VECTRA™
Security that thinks™

PRODUKTDATENBLATT

Plattformen der X-Serie und Sensoren der S-Serie

HIGHLIGHTS

- Entdeckung von Angriffen unabhängig von der Methode und dem Ort des ursprünglichen Eindringens
- Bedrohungsmeldung über mehrere Phasen eines komplexen, zielgerichteten Angriffs
- Erstellung klarer, intuitiver Berichte und Bereitstellung aller unterstützenden Daten mit einem Klick
- Anzeige von Threat- und Certainty-Updates in Echtzeit während eines aktiven Angriffs
- Entdeckung von Bedrohungen ohne Signaturen mithilfe einer Kombination aus Data Science und maschinellem Lernen
- Erkennung von Angriffen auf allen Betriebssystemen, Anwendungen, Geräten und Browsern.
- Zum Einsatz im passiven Modus an einem SPAN- oder Tap-Port

Vectra Networks präsentiert ein neuartiges Verteidigungssystem gegen APT-Angriffe zur Echtzeit-Erkennung von Bedrohungen und Analyse von aktiven, unbefugten Netzwerkzugriffen. Die Vectra-Technologie setzt dort an, wo Perimetersicherheit aufhört; die Bereitstellung einer gründlichen, kontinuierlichen Analyse des internen sowie des Internet-Netzwerkverkehrs ermöglicht die automatische Erkennung aller Phasen eines unbefugten Zugriffs, beim Versuch der Spionage, des Datendiebstahls und der Ausbreitung eines Angreifers in Ihrem Netzwerk.

Durch eine Kombination aus Methoden der Data Science, maschinellen Lernverfahren sowie der Verhaltensanalyse erkennt Vectra proaktiv die Anwesenheit bekannter und unbekannter Bedrohungen und erfordert dabei keine Signaturen oder komplizierte Konfiguration.

Alle Entdeckungen werden automatisch ausgewertet, korreliert und die größten Bedrohungen schnell priorisiert, so dass Sie den Angriff stoppen und seine Auswirkungen eindämmen können.

Entdeckt alle Phasen eines Angriffs

Der Erfolg eines modernen Angreifers basiert auf dessen Fähigkeit, auszuharren und sich methodisch in einem Netzwerk ausbreiten zu können, um sich auf diese Weise letztendlich Zugang zu wichtigen Assets zu verschaffen.

Selbst der anspruchsvollsten Perimetersicherheitstechnologie fehlt die nötige interne Transparenz, um diese Bedrohungen zu erkennen. Vectra bietet eine kontinuierliche Analyse des internen Netzwerkverkehrs und ermöglicht somit die automatische Erkennung aller Phasen dieser schleichenden Angriffe, einschließlich interner Reconnaissance, der internen Verbreitung von Malware, des Diebstahls von Kontozugangsdaten, der Akkumulation von Daten, Datendiebstahl und einer Vielzahl von anderen versteckten Kommunikationsaktivitäten. Alle entdeckten Bedrohungen werden automatisch korreliert, um so den wahren Umfang und Verlauf eines Angriffs leicht sichtbar zu machen.

Security that Thinks™ — Ein Sicherheitssystem, das mitdenkt

Die Vectra-Plattform überwacht, erlernt und merkt sich Verhaltensweisen kontinuierlich und kann dadurch Bedrohungen automatisch entdecken und den nächsten Schritt eines Cyber-Angreifers antizipieren. Durch den Einsatz einer zum Patent angemeldeten Methode der Data Science und maschinellem Lernen kann Vectra Sicherheitsbedrohungen ohne Signaturen oder Reputationslisten erkennen, gerade wenn die Bedrohung oder das Angriffstool vorher noch nie eingesetzt wurde.

Priorisierte Bedrohungserkennung

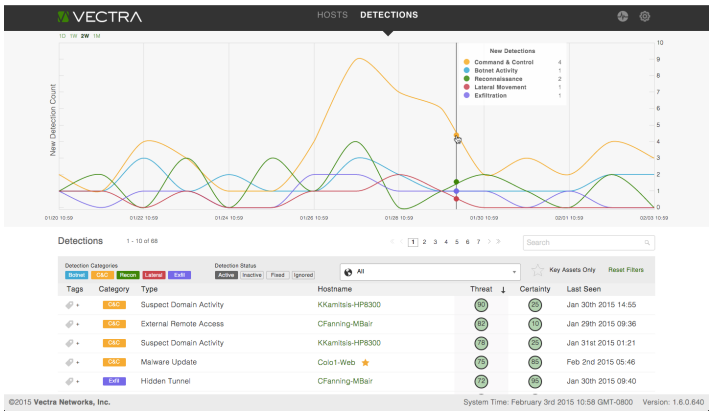
Vectra liefert priorisierte und kontextuelle Warnungen und ermöglicht dadurch ein schnelles und entschlossenes Handeln, um einen Angriff zu stoppen. Warnungen werden automatisch pro Host korreliert und auf dem intuitiven Threat Certainty Index™ angezeigt. Der Threat Certainty Index liefert eine visuelle Darstellung der spezifischen Netzwerk-Hosts, die Angriffsindikatoren der höchsten Gewissheitstufe (Certainty) aufweisen und das höchste Risiko für die Organisation darstellen.

Aufschlussreiches Reporting in Echtzeit

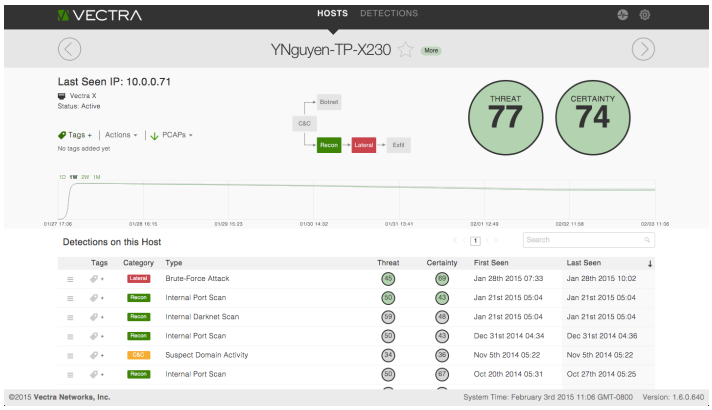
Vectra-Plattformen zeigen intuitiv das Fortschreiten einer Bedrohung über mehrere Phasen eines Angriffs an und ermöglichen einen schnellen Zugriff auf alle Detailebenen. Die Benutzeroberfläche zeigt die Phase des Angriffs und eine Zusammenfassung der entdeckten Bedrohung an. Details zum Angriff können mit nur einem Klick aufgerufen werden. Dort können die exakten Pakete zwischen dem kompromittierten Host in Ihrem Netzwerk und weiteren angegriffenen, internen Ressourcen oder externe Parteien, mit denen der Angreifer kommuniziert, angezeigt werden.

Eine Rundumlösung

Moderne Netzwerke und das „Internet der Dinge" umfassen oft eine verwirrende Anzahl von Geräten, Betriebssystemen und Anwendungen und es ist praktisch unmöglich, dass Signaturen, Sandboxen, Host-Detailansichten und Endpoint-Agenten diese alle unterstützen. Durch die Anwendung von Methoden der Data Science kann Vectra im Netzwerk beobachtete Verhaltensweisen und Muster des Datenverkehrs analysieren und Bedrohungen auf der gesamten, äußerst variablen Angriffsfläche erkennen.



Ansicht der erkannten Gefahren



Host-Detailansicht

Sofort einsatzbereit

Vectra-Plattformen werden im passiven Modus eingesetzt und sind in unterschiedlichen Bauformen erhältlich und ermöglichen Ihnen so die uneingeschränkte Einsicht in Ihr Netzwerk. Die Plattformen der All-in-One-X-Serie eignen sich für große Netzwerkinfrastrukturen und werden häufig in der Nähe der zentralen Netzwerk-Switche oder WAN-Gateways eingesetzt, wo sie den gesamten Benutzerdatenverkehr zum Internet und zu Ihrem Rechenzentrum überwachen können. Die Sensoren der S-Serie arbeiten in Verbindung mit einer X-Serien-Plattform und bieten so eine erweiterte Abdeckung zur Überwachung des Datenverkehrs von Access Layer-Switchen oder Remote-Arbeitsplätzen. Die Implementierung beider Vectra-Lösungen ist sehr einfach und voll automatisiert. Konfigurieren Sie einfach die Management-IP-Adresse und die Plattform erlernt alle weiteren benötigten Details von selbst.

360-Grad-Erkennung

Vectra-Plattformen überwachen kontinuierlich den gesamten Benutzerdatenverkehr zu und von internen Quellen sowie dem Internet. Durch den Einsatz von Methoden der Data Science und des maschinellen Lernens ermöglicht die Vectra-Plattform die automatisierte Erkennung eines Angriffs in jeder Phase, unabhängig von dessen

Ursprung. Durch die kontinuierliche Überwachung von Interaktionen identifiziert Vectra das gefährliche Verhalten von APT-Angriffen.

Immer auf dem neuesten Stand

Mit dem Vectra-Cloud-Service kann Ihre Plattform Änderungen in der Bedrohungslage in Echtzeit wahrnehmen und mittels maschineller Lernverfahren an anderen Standorten beobachtete Verhaltensweisen, die mit neuen Angriffsvektoren verbunden sind, wiedererkennen. Zudem sorgt der Cloud-Service dafür, dass stets die neueste Software ausgeführt wird.

Zum Patent angemeldete Innovation

Vectra-Technologie basiert auf einer branchenweit führenden Architektur, die Methoden der Data Science und des maschinellen Lernens kombiniert einsetzt, um von Cyber-Kriminellen verwendete komplexe Malware sowie APT-Akteure zu erkennen.

Community-Threat-Analyse

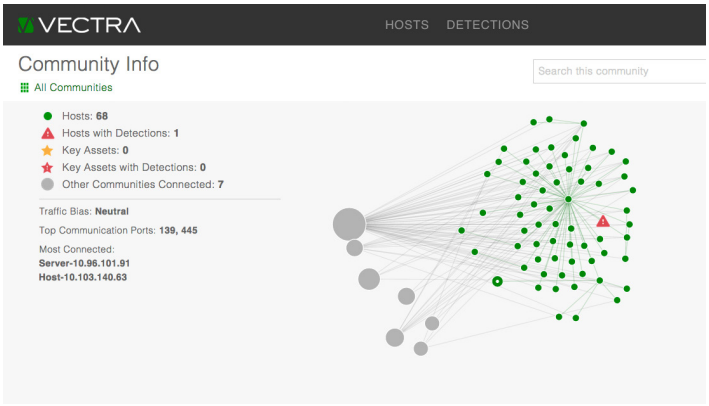
Vectra verwendet maschinelle Lernverfahren, um normale Benutzer- und Gerätegruppen im Netzwerk zu identifizieren. Diese Analyse ermöglicht die automatische Identifizierung der am häufigsten abgerufenen Assets in Ihrem Netzwerk. Gruppen werden logisch zugeordnet und auf der Benutzeroberfläche angezeigt, so dass die Nähe einer entdeckten Bedrohung zu wichtigen Assets und miteinander verbundenen Enduser-Hosts leicht erkannt werden können.

Skalierbare, verteilte Architektur

Die skalierbare, verteilte Architektur von Vectra Networks ermöglicht Kunden die uneingeschränkte Einsicht in ihr Netzwerk, und zwar unabhängig von der Größe und der geografischen Verteilung ihres Unternehmens. Die Sensoren der S-Serie und die X-Serien-Plattformen können auf Netzwerke jeder beliebigen Größe und über unterschiedliche Standorte hinweg skaliert werden und liefern eine zentrale Analyse, Erkennung und Korrelation von Sicherheitsbedrohungen.

Plattformen der X-Serie

Die Software der X-Serien-Plattform ist vorinstalliert auf einem rahmenmontierbaren Gerät in Normalgröße erhältlich, das selbst auf die größten Netzwerke skaliert werden kann. Die X-Serien-Plattform kann daher entweder als ein All-in-One-Gerät zur Überwachung von Datenverkehr und zur Echtzeit-Erkennung von Bedrohungen oder in Kombination mit den Sensoren der S-Serie, die Datenverkehr überwachen und Metadaten von den Sensoren auswerten, eingesetzt werden. Die X-Serien-Plattform führt die Erkennung, Analyse und Korrelation der Bedrohungen auf den Metadaten von Sensoren durch.



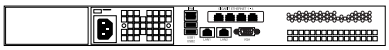
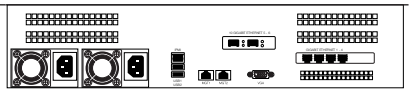
Community-Threat-Analyse

Sensoren der S-Serie

Bei den Sensoren der S-Serie handelt es sich um kleine, spezielle Sensoren, die leicht an Remote-Standorten oder mit Access-Switchen bereitgestellt werden können. Die Sensoren überwachen passiv den Netzwerkverkehr, extrahieren daraus kritische Metadaten und leiten die Metadaten zur Gefährdungsanalyse an eine X-Serien-Plattform weiter. Die kleine Größe und das einfache Bereitstellungsmodell der S-Serie ermöglicht Unternehmen eine umfassende Abdeckung des gesamten Netzwerks, insbesondere von Remote-Standorten, einschließlich in kleinen Büros, Kliniken und Einzelhandelsfilialen.

Warum Vectra

Vectra bietet eine völlig neue Art der Netzwerksicherheit. Vectra ist es gelungen, basierend auf Methoden der Data Science und des maschinellen Lernens eine mitdenkende IT Sicherheitslösung zu entwickeln, die anomale und potenziell gefährliche Verhaltensweisen innerhalb des Netzwerks automatisch erkennt und diese in Echtzeit und mit Kontext meldet, so dass Sie sofort handeln können.

	S2 Sensor	X4 Plattform	X20 Plattform
Capture-Ports	• Vier 10/100/1000BASE-T-Ports	• Vier 10/100/1000BASE-T-Ports	• Vier 10/100/1000BASE-T • Zwei 10 Gigabit Ethernet SFP+
Management-Ports	• Ein 10/100/1000BASE-T Out-of-Band-Support-Port • Ein RJ-45-Serial-Console-Port	• Zwei 10/100/1000BASE-T-Ports • Ein VGA-Video-Port • Zwei USB-2.0-Ports • Ein DB-9-Serial-Port	• Zwei 10/100/1000BASE-T-Ports • Eln VGA-Video-Port • Zwei USB-2.0-Ports • Ein DB-9-Serial-Port
Speicherkapazität	• 1 TB Festplatte	*Raw Storage* • 4 TB Festplatte *Konfigurierter Speicher* • Zwei vollständig redundante 1 TB Festplatten für das Betriebssystem • Zwei 1 TB Festplatten zum Disk-Striping für Daten	*Raw Storage* • 6.8 TB Festplatte *Konfigurierter Speicher* • Zwei vollständig redundante 1 TB Festplatten für das Betriebssystem • Acht 600 GB Festplatten zum Disk-Striping für Daten
Eingangsspannung	Automatische Erkennung 100-240 VAC, 50-60 Hz	Automatische Erkennung 100-240 VAC, 50-60Hz	Automatische Erkennung 100-240 VAC, 50-60Hz
Leistung	60W	1800 W	1800 W
Strom	5A	7,5A-18A	7,5A-18A
Abmessungen	1,74 Zoll (44,19 mm) H 9,09 Zoll (230,88 mm) B 7,74 Zoll (196,59 mm) T	1,7 Zoll (43,18 mm) H 17,2 Zoll (436,88 mm) B 31 Zoll (787,40 mm) T	3,5 Zoll (88,90 mm) H 17,2 Zoll (436,88 mm) B 31 Zoll (787,40 mm) T
Gewicht	2,3 kg (5,18 lbs)	21,8 kg (48 lbs)	24,5 kg (54 lbs)
Umgebung	*Betriebstemperature:* 32° bis 104° F (0° bis 40° C) *Temperatur außer Betrieb:* -4° bis 158° F (-20° bis 70° C)	*Betriebstemperature:* 50° bis 95° F (10° bis 35° C) *Temperatur außer Betrieb:* -40° bis 158° F (-40° bis 70° C)	*Betriebstemperature:* 50° bis 95° F (10° bis 35° C) *Temperatur außer Betrieb:* -40° bis 158° F (-40° bis 70° C)
Rückseite			

VECTRA™
Security that thinks.™