Tags	Category	Type	Hostname	Threat	Certainty	Last Seen
	Recon	Internal Port Scan	BSmith_Win7	60	80	Jan 13th 2016 08:17
	Botnet	Outbound Spam	OGray-Win7	23	95	Jan 13th 2016 08:09
	C&C	Suspicious HTTP	BSmith_Win7	57	90	Jan 13th 2016 07:59

© 2016 Vectra Networks, Inc.

Detection view of the X-series

Summary

Vectra technology picks up where perimeter security leaves off by providing deep, continuous analysis of internal and Internet network traffic to automatically detect all phases of an attack – from campuses to remote sites to data centers and the cloud.



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

The Vectra scalable distributed architecture, represented by the S-series sensors, vSensors and X-series platforms, scales to accommodate any size network across geographically dispersed sites while delivering the centralized analysis, detection and correlation of threats.

VECTRA®
Security that thinks®

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