VECTRA™
Security that thinks™

Whitepaper

Neu definierte Netzwerksicherheit

Die mitdenkende IT Sicherheitslösung von Vectra ermittelt und erkennt Angriffe in Echtzeit

Zusammenfassende Übersicht

So gut wie alle Organisationen haben infizierte Hosts innerhalb ihrer Netzwerke. Am Netzwerkperimeter bereitgestellte, präventionszentrierte Sicherheitslösungen bieten eine nur unvollständige Lösung, um einen Angriff aufzuhalten. Haben sich Angreifer erst einmal Zugriff zum Netzwerk verschafft, können sie ihre Ausbeutung dort ganz ungehindert außerhalb des Überwachungsbereichs der Perimeterlösung durchführen.

Die Implementierung von automatisierten Funktionalitäten zur Angriffserkennung und -berichterstattung in Echtzeit, die vielfältige Möglichkeiten bieten, einen Angriff aufzuhalten, hat bei Sicherheitsexperten heute oberste Priorität. Sicherheitstechnologien müssen in der Lage sein, Daten ununterbrochen zu beobachten, zu verarbeiten, aufzurufen und automatisch zu analysieren, um so den nächsten Schritt des Angreifers antizipieren zu können.

Die Vectra X-Serien-Plattform bietet als erstes System ein neues Niveau der Intelligenz und Automatisierung und kann einen Cyberangriff während der Durchführung erkennen und die Handlungen des Angreifers verfolgen. Die zum Patent angemeldete Technologie der Vectra Plattform prägt sich die typischen Muster des Netzwerkverkehrs sowie unterschiedliche beobachtete Verhaltensweisen ein und erkennt so über Stunden, Tage und Wochen beobachtetes anomales Verhalten.

Die Vectra-Plattform priorisiert automatisch Angriffe, die das größte Risiko darstellen, und ermöglicht es Unternehmen somit, ihre Zeit und Ressourcen schnell und gezielt einzusetzen.

Lesen Sie dieses Whitepaper, um zu erfahren, wie Vectra IT- und Sicherheitsanalysten dazu befähigt, Angriffe sogar während ihrer Ausführung zu stoppen.

„Die Bedrohung durch komplexe, zielgerichtete Angriffe, auch bekannt als ‚Advanced Persistent Threats' (fortgeschrittene, andauernde Bedrohungen) kurz APTs, hat eine Welle der Innovation in der Cybersicherheitsbranche ausgelöst."

—Gartner[4]

Cyberangriffe stellen für Unternehmen jeder Größe und in jeder Branche inzwischen einen Teil des Alltags dar. In den Nachrichten liest man fast jeden Tag über einen weiteren, schweren Fall des Datendiebstahls, bei dem Kreditkartennummern oder andere persönliche Informationen gestohlen wurden, oder eine Reportage über die Schattenwelt der Cyberkriminellen. Sie verwenden hoch entwickelte Geschäftsmodelle, wobei Spezialisten für die Verbreitung von Infektionen und den Einsatz von Botnets verantwortlich sind und das „Verkaufspersonal" die gestohlenen Daten verkauft.

Haben Angreifer erst einmal die Kontrolle über die Hosts des Unternehmens übernommen, verkaufen sie faktisch betrachtet eine Cloud-Service-Plattform an den Meistbietenden, und zwar auf Kosten dieses Unternehmens.

Ein Bericht des Weltwirtschaftsforums und von McKinsey & Company[1] merkt an, dass „Bedenken über Cyberangriffe inzwischen messbare negative Auswirkungen auf einige Unternehmensbereiche haben".

Dort haben Nachforschungen ergeben, dass 80 Prozent der Unternehmen angaben, sich nicht dazu imstande zu fühlen, gegen die rapide weiterentwickelnden Fähigkeiten von Angreifern vorzugehen, und dass eskalierende Sicherheitsbedenken den Fortschritt von Cloud-Computing und den Einsatz von mobilen Geräten beeinträchtigen könnten.

Der Schaden am Ruf und Namen eines Unternehmens oder der Verlust des intellektuellen Eigentums oder der Geschäftsgeheimnisse einer Organisation kann verheerende Auswirkungen haben. Jedoch ist der Diebstahl von Kreditkarteninformationen oder geistigem Eigentum verglichen mit Cyberspionage und Cyberkriegsführung praktisch ein Bagatelldelikt.

Prävention allein ist nicht genug

Die wirksame Prävention von komplexen Angriffen und Malware im Netzwerk hat in den letzten drei Jahren dramatisch abgenommen. Bisher war die bewährteste Strategie eine mehrschichtige Verteidigung mit präventionsorientierten Produkten wie Firewalls, Intrusion-Prevention-Systemen (IPS), Web-Sicherheitsproxys, Nutzlast-Analyse-Tools und Antivirensoftware.

„Im Jahr 2020 ist Prävention zwecklos. Komplexe, zielgerichtete Angriffe machen präventionsorientierte Strategien überflüssig", erklärte Gartner im Jahr 2013.[2]

Die Ereignisse, die sich seit der Veröffentlichung dieses Berichts abgespielt haben, haben das Problem nur verschärft.

„Unternehmen sind zu sehr auf blockierende und präventionsorientierte Mechanismen angewiesen, die immer weniger vor komplexen Angriffen schützen", schreibt Gartner in einem Bericht aus dem Jahr 2014.[3]

1 „Risk and Responsibility in a Hyperconnected World," Weltwirtschaftsforum in Zusammenarbeit mit McKinsey & Company, Januar 2014, http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

2 „Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence," von Neil MacDonald, Gartner, 30 Mai 2013, ID G00252476, http://www.gartner.com/document/2500416

3 „Designing an Adaptive Security Architecture for Protection From Advanced Attacks," von Neil MacDonald and Peter Firstbrook, 12 Februar 2014, ID G00259490, https://www.gartner.com/doc/2665515/designing-adaptive-security-architecture-protection

4 „Five Styles of Advanced Threat Defense," von Lawrence Orans and Jeremy D'Hoinne, Gartner, 20 August 2013, ID G00253559

Haben sich Angreifer erst einmal Zugang zum Netzwerk verschafft, können sie ihre Ausbeutung dort ganz ungehindert außerhalb des Überwachungsbereiches der Perimeterlösungen durchführen.

Vier Gründe, weshalb Sie Ihr Sicherheitsdenken umstellen sollten

„Umfassender Schutz erfordert einen adaptiven Schutzprozess, bei dem vorausschauende und präventive Fähigkeiten sowie Erkennungs- und Reaktionsfähgkeiten integriert werden.“ Gartner empfiehlt Architekten in der Informationssicherheitsbranche, „ein Umdenken ihrer Denkweise von ‚Incident Response‘ auf ‚Continuous Response‘, bei der davon ausgegangen wird, dass Systeme ständig kompromittiert werden und kontinuierliche Überwachung und Sanierung erfordern.“

1. **Organisationen sind zunehmend miteinander verbunden und weiten ihren Netzwerkperimeter zunehmend aus.** Dieser erhält dadurch Schwachstellen, die anfällig für Angriffe sind. Der explosionsartige Anstieg von mobilen Mitarbeitern und die Umstellung auf Cloud-Dienste hat zur Folge, dass Firmenanwendungen und -daten sich weit über das hochsichere Rechenzentrum eines Unternehmens hinaus erstrecken. Die Laptops und mobilen Geräte von Mitarbeitern können in einem Café infiziert werden und diese Infektion wird geradewegs durch die Vordertür in das Unternehmen eingeschleust. Die zusätzliche Implementierung von „Bring your own device (BYOD)“ erschwert es Unternehmen noch weiter, effektive Richtlinien bezüglich der erforderlichen Sicherheitssoftware, die auf Geräten installiert sein sollte, festzulegen und zu implementieren.

   Die Infektionen auf diesen Geräten können sich ausbreiten, wenn sie eine Verbindung zum Unternehmensnetzwerk herstellen und dadurch letzten Endes andere Anwendungen, Datenbanken und Benutzer den Bedrohungen aussetzen, die dadurch Ziele eines Angriffs werden können.

2. **Komplexe Bedrohungen übersteigen die Fähigkeiten aktueller Sicherheitskontrollen und Versuche, weitere Steuerelemente hinzuzufügen, schlagen fehl.** Organisationen müssen sich sowohl gegen opportunistische Bedrohungen wie Massenangriffe als auch gegen weniger verbrei-tete, gezielte Angriffe verteidigen.

   Besonders besorgniserregend sind hierbei Bedrohungen, die schleichend und beharrlich und oftmals in Phasen, über Tage, Wochen oder sogar Monate erfolgen. Angreifer führen die erste Kompromittierung aus der Ferne aus und weiten den Angriff dann lateral und in verändernder Form aus, um ihr Endziel zu erreichen.

3. **Jedes präventionszentrierte Produkt bietet nur eine unvollständige Lösung, um eine Bedrohung zu erkennen, bevor diese den Perimeter passieren und in das Netzwerk eindringen kann.** Eine Firewall oder IPS überwacht einzelne Kommunikations-Sessions zwischen Geräten und versucht, einen Angriff auf der Grundlage von früheren beobachteten ähnlichen Angriffen oder anhand des Reputationswerts eines Fremdsystems zu erkennen. Aber Malware und die Orte, mit denen es kommuniziert, mutieren schnell, um derartige Schutzmaßnahmen zu umgehen. Immer mehr Angreifer verwenden Verschlüsselung und andere Mittel der Verschleierung, die es für präventive Sicherheitsprodukte oft unmöglich machen, eine „Signatur“ zu erstellen, die das Angriffsmuster beschreibt – und für Zero-Day-Attacks sind keine Muster verfügbar. Hat sich ein Angreifer erst einmal Zugang zum Netzwerk verschafft, kann er seine Ausbeutung dort ganz ungehindert, außerhalb des Überwachungsbereiches der Perimeterverteidigung durchführen.

Vectra bietet vielfältige Möglichkeiten, einen Angriff aufzuhalten, und ist daher die perfekte Ergänzung für existierende präventionszentrierte Sicherheitslösungen.

4. **Beim Einsatz einer präventionsbasierenden Sicherheitsstrategie sind die IT-Ressourcen schnell erschöpft.** Den meisten IT-Abteilungen stehen nur begrenzte Mittel zur Deckung des wachsenden Sicherheitsbedarfs des Unternehmens zur Verfügung. Ein erfahrener Sicherheitsanalytiker oder -berater benötigt möglicherweise Wochen, um eine Firewall oder ein IPS richtig zu optimieren, so dass es operativ wirksam ist. Das Isolieren einer neu entdeckten, möglichen Bedrohung kann einen ganzen, langen Tag in Anspruch nehmen, wobei unzählige Warnungen durchsucht werden müssen.

   Netzwerksicherheit ist seit jeher eine komplexe Angelegenheit, gestaltet sich heutzutage jedoch so kompliziert, dass Unternehmen, die auf die Analyse großer Datenmengen spezialisiert sind, in die Sicherheitsbranche einsteigen. Zudem gibt es einfach nicht genügend hochqualifizierte Sicherheitsexperten, um die Nachfrage decken zu können.

Es ist ein neuer Ansatz erforderlich. Vectra bringt Netzwerksicherheit auf die nächsthöhere Stufe, um es Unternehmen zu ermöglichen, Mobilität und Cloud-Dienste umfassend in ihre Arbeit miteinzubeziehen und sich unbesorgt mit Partnern und Kunden verbinden zu können, ohne dass Sicherheitsbedenken ihrem Geschäft im Wege stehen.

Sicherheit, die überwacht, mitdenkt, wiedererkennt und antizipiert

Vectra ist eine mitdenkende IT sicherheitslösung – ein Gehirn innerhalb Ihres Netzwerks. Vectra überwacht, erlernt und merkt sich Verhaltensweisen kontinuierlich und erkennt und antizipiert den nächsten Schritt eines Angriffs in Echtzeit. Durch eine Kombination aus Strategien der Sicherheitsforschung, Data Science und maschinellen Lernverfahren bietet Vectra einen Echtzeit-Einblick in APT-Angriffe. Dieser Einblick ist voll automatisiert und liefert klare, intuitive Berichte, damit Organisationen entscheidende Sofortmaßnahmen ergreifen können, um einen Angriff zu stoppen oder seine Auswirkungen einzudämmen.

Echtzeit-Einblicke in APT-Angriffe. Durch maschinelles Lernen und Data Science kann Vectra APT-Angriffe während mehrerer Phasen und über den gesamten Angriffslebenszyklus hinweg erkennen (siehe Abbildung 1). Vectra bietet vielfältige Möglichkeiten, um einen Angriff aufzuhalten und ist daher die perfekte Ergänzung für existierende, präventionszentrierte Sicherheitslösungen. Die Unterbrechung eines aktiven Angriffs zu jedem beliebigen Zeitpunkt kann mögliche Verluste verhindern oder deutlich vermindern.

Wird ein Gerät durch einen opportunistischen oder einen gezielten Angriff kompromittiert, kann der Angreifer sofort einen Ausgangs-

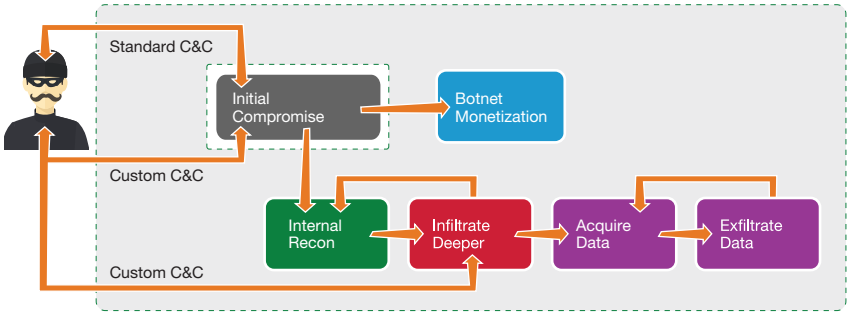

Abbildung 1: Vectra verleiht Sicherheitsanalytikern einen entscheidenden Vorteil gegenüber Cyberangriffen. Präventionszentrierte Sicherheitslösungen bieten nur unvollständige Möglichkeiten, um eine anfängliche Kompromittierung zu entdecken. Vectra bietet Einblick in jede Phase des laufenden Angriffs - vom benutzerdefinierten Command-and-Control hin zum Datendiebstahl.

Vectra erlernt die typischen Muster und Verhaltensweisen des Netzwerkverkehrs und erkennt über Stunden, Tage und Wochen anomales Verhalten.

und Rückzugspunkt im Netzwerk herstellen. Das kompromittierte Gerät kann dann durch interne Reconnaissance seine Lage ermitteln und feststellen, was es ausbeuten könnte. Der Angriff breitet sich möglicherweise lateral aus, auf der Suche nach internen Servern mit wertvollen Daten oder Web-Servern, um Schwachstellen in Anwendungen ausfindig zu machen.

Werden Geräte ausgebeutet, erkennt Vectra die Anzeichen von automatisierte Formen der Monetarisierung – das Versenden von Spam, Werbeanzeigen-Klickbetrug, Bitcoin-Mining oder einen ausgehenden Denial-of-Service-Angriff – Verhaltensweisen, die ein Gerät einer Organisation verwendet, um andere Geräte oder Internet-Dienste anzugreifen.

Wenn Angreifer erfolgreich wertvolle Daten erlangen, müssen sie diese aus der Organisation herausschleusen. Datendiebstahl erfolgt in der Regel durch eine Reihe von gutartigen Vermittlern, bevor das endgültige Ziel erreicht wird. Die Daten können z. B. an einen zuvor kompromittierten Server eines Hosting-Providers gesendet und dann später vom Angreifer abgerufen werden. Vectra achtet gezielt auf einen solchen Datendiebstahl anstatt sich darauf zu konzentrieren, wohin die Daten gesendet werden, wenn sie das Netzwerk des Unternehmens verlassen.

Vectra beobachtet, erlernt und merkt sich Verhaltensweisen mit der Zeit. Vectra überwacht ständig anstatt nur gelegentlich Scans durchzuführen und weiß daher,

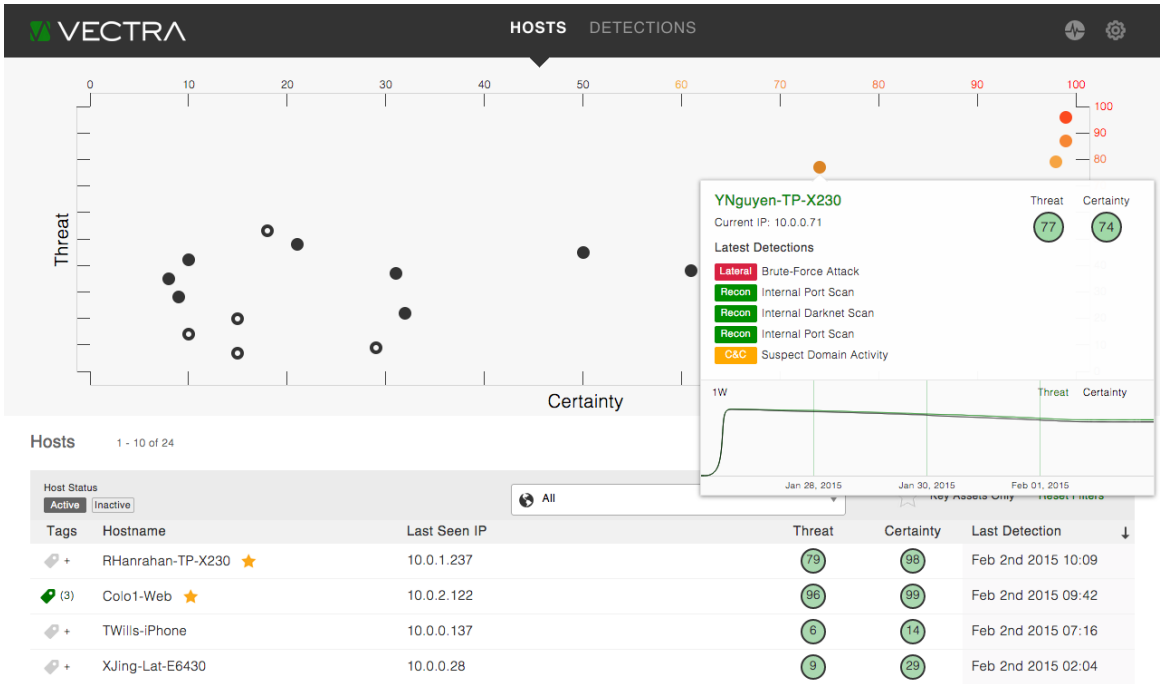

Abbildung 2: Der Vectra Threat Certainty Index priorisiert die Hosts mit den höchsten Sicherheitsrisiken und zeigt kontextuelle Informationen über die Bedrohung an.

Die mitdenkende IT Sicherheitslösung von Vectra erledigt die harte Arbeit, indem sie im Kommunikationsstrom im Netzwerk einen Angriff erkennen und den nächsten Schritt in Echtzeit antizipieren kann, um diesen aufzuhalten.

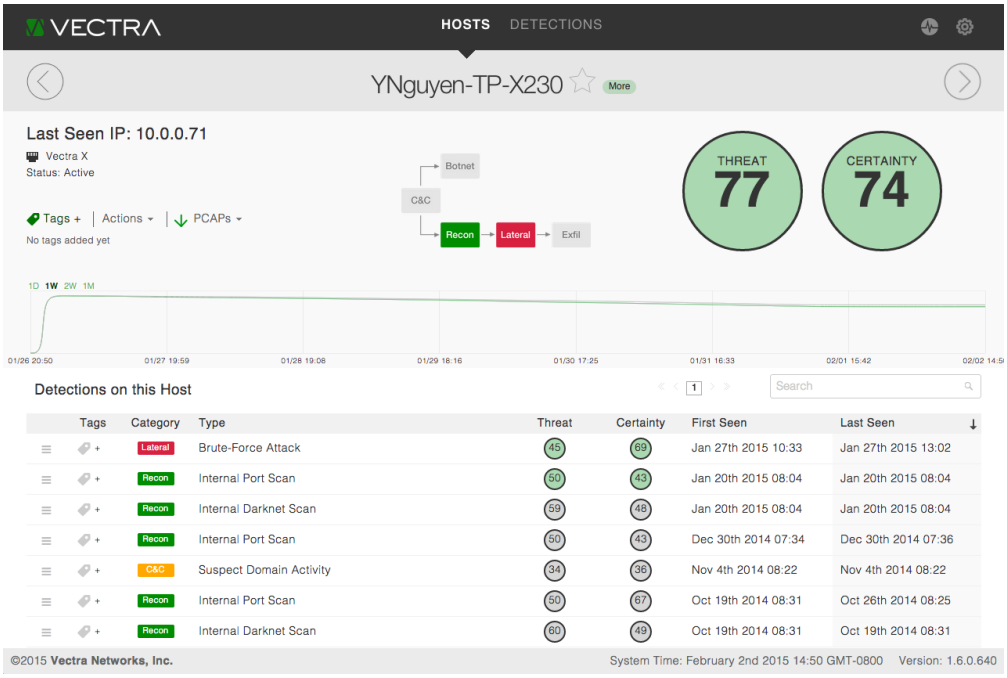

Abbildung 3: Administratoren können Details im Drilldown-Verfahren ganz genau analysieren, z. B. auf einem bestimmten Gerät erkannte Bedrohungen.

wann ein Angriff beginnt, sich ändert oder sich zurückzieht. Und weil es innerhalb der Netzwerkperimeter bereitgestellt wird, kann Vectra den Fluss des Benutzerdatenverkehrs vom und zum Internet sowie von und zum Rechenzentrum überwachen, um anomales Verhalten zu identifizieren. Vectra identifiziert Angriffe auf allen Betriebssystemen, Anwendungen, Geräten und Browsern. Vectra erlernt die typischen Muster und Verhaltensweisen im Netzwerkverkehr und erkennt über Stunden, Tage und Wochen beobachteten anomales Verhalten. Ein Laptop, der E-Mails verschickt, ist nicht auffällig, aber wenn das E-Mail-Aufkommen plötzlich stark ansteigt oder der Laptop das Innere des Netzwerks ausspioniert, kann dies auf ein größeres Problem hinweisen.

Priorisierte Bedrohungserkennung. Der innovative Vectra Threat Certainty Index™ zeigt größere Bedrohungen in Echtzeit automatisch an, basierend auf einem kontextuellen Scoring-Prozess (siehe Abbildung 2). Vectra überwacht, erlernt und merkt sich Verhaltensweisen und erkennt dabei bestimmte Verhaltensprozesse, die sich im Laufe der Zeit wiederholen. Vectra destilliert davon die wichtigsten Verhaltensweisen und analysiert diese über Tage, Wochen oder sogar Monate hinweg.

Vectra verfügt über einen längerfristigen Speicher als andere Echtzeit-Produktlösungen der neuesten Generation und kann daher einen Angriff in Kontext setzen und das Risiko für das Unternehmen besser einschätzen. Administratoren müssen keine Gigabytes an Log-Dateien durchforsten oder Analysetools für große Datenmengen benutzen, um festzustellen, ob eine Bedrohung real ist.

Intuitives, adaptives Reporting. Dank des Vectra Threat Certainty Index, der die größten Bedrohungen in Echtzeit anzeigt, können Sicherheitsmanager ihre Maßnahmen zur

Verringerung und Behebung einer Bedrohung priorisieren. Die IT-Abteilung kann dadurch ganz einfach Prioritäten setzen und zum Beispiel zunächst einen Laptop, der von einem Angreifer für Datendiebstahl verwendet wird, außer Betrieb setzen, bevor die Reinigung eines infizierten Rechners, der für Werbeanzeigen-Klickbetrug verwendet wird, durchgeführt wird.

Vectra bietet kompromisslose, visuelle Klarheit. Sicherheitsadministratoren können die Details einer Bedrohung im Drilldown-Verfahren ganz genau analysieren, einschließlich der Paket-Erfassungen, die die Identifikation des Verhaltens ermöglichen (siehe Abbildung 3). Die Berichterstattung von Vectra kann das sukzessive Fortschreiten einer Bedrohung dokumentieren.

Vectra bietet operative Effizienz. Vectra erledigt alle komplexen, sicherheitsbezogenen Arbeiten und entlastet durch seine Sicherheitsüberwachung in Echtzeit die Netzwerkverwaltung. Administratoren müssen keine detaillierte, zeitaufwendige Konfiguration durchführen oder Wochen mit dem Tuning der Plattform verbringen. Wenn die Vectra-Plattform an das Netzwerk angeschlossen ist, erlernt sie automatisch alles, das sie wissen muss, und erstellt Modelle normaler Verhaltensweisen der mit dem Netzwerk verbundenen Geräte. Vectra wird automatisch über einen Cloud-Service aktualisiert, damit der Schutz stets auf dem neuesten Stand ist.

Ein Sicherheitssystem, das mitdenkt.

Die Zeit ist reif für ein intelligentes Sicherheitssystem. Angreifer befinden sich bereits in Ihrem Netzwerk auf der Suche nach einer Möglichkeit, qualitativ hochwertige Daten zu stehlen oder ihre Angriffsziele auszuweiten. Die mitdenkende IT Sicherheitslösung von Vectra erledigt die harte Arbeit, indem sie im Kommunikationsstrom im einen Angriff erkennen und den nächsten Schritt in Echtzeit antizipieren kann, um den Angriff aufzuhalten.

Sehen Sie sich an, wie Vectra funktioniert, unter
www.vectranetworks.com/resources/#demo