CrowdStrike – Produkte

CROWDSTRIKE

ENDGERÄTESCHUTZ – EIN LEITFADEN FÜR DIE BESCHAFFUNG

So finden Sie die beste Lösung für den Schutz Ihrer Endgeräte

KURZDARSTELLUNG

Die Endgerätesicherheit ist eine der wichtigsten Komponenten einer Cybersicherheitsstrategie. Aus dem SANS Endpoint Security Survey Report 2018 geht hervor, dass mehr als 80 Prozent der bekannten Sicherheitsverletzungen ein Endgerät betrafen. Wer heute für den Schutz der Endgeräte eines Unternehmens verantwortlich ist, hat es nicht leicht, die beste Lösung für diese Aufgabe zu finden. Angesichts von Hunderten von Optionen auf dem Markt und Leistungsmerkmalen, die nahezu identisch klingen, ist die Wahl der richtigen Lösung für den Endgeräteschutz komplex.

Nach Auffassung von CrowdStrike® sollte eine umfassende und effiziente Lösung für den Endgeräteschutz fünf zentrale Elemente umfassen. Folgende Kriterien können hierbei als Richtlinie für die Bewertung und Auswahl einer Lösung dienen.

- **Prävention** zur Abwehr von so vielen bösartigen Elementen wie möglich
- **Erkennung** zum Auffinden und Ausschließen von Angreifern
- **Verwaltete Bedrohungssuche** zur Verbesserung der Erkennung über die Automatisierung hinaus
- **Integrierte Bedrohungsaufklärung** zum besseren Verständnis der Lage und zur Wahrung eines Vorsprungs gegenüber potenziellen Angreifern
- **IT-Hygiene und Schwachstellenbewertung** zur Vorbereitung und Stärkung der Umgebung gegen Bedrohungen und Angriffe

CrowdStrike empfiehlt, diese fünf Leistungsmerkmale über eine Cloud-basierte Architektur bereitzustellen. Nur so lassen sich die Geschwindigkeit, Flexibilität und Leistung erreichen, die zur Abwehr versierter Angreifer erforderlich sind. Darüber hinaus sollten diese Leistungsmerkmale in einem einzigen schlanken Agenten kombiniert werden, der die Endgeräte nicht unnötig belastet.

Mit Falcon® stellt CrowdStrike eine Plattform für den Endgeräteschutz der nächsten Generation bereit, die alle genannten Elemente in einem einzigen Cloud-basierten Agenten vereint. Falcon vereint die Technologien, die erforderlich sind, um Sicherheitsverletzungen erfolgreich zu unterbinden. Dies umfasst Virenschutz der nächsten Generation (NGAV), Endgeräteerkennung und Reaktion (EDR), IT-Hygiene, Schwachstellenbewertung, verwaltete Bedrohungssuche (Managed Threat Hunting) rund um die Uhr sowie Bedrohungsaufklärung (Threat Intelligence). Alle Leistungsmerkmale zur kontinuierlichen Vorbeugung von Sicherheitsverletzungen sind in einem einzigen Agenten vereint, der innerhalb weniger Stunden bereitgestellt werden kann, ohne die Leistung der Endgeräte oder das Benutzererlebnis zu beeinträchtigen. Die Falcon-Plattform stoppt kontinuierlich Sicherheitsverletzungen. Sie ist damit eine ebenso kompromisslose wie bewährte Lösung der nächsten Generation zum Schutz von Endgeräten.

Angesichts von Hunderten von Optionen auf dem Markt und Leistungsmerkmalen, die nahezu identisch klingen, ist die Wahl der richtigen Lösung für den Endgeräteschutz sehr komplex.

EINLEITUNG

Der Schutz von Endgeräten ist seit jeher ein wichtiger Bestandteil aller Sicherheitsstrategien, da Endgeräte ein bevorzugtes Angriffsziel sind. Mittlerweile schützen fast alle Unternehmen ihre Endgeräte auf die eine oder andere Art. Da Angreifer aber heute selbstverständlich davon ausgehen, dass Endgeräte geschützt sind, entwickeln sie immer anspruchsvollere Verfahren und Möglichkeiten, diesen Schutz zu umgehen. Dieser Sachverhalt führt zu Tausenden von erfolgreichen Sicherheitsverletzungen, die die Grenzen der herkömmlichen Endgerätesicherheit deutlich machen. Der Bedarf nach einem besseren Endgeräteschutz hat dazu geführt, dass 76 Prozent der Unternehmen planen, ihren AV-Anbieter innerhalb der nächsten 12 bis 14 Monate* zu wechseln. Als Grund Nr. 1 für den Wechsel gilt die mangelnde Wirksamkeit in der Abwehr moderner Bedrohungen**.

Der Bedarf an einem besseren Endgeräteschutz ließ zudem eine Vielzahl neuer Produkte entstehen, die alle für sich in Anspruch nehmen, bahnbrechende Neuerungen einzuführen. Die Vielzahl dieser Produkte kann die Suche nach der richtigen Lösung zu einem fast hoffnungslosen Unterfangen machen.

Dieser Leitfaden soll Sicherheitsexperten unterstützen, indem er die wirklich entscheidenden Elemente für einen wirksamen Schutz vor modernen Bedrohungen definiert.

ENTSCHEIDENDE ELEMENTE: WORAUF SIE BEIM ENDGERÄTESCHUTZ ACHTEN SOLLTEN

Eine leistungsfähige Lösung zum Schutz von Endgeräten ist mehr als eine Sammlung von Features, die unter einem Dachprodukt vereint sind. Ein wirksamer Schutz ist nur dann gegeben, wenn Sicherheitsverletzungen konzeptionell über das gesamte Angriffskontinuum hinweg gestoppt werden, anstatt ständig einzelne Schutzfunktionen zu kumulieren, die bei Entdeckung einer neuen Angriffstechnik jeweils hinzugefügt werden.

Die ideale Endgerätelösung sollte ein komplettes Paket bieten, das nicht nur auf moderne Schutztechnologien setzt, sondern auch alle verfügbaren Mittel innovativ dazu nutzt, versierte Angreifer auf Augenhöhe abzuwehren. Damit Verteidiger Angreifer ausbremsen können, sollte dieses Paket sowohl eine integrierte Bedrohungsaufklärung als auch eine von Spezialisten unterstützte Bedrohungserkennung und Reaktion umfassen, sowie eine Cloud-basierte Architektur, die den Angreifern stets einen Schritt voraus ist. Nur dann kann die Endgerätelösung die Art von Funktionen für Antizipation, Prävention, Erkennung, Sichtbarkeit und Reaktion bereitstellen, die einen bestimmten Angreifer stets aufs Neue schlagen können.

Entscheidungsträger sollten insbesondere auf fünf entscheidende Elemente achten: Virenschutz der neuesten Generation (NGAV), Endgeräteerkennung und Reaktion (EDR), verwaltete Erkennung und Reaktion (MDR), Bedrohungsaufklärung sowie IT-Hygiene und Schwachstellenbewertung. Die Kombination dieser Elemente gewährleistet eine umfassende, robuste und wirksame Lösung zum Schutz von Endgeräten.

Dieser Leitfaden soll Sicherheitsexperten unterstützen, indem er die wirklich entscheidenden Elemente für einen wirksamen Schutz vor modernen Bedrohungen definiert.

*Enterprise Strategy Group: Umfrage zur Endgerätesicherheit
** Die von den Marktforschungsunternehmen Gartner und Forrester befragten Kunden nannten dies ihr wichtigstes Anliegen

DIE 5 ENTSCHEIDENDEN ELEMENTE DES ENDGERÄTESCHUTZES

PRÄVENTION	ERKENNUNG	VERWALTETE BEDROHUNGSSUCHE	ANTIZIPATION	EINSATZBEREITSCHAFT
NGAV (Antivirus der nächsten Generation)	EDR (Endgeräteerkennung und Reaktion)	MDR (Verwaltete Erkennung und Reaktion)	Bedrohungsaufklärung	IT-Hygiene und Schwachstellenbewertung

ENTSCHEIDENDES ELEMENT EINS: PRÄVENTION

SCHUTZ VOR MALWARE UND MEHR

Warum Sie einen Virenschutz der neuesten Generation benötigen

Es gibt gute Gründe, warum herkömmliche, malware-zentrierte Produkte nicht ausreichend gegen die heutigen Bedrohungen und Angreifer schützen.

Erstens erreichen malware-zentrierte Lösungen nur eine Effektivitätsrate von 99 Prozent und lassen folglich eine kleine aber möglicherweise entscheidende Lücke. Diese Lücke eröffnet Angreifern ein ideales Einstiegsfenster für die Beschaffung oder Erstellung von Zero-Day-Malware. Zweitens bleibt der malware-zentrierte Schutz unwirksam gegenüber den immer ausgefeilteren datei- und malwarefreien Taktiken der heutigen versierten Angreifer. Studien zeigen sogar, dass 50 bis 60 Prozent der heutigen Sicherheitsverletzungen überhaupt nicht durch Malware verursacht werden, sondern durch Techniken wie Social Engineering oder Identitätsdiebstahl aus anderen Quellen.

Eine solide Endgeräteschutzlösung muss diese Herausforderungen bewältigen, indem sie über die einfache Identifizierung und Bekämpfung bekannter Malware hinausgeht. Sie sollte vor bekannter und unbekannter Malware schützen, indem sie Technologien wie Machine Learning (ML) einsetzt, deren Wirksamkeit nicht von täglichen Updates abhängt. Weiterhin sollte sie eine umfassende Verhaltensanalyse nutzen, um automatisch nach Anzeichen von Angriffen zu suchen und diese noch während des laufenden Angriffs zu stoppen. Darüber hinaus sollte die ideale Lösung Endgeräte vor allen Arten von Bedrohungen schützen, also vor bekannter und unbekannter Malware bis hin zu datei- und malwarefreien Angriffen, indem sie alle notwendigen Technologien für einen optimalen Schutz kombiniert.

Die folgende Tabelle zeigt die wichtigsten Anwendungsfälle und entscheidenden Leistungsmerkmale, die die NGAV-Komponente einer wirksamen Lösung zum Schutz von Endgeräten zur Verfügung stellen sollte.

Es gibt gute Gründe, warum herkömmliche, malware-zentrierte Produkte nicht ausreichend gegen die heutigen Bedrohungen und Angreifer schützen.

NGAV: ANWENDUNGSFÄLLE UND WESENTLICHE LEISTUNGSMERKMALE

Prävention gegen bekannte und Zero-Day-Malware	**Erforderliche Merkmale** ■ Machine Learning am Endgerät zur Prävention bekannter und unbekannter Malware ■ Automatisierte Malware-Analyse (z. B. Sandboxing) ■ Integrierte Bedrohungsaufklärung ■ Benutzerdefinierte Whitelisting- und Blacklisting-Funktionen ■ Automatische Einbindung von Gefährdungsindikatoren (IOC) Dritter
	Evaluierungskriterien ● Unabhängige Testergebnisse von Dritten ● Rate der falsch Positiven
	Relevante Fragen ● Ist das Produkt signaturbasiert oder nutzt es Machine Learning? ● Wenn das Produkt Machine Learning nutzt, muss das Endgerät dann zwingend mit der Cloud verbunden sein? ● Welches der Präventionsmerkmale erfordert eine Verbindung zur Cloud? ● Falls Malware nicht blockiert wird, welche anderen Präventionsmechanismen bietet das Produkt?
Schutz vor Ransomware	**Erforderliche Merkmale** ■ Machine Learning am Agenten ■ Verhaltensanalyse/Angriffsindikatoren (IOAs) speziell für Ransomware ■ Integrierte Bedrohungsaufklärung
	Evaluierungskriterien ● Wirksamkeit gegen aktuelle Ransomware wie WannaCry und NotPetya ● Testergebnisse von Dritten
	Relevante Fragen ● Welche Methoden werden zur Prävention von Ransomware eingesetzt? ● Welche Methoden werden zur Prävention von Zero-Day-Ransomware eingesetzt? ● Wie hat sich das Produkt bisher bei Ransomware-Angriffen wie WannaCry oder NotPetya bewährt?
Prävention gegen Angriffe ohne Malware oder Dateien: Schutz der Endgeräte gegen alle Arten von Bedrohungen, nicht nur gegen Malware und Exploits	**Erforderliche Merkmale** ■ Schutz vor bekannten Exploits ■ Schutz vor Zero-Day-Exploits ■ Schutz des Arbeitsspeichers ■ Verhaltensbasierte Blockierung anhand von Angriffsindikatoren
	Evaluierungskriterien ● Erfolgreich bestandener Test von Angriffssimulationen gemäß MITRE ● Wirksamkeit bei Übungsläufen gegen das „rote Team“
	Relevante Fragen ● Welche Arten von bösartigen Aktivitäten ohne Malware werden blockiert? ● Werden Angreifer blockiert, die sich für ihre Aktionen mit gestohlenen Zugangsdaten angemeldet haben und legitime Tools nutzen? ● Welche Bereiche des MITRE-ATT&CK-Frameworks werden geschützt? ● Kann die Lösung eine böswillige Nutzung legitimer Anwendungen wie PowerShell verhindern? Wie? ● Wie blockiert die Lösung Exploits? ● Ist das Produkt in der Lage, Zero-Day-Exploits zu blockieren? ● Falls ein Angriff nicht blockiert wird, welche anderen Präventionsmechanismen setzt das Produkt ein? ● Welche Art von Arbeitsspeicher-Schutzmechanismen bietet das Produkt an?

Jederzeit maximaler Schutz: Schützt stets auf maximalem Niveau	**Erforderliche Merkmale** ■ Keine täglichen Updates für Schutz auf höchstem Niveau erforderlich ■ Schutz funktioniert auch offline, wenn keine Verbindung zur Cloud besteht ■ Machine Learning am Endgerät funktioniert auch offline ohne Verbindung zur Cloud
	Evaluierungskriterien ● Häufigkeit von Updates (Produkt, Malware-Signaturen oder DAT-Dateien usw.), die vom Hersteller bereitgestellt werden, sowie deren Performance-Auswirkungen. Aus der Häufigkeit lässt sich schließen, wie oft das Produkt aktualisiert werden muss, um wirksam zu bleiben ● Nachweis der Wirksamkeit bei bekannter und unbekannter Malware sowie bösartigen Aktionen auf ein Endgerät, das nicht online ist
	Relevante Fragen ● Wie oft muss das Produkt aktualisiert werden, um das höchste Schutzniveau zu gewährleisten? ● Welche Prävention leistet das Produkt ohne Internet-Verbindung, wenn der Benutzer eine Datei öffnet oder eine ausführbare Datei anklickt oder bösartige Aktionen ausführt?
Schnelle Reaktion und Abhilfe	**Erforderliche Merkmale** ■ Bösartige Dateien können unter Quarantäne gestellt werden ■ Erkennungsinformationen können für Untersuchungszwecke mindestens 90 Tage aufbewahrt werden ■ Dateien unter Quarantäne werden zur automatischen Analyse an die Sandbox übergeben ■ Eine API ermöglicht die Integration mit bestehenden Orchestrierungs-/Case-Management-Systemen des Kunden
	Evaluierungskriterien ● Liste der von der Lösung unterstützten Maßnahmen ● Liste der bestehenden Orchestrierungs- und Ticketing-Systeme für Sicherheitsaufgaben, in die das Produkt integriert werden kann
	Relevante Fragen ● Welche Reaktionsmöglichkeiten bietet das Produkt? ● Wie lässt sich das Produkt in bestehende Sicherheitswerkzeuge integrieren? ● Liefert das Produkt mit seinen Warnmeldungen einen Kontext zur Verbesserung der allgemeinen Abwehr? ● Kann das Produkt aus Warnmeldungen Gefährdungsindikatoren erzeugen, die zur Verbesserung der allgemeinen Abwehr dienen?

DAS KONZEPT VON CROWDSTRIKE

Die CrowdStrike Falcon Endpoint Protection-Plattform bietet eine neue Generation von Präventionsmerkmalen zur wirksamen Abwehr neuer Tools und Techniken, die heutige Angreifer nutzen. Gleichzeitig schließt die Lösung die von älteren Antivirenprodukten hinterlassene Lücke. Die Falcon-Plattform kombiniert eine Reihe leistungsstarker Methoden zur Abwehr von Taktiken, Techniken und Verfahren (TTPs), die die heutigen Angriffe so erfolgreich machen. Diese Kombination von Methoden ermöglicht es Falcon, nicht nur vor existierender Malware zu schützen, sondern auch Zero-Day-Malware, Exploits und insbesondere dateilose und malwarelose Angriffe zu verhindern. Falcon nutzt die jeweils geeignete Präventionsfunktion zum jeweils richtigen Zeitpunkt, sodass Sicherheitsverletzungen über das gesamte Angriffskontinuum verhindert werden.

Falcon nutzt an den Endgeräten Machine Learning und schützt damit vor bekannter und unbekannter Malware noch vor deren Ausführung. Das Machine Learning von Falcon ist so leistungsstark, dass Falcon-Kunden schon sofort nach der Implementierung vor der Ransomware WannaCry und NotPetya geschützt sind, ohne Updates oder Konfigurationsmaßnahmen durchführen zu müssen.

Mit Exploit-Minimierung schützt Falcon vor Angreifern, die Exploits als Komponente ihrer Angriffe mit oder ohne Malware nutzen. Hierbei werden Exploits gestoppt, die sich gezielt bestimmter Schwachstellen bedienen. Das gilt für bekannte Exploits ebenso wie für Zero-Day-Exploits. So wird eine Gefährdung der Hostsysteme verhindert.

Gegen versierte Angreifer, die ihre Taktik nicht auf den Einsatz von Malware und Exploits beschränken, setzt Falcon Angriffsindikatoren ein. Dies sind verhaltensbasierte Algorithmen, die darauf abzielen, die Absicht oder das Ziel der Angreifer zu erkennen, unabhängig von den beim Angriff verwendeten Tools. Auf Angriffsindikatoren basierte Präventionsfunktionen ermöglichen es, Bedrohungen zu verhindern, bei denen herkömmliche Technologien wie Signaturen, Whitelisting oder Sandboxing nicht greifen.

ENTSCHEIDENDES ELEMENT ZWEI: ERKENNUNG

ANGRIFFE SICHTBAR MACHEN UND ANGREIFER FERNHALTEN

Warum EDR unverzichtbar ist

Angreifer erwarten, dass ihre Ziele durch bestimmte Präventionsmaßnahmen geschützt sind. Sie haben daher ihre Methoden verfeinert und entsprechende Präventionstechniken entwickelt. Zu diesen Techniken gehören Identitätsdiebstahl, dateilose Angriffe oder Angriffe auf die Software-Lieferkette. Wenn ein Angreifer in der Lage ist, Fuß zu fassen, ohne dass ein Alarm ausgelöst wird, spricht man von „silent failure", also einem „unbemerkten Versagen" der Schutzmaßnahmen, wodurch Angreifer sich tagelang, wochenlang oder sogar monatelang unbemerkt in einer Umgebung aufhalten können. Die Lösung für „silent failure" ist EDR, also Endgeräteerkennung und Reaktion. Sicherheitsverantwortliche können damit Angriffe schnellstmöglich sichtbar machen.

Ein umfassendes EDR-System sollte alle relevanten Aktivitäten an einem Endgerät aufzeichnen und einer eingehenderen Inspektion unterziehen, sowohl in Echtzeit als auch nach dem Vorfall. Eine effiziente EDR-Lösung sollte zudem intelligent sein und bösartige Aktivitäten automatisch erkennen können, ohne dass die Sicherheitsverantwortlichen Erkennungsregeln schreiben oder abstimmen müssen.
Auch muss das EDR-System eine einfache Möglichkeit bieten, eine aufgedeckte Sicherheitsverletzung abzufedern. Dies könnte bedeuten, dass die exponierten Endgeräte isoliert werden, um die laufende Sicherheitsverletzung zu stoppen und zu beheben, bevor Schaden entsteht.

Die folgenden Anwendungsfälle sollen dabei helfen, die EDR-Funktionalität der in Betracht gezogenen Endgerätelösungen zu bewerten.

EDR: ANWENDUNGSFÄLLE UND WESENTLICHE LEISTUNGSMERKMALE

Automatische Aufdeckung versteckter Angreifer: Sicherheitsverletzungen erkennen	**Erforderliche Merkmale** ■ Automatische Erkennung von Ereignissen — intelligente Endgeräteerkennung und Reaktion mit integrierter Echtzeitfunktionalität ■ Automatische Erkennung basierend auf Verhaltensanalysen wie Angriffsindikatoren ■ Integration in die Bedrohungsaufklärung
	Evaluierungskriterien ● Keine Feinabstimmung, keine Erstellung von Regeln, keine komplexe Konfiguration ● Wirkliche Leistung statt Pen Tests
	Relevante Fragen ● Welche Art von Erkennungs- oder Korrelationsregeln muss geschrieben werden, bevor das Produkt Vorfälle erkennen kann? ● Welches Expertenwissen ist für den Einsatz der Lösung erforderlich?

Ermitteln unbekannter Risiken und Suche nach Bedrohungen: Angriffe erkennen, bei denen die Präventionsmaßnahmen nicht greifen. Verweildauer der Angreifer drastisch verkürzen	**Erforderliche Merkmale** ■ Erfassen von Rohdaten, auch wenn sie keinen Warnmeldungen und Erkennungen zugeordnet sind ■ Bereitstellen der Rohdaten von Ereignissen über einen längeren Zeitraum (Monate bis Jahre) ■ Betrieb im Kernel-Modus, damit die volle Sichtbarkeit gegeben ist und keine blinden Flecken verbleiben ■ Vollständig konfigurierbare Suche in Echtzeit und im historischen Verlauf ■ Gleichzeitige unternehmensweite Suche ohne Beeinträchtigung der Endgeräte ■ Antwort auf Abfragen in max. fünf Sekunden
	Evaluierungskriterien ● Welche Art von Ereignissen kann das Produkt beobachten und sammeln, z. B. Dateisystem, Ausführung von Prozessen/ Threads/DLLs/Diensten, Registrierung, Kernel-Objekt, Aktivitäten im Netzwerk, Benutzeranmeldungen, Memory Injection, USB-Laufwerke, Kommandozeilenbefehle usw. ● Verfügbarkeit einer Aufbewahrungsfrist für alle Rohdaten von Ereignissen
	Relevante Fragen ● Was macht die Lösung sichtbar (z. B. Kernel-Ebene)? ● Welche Telemetriedaten der Endgeräte werden vom Agenten erfasst? ● Wie unterstützt das Produkt die proaktive Bedrohungssuche? ● Wie werden Such- und Abfrageergebnisse erzielt (z. B. Abfragen von Endgeräten, Abfragen einer Cloud-Datenbank)? ● Liefert die Suche Echtzeit-Ergebnisse? ● Wo und wie lange werden die Rohdaten von Ereignissen gespeichert?
Beschleunigung von Untersuchungen und forensischen Analysen	**Erforderliche Merkmale** ■ Intuitive und umfassende Visualisierung von Alarmen mit Anzeige des vollständigen Angriffsverlaufs in einem Prozessbaum; Drill-Down- und Pivot-Funktionen ■ Zuordnung der Angriffsschritte zu einem branchenüblichen Angriffsframework, wie beispielsweise MITRE ATT&CK ■ Bereitstellung der forensischen Daten, auch wenn das Endgerät nicht verfügbar, nicht zugänglich oder zerstört ist ■ Erkennungsergebnisse mit vollständigen Kontexten und Warnmeldungen, einschließlich Bedrohungsaufklärung ■ Flexible Datenvorhaltung für alle Rohereignisdaten mit Möglichkeit zur Verlängerung auf ein ganzes Jahr ■ Abfragesprache gemäß Industriestandard zur Suche nach Ereignisdaten
	Evaluierungskriterien ● Screenshot oder Demo zur Alarmvisualisierung ● Proof of Concept (POC) oder Proof of Value (POV) ● Branchenüblicher Framework zur Angriffsdarstellung
	Relevante Fragen ● Macht die Lösung Angaben dazu, wie ein Angreifer auf die Umgebung zugreift? ● Wie unterstützt die Lösung Sicherheitsanalysten dabei, Warnmeldungen zu visualisieren, logische Verbindungen zwischen Ereignissen herzustellen sowie auf andere Ereignisse und Endgeräte zuzugreifen? ● Anhand welcher Merkmale kann die Lösung bösartiges Verhalten während oder nach dem Auftreten erkennen?
Beschleunigte Problembeseitigung und Reaktion	**Erforderliche Merkmale** ■ Fähigkeit zur Isolation von Endgeräten im Netzwerk ■ Fähigkeit zur Verschiebung von Dateien in die Quarantäne ■ Fähigkeit zur Remote- und Echtzeit-Ausführung von Befehlen auf verdächtigen Endgeräten ■ API zur Integration in die bestehenden Orchestrierungs-/Fallmanagementsysteme des Kunden
	Evaluierungskriterien ● Auflistung der in der Lösung verfügbaren Reaktionsfunktionen
	Relevante Fragen ● Welche Reaktionsmöglichkeiten bietet die Lösung? ● Wie lässt sich die Lösung in bestehende Sicherheits- und Unternehmenswerkzeuge integrieren, beispielsweise in SOAR-Lösungen?

DAS KONZEPT VON CROWDSTRIKE

CrowdStrike Falcon Insight™ EDR überwacht und protokolliert Aktivitäten an den Endgeräten und bietet die notwendige Sichtbarkeit in Echtzeit und im historischen Verlauf, um Manipulationen von Angreifern erkennen zu können. Sicherheitsverantwortliche werden zudem in die Lage versetzt, Vorfälle schnell untersuchen und lösen zu können. Nach diesem Konzept werden Angreifer gestoppt, bevor sie Schaden anrichten können. Gleichzeitig wird das Risiko eines unbemerkten Versagens der Schutzmaßnahmen beseitigt.

Falcon verfügt zudem über automatische und manuelle Analysefunktionen, die während oder nach einem Ereignis ausgeführt werden können. Die automatische Analyse dient dazu, Aktivitäten von Angreifern sofort zu erkennen, sofern es ihnen gelungen ist, sich Zugang zu verschaffen. Die manuelle Analysefunktion sorgt für umfassende Sichtbarkeit und Kontextinformationen. Beides ist wichtig für die proaktive Bedrohungssuche, die schnelle Untersuchung von Vorfällen sowie deren Behebung. Darüber hinaus gewährleistet die Cloud-basierte Architektur von CrowdStrike die Geschwindigkeit und Skalierbarkeit, um bei Bedarf alle notwendigen Endgeräteereignisse monatelang zu sammeln und aufzubewahren, auch wenn die Endgeräte nicht verfügbar sind, zerstört oder gelöscht wurden (wie dies bei virtuellen Workloads der Fall sein kann).

Falcon Insight schafft Sichtbarkeit in Echtzeit und im historischen Verlauf. Die Lösung stellt die notwendigen Mittel zur Datenanalyse bereit, damit Unternehmen ein mögliches unbemerktes Versagen der Schutzmaßnahmen schnell erkennen und mit den geeigneten Tools darauf reagieren können.

ENTSCHEIDENDES ELEMENT DREI: VERWALTETE BEDROHUNGSSUCHE

WENN DIE AUTOMATISIERTE ERKENNUNG NICHT AUSREICHT

Warum die verwaltete Bedrohungssuche so wichtig ist

Es gibt Fälle, bei denen die automatische Erkennung von Angriffen nicht greift. Deutlich wird dies anhand der anhaltenden Sicherheitsverletzungen, die auch in Umgebungen auftreten, in denen neue und weitreichende Sicherheitstechnologien eingesetzt werden. Das liegt daran, dass passive automatisierte Warnmeldungen auf voreingestellten Parametern basieren, die von bestimmten Angreifern getestet und umgangen werden können. Aus diesem Grund ist eine proaktive Bedrohungssuche unter Federführung von Experten ein Muss für jedes Unternehmen, das Bedrohungen in Echtzeit erkennen und darauf reagieren will oder diese Fähigkeit verbessern möchte.

Die Bedrohungssuche spielt eine entscheidende Rolle bei der Früherkennung von Angriffen und Angreifern. Es handelt sich um einen proaktiven Ansatz, bei dem Experten nach verdächtigen Aktivitäten suchen, anstatt sich passiv auf Technologien zu verlassen, die automatisch die Aktivitäten eines potenziellen Angreifers erkennen und Warnmeldungen auslösen. Die frühzeitige Erkennung und Untersuchung solcher Aktivitäten ermöglicht es Unternehmen, Angriffe zu stoppen, bevor sie Schaden anrichten können.

Leider machen fehlende Ressourcen und Kenntnisse eine proaktive Bedrohungssuche für die meisten Unternehmen unerreichbar. Die ohnehin hoch belasteten internen Teams sind nicht in der Lage, rund um die Uhr böswillige Aktivitäten zu überwachen. Oft können sie zudem nicht effizient auf extrem komplexe Angriffe reagieren. Dies kann zu Verzögerungen bei den Ermittlungen führen, wodurch Warnungen nicht immer zeitnah bearbeitet werden. Dies führt letztlich zu längeren Verweilzeiten und dem erhöhten Risiko, dass Angreifer ihre Ziele erfolgreich erreichen.

Die verwaltete Bedrohungssuche löst dieses Problem, indem sie auf ein Expertenteam zurückgreift, das nicht nur bösartige Aktivitäten findet, die von automatisierten Systemen übersehen wurden, sondern diese Aktivitäten auch gründlich analysiert und den Kunden Leitlinien für die richtige Reaktion an die Hand gibt.

Die folgende Tabelle soll dabei helfen, die wesentlichen Leistungsmerkmale zu identifizieren, die eine Lösung für verwaltete Bedrohungssuche bieten muss. Zudem soll sie Hinweise zur Evaluierung und Einordnung der verschiedenen Optionen geben.

> Eine proaktive Bedrohungssuche unter Federführung von Experten ist ein Muss für jedes Unternehmen, das Bedrohungen in Echtzeit erkennen und darauf reagieren will oder diese Fähigkeit verbessern möchte

VERWALTETE BEDROHUNGSSUCHE: ANWENDUNGSFÄLLE UND WESENTLICHE LEISTUNGSMERKMALE

Beseitigung falscher Negative und Verkürzung der Verweildauer von Angreifern: Beseitigung der Lücken in der Bedrohungserkennung und in der Vorfallreaktion	**Erforderliche Merkmale** ■ Erfahrene und engagierte Experten für die Bedrohungssuche im eigenen Haus ■ Suche nach Bedrohungen rund um die Uhr als Service ■ Fähigkeit zum Auffinden von Vorfällen, die bislang kein anderes System erkannt hat ■ Sofortiger Zugriff auf Experten für Bedrohungsaufklärung zur schnelleren Analyse ■ Höchste Effizienz durch automatische und originäre Integration in die Bedrohungsaufklärung
	Evaluierungskriterien ● Anzahl der neuartigen Sicherheitsverletzungen, die pro Jahr erkannt und verhindert werden ● Anzahl der untersuchten Ereignisse pro Jahr ● Art der Plattform, die für die Bedrohungssuche verwendet wird ● Test durch „rotes Team“
	Relevante Fragen ● Werden eigene Services zur verwalteten Bedrohungssuche angeboten oder muss sich der Kunde hierzu auf einen Drittanbieter verlassen? ● Welche Art von Plattform wird für die Bedrohungssuche eingesetzt?
Priorisierung der dringlichsten Warnungen; Gewährleistung, dass kritische Warnungen nicht unter den Tisch fallen	**Erforderliche Merkmale** ■ Fähigkeit zur Benennung der dringlichsten Bedrohungen in der betreffenden Umgebung ■ Erweiterte Kommunikation als geschlossener Regelkreis, damit wichtige Warnmeldungen beachtet werden
	Evaluierungskriterien ● Service Level Agreements (SLAs) ● Dokumentierter Feedback-Prozess als geschlossener Regelkreis
	Relevante Fragen ● Nach welchem Prozess wird das Unternehmen darüber informiert, dass ein Vorfall entdeckt wurde? ● Gibt es einen Eskalationsprozess für Warnungen? Wenn ja, welche Art von Warnungen werden eskaliert und wann?
Anleitung durch den Reaktionsprozess	**Erforderliche Merkmale** ■ Generierung aussagekräftiger Warnmeldungen ■ Unterstützung und Anleitung bei Vorfällen ■ Anleitung zur Ergreifung der nächsten Maßnahmen und Vorschläge zur Minderung der Risiken bei erkannten Bedrohungen
	Evaluierungskriterien ● Musterwarnungen überprüfen ● Siehe Empfehlungsmuster
	Relevante Fragen ● Wie kommunizieren die Experten für Bedrohungssuche mit dem Kunden? ● Welche Informationen liefert das Expertenteam über die von ihm entdeckten bösartigen Aktivitäten?

Erweiterung des aktuellen Sicherheitsteams: Schnell und kostengünstig einen höheren Sicherheitsreifegrad erreichen	
	Erforderliche Merkmale ■ Fähigkeit zur Verfolgung gegnerischer Aktivitäten in Echtzeit ■ Überwachung nach einem Vorfall, um gerüstet zu sein, falls die Angreifer zurückkommen ■ Behebung falsch positiver Warnmeldungen
	Evaluierungskriterien ● Zeit zwischen der ersten Erkennung und dem detaillierten Vorfallsbericht mit der Anleitung zur Problemlösung ● Anzahl der erkannten Vorfälle zusätzlich zu den Vorfällen, die das eigene, interne Team erkennt ● Anzahl der untersuchten potenziellen Vorfälle zusätzlich zu den Vorfällen, die die Sicherheitsverantwortlichen des Kunden erkennen ● Test durch „rotes Team“ ● Kundenreferenzen und Erfahrungsberichte
	Relevante Fragen ● Wie erfahren sind die Experten für Bedrohungssuche und aus welchen Bereichen kommen sie? ● Sind sie auf die Suche nach Bedrohungen spezialisiert? Wenn nicht, welche weiteren Aufgaben nehmen sie wahr? ● Wie schneiden sie in der Bewertung durch andere Kunden ab?

DAS KONZEPT VON CROWDSTRIKE

Hinter CrowdStrike Falcon OverWatch™ steht ein beispielloses Team von engagierten Experten für die Bedrohungssuche, die in Verbindung mit den von der Falcon-Plattform gesammelten Daten in der Lage sind, Angriffe abzuwehren, die von keinem anderen System oder keiner anderen Technologie erkannt würden.

Das OverWatch-Team besteht aus hochqualifizierten und erfahrenen Analysten, die rund um die Uhr proaktiv nach Bedrohungen suchen. Sie beseitigen falsch negative Ergebnisse, indem sie bestehende Sicherheitsmechanismen erweitern und die Lücken in der Erkennung von Bedrohungen und der Vorfallreaktion schließen. Dies führt zu einer drastischen Verkürzung der Verweildauer von Angreifern oder deren vollkommener Beseitigung.

Mit OverWatch profitieren Anwender von den branchenweit besten Spezialisten für Sicherheit und Bedrohungssuche. Das Team nutzt die Vorteile der Cloud-nativen Architektur von CrowdStrike auf Basis des CrowdStrike Threat Graph™ und fahndet proaktiv nach ungewöhnlichen oder neuen Aktivitäten von Angreifern, die von Sicherheitstechnologien nicht erkannt werden können. Sobald eine Bedrohung identifiziert wird, arbeitet OverWatch Seite an Seite mit dem Kunden, leistet kompetente Beratung bei der Bewältigung des Vorfalls und gibt Anleitungen zu dessen Behebung. OverWatch bringt das wesentliche Element der menschlichen Expertise und Erfahrung ein, damit potenziellen Angreifern keine Lücke bleibt. Dies ist der Schlüssel gegen Sicherheitsverletzungen.

ENTSCHEIDENDES ELEMENT VIER: ANTIZIPATION

MIT BEDROHUNGSAUFKLÄRUNG DEN ANGREIFERN IMMER EINEN SCHRITT VORAUS SEIN

Warum Bedrohungsaufklärung unverzichtbar ist

Angreifer operieren schnell und verdeckt. Für Sicherheitstechnologien ebenso wie für Sicherheitsexperten ist es daher nicht einfach, mit den jeweils neuesten Bedrohungen Schritt zu halten und sich proaktiv vor ihnen zu schützen. Bedrohungsaufklärung hilft dabei, potenzielle Bedrohungen zu verstehen und effektiv vorherzusagen. Unternehmen können so das “Wer” und “Wie” des nächsten Angriffs antizipieren. Die Sicherheitsverantwortlichen können sich auf die Priorisierung und Konfiguration von Ressourcen konzentrieren, damit sie auf künftige Angriffe wirksam reagieren können.

Darüber hinaus liefert Bedrohungsaufklärung die Informationen, die die Sicherheitsteams befähigen, Vorfälle schneller zu verstehen, darauf zu reagieren und zu beheben, wodurch die Untersuchung von Vorfällen und die Reaktion darauf beschleunigt werden. Sicherheitsexperten, die sich mit dem Schutz von Endgeräten befassen, dürfen sich daher nicht nur auf die Sicherheitsinfrastruktur konzentrieren.

Eine fundierte Bedrohungsaufklärung muss als Teil der Gesamtlösung einbezogen werden. Die unkomplizierte Bereitstellung der entsprechenden Informationen ermöglicht schnellere und bessere Entscheidungen und Reaktionen. Anwender sollten dabei sicherstellen, dass die bereitgestellte Bedrohungsaufklärung nahtlos in die Endgerätelösung integriert ist und automatisierbar ist.

Die folgende Tabelle soll dabei helfen, die Integration der Bedrohungsaufklärung in die in Betracht kommende Lösung für den Endgeräteschutz zu bewerten.

INTEGRATION DER BEDROHUNGS-AUFKLÄRUNG: ANWENDUNGSFÄLLE UND WESENTLICHE LEISTUNGSMERKMALE

Maximierung der Abwehr: Priorisierung der Aktivitäten und Ressourcen; proaktiver Schutz gegen künftige Angriffe	**Erforderliche Merkmale** ■ Automatisch generierte, benutzerdefinierte Gefährdungsindikatoren und Informationen über Bedrohungen, die für eine gegebene Umgebung tatsächlich relevant sind, werden innerhalb weniger Minuten bereitgestellt ■ Automatisch eingebundene Gefährdungsindikatoren von Dritten ■ Berichte über Angreiferprofile zur Priorisierung von Aktivitäten und Ressourcen (z. B. welche Patches besonders wichtig sind usw.)
	Evaluierungskriterien ● Der Anbieter betreibt die Bedrohungsaufklärung in Eigenregie (ohne auf die Feeds von Dritten angewiesen zu sein) ● Der Anbieter ist in der Lage, Bedrohungsaufklärung und Informationen auf mehreren Ebenen bereitzustellen: strategisch, operativ, taktisch
	Relevante Fragen ● Wie werden Daten aus der Bedrohungsaufklärung in die Endpoint-Protection-Lösung integriert? ● Wie können Kunden die Daten aus der Bedrohungsaufklärung nutzen? Wie werden die Daten präsentiert und formatiert? ● Wie oft werden die Daten aus der Bedrohungsaufklärung aktualisiert? ● Wie viele Quellen und welche Art von Quellen verwendet der Anbieter für seinen Service?
Schnellere Erkennung	**Erforderliche Merkmale** ■ Automatische Warnungen zu gegnerischen Aktivitäten (nationalstaatliche Akteure oder Internetkriminelle), die in der Umgebung erkannt werden ■ Automatische Erkennung basierend auf der eigenen taktischen Bedrohungsaufklärung des Anbieters (z. B. bekannte gefährliche IPs, Domänen, Dateien usw.) ■ Möglichkeit zur automatischen Erzeugung und Nutzung von Gefährdungsindikatoren ■ Möglichkeit zur Durchführung benutzerdefinierter Prüfungen auf Gefährdungsindikatoren
	Evaluierungskriterien ● Integrationsgrad der Bedrohungsaufklärung in das Produkt - wie viel wird automatisiert und wie viel muss manuell bearbeitet werden?
	Relevante Fragen ● Erfahre ich, wer meine Organisation angreift? ● Was ist das Motiv des Angreifers? ● Welche Taktiken und Techniken verwendet der Angreifer? ● Welche Werkzeuge könnte er einsetzen?

Beschleunigung von Untersuchungen und Abhilfemaßnahmen	**Erforderliche Merkmale** ■ Ergänzung von Warnmeldungen und Erkennungen durch zusätzlichen Kontext zur beschleunigten Untersuchung ■ Zuordnung der Angriffe zu Angreifern oder Gruppen, damit klar ist, wer angreift, warum und mit welcher Priorität die Maßnahmen ergriffen werden müssen ■ Fähigkeit zur automatischen Analyse von Malware mit sofortiger Erstellung von Gefährdungsindikatoren und detaillierten Analyseberichten ■ Bereitstellung von Profilen zu Akteuren und Angreifern
	Evaluierungskriterien ● Fundierte Informationen: Wie können die Informationen zur Bedrohungsaufklärung genutzt werden?
	Relevante Fragen ● Welche Art von Informationen zur Bedrohungsaufklärung ist in den Warnmeldungen und Erkennungen enthalten?

DAS KONZEPT VON CROWDSTRIKE

CrowdStrike Falcon ist die erste Plattform, die die Bedrohungsaufklärung nahtlos in den Schutz der Endgeräte integriert, Untersuchungen von Vorfällen automatisiert und die Reaktion auf Sicherheitsverletzungen beschleunigt. Die sofortige Analyse von Bedrohungen, denen die Endgeräte ausgesetzt sind, kombiniert mit der Expertise des globalen CrowdStrike Falcon Intelligence™ Teams, ermöglicht es den Sicherheitsverantwortlichen, in Unternehmen und Institutionen für prädiktive Sicherheit zu sorgen, und zwar unabhängig von Größe und Kenntnisstand.

Falcon liefert die kritischen Sicherheitsinformationen, die Sicherheitsverantwortliche benötigen, um Angreifern voraus zu sein und Vorfälle so schnell wie möglich zu priorisieren und darauf effektiv zu reagieren. Falcon nutzt die Informationen und Erkenntnisse des Falcon Intelligence-Teams in vollem Umfang, um zusätzliche Kontexte für Warnungen und Vorfälle bereitzustellen.

Dadurch entfällt die ressourcenaufwendige Komplexität in den Untersuchungen zu Vorfällen. Die Endgeräteerkennung und Reaktion erreicht damit eine neue Stufe. Die Lösung macht nicht nur transparent, was am Endgerät passiert ist, sondern legt auch das „Wer, Warum und Wie" hinter dem Angriff offen. So ordnet Falcon beispielsweise Tools, Domänen, IPs, Taktiken und Techniken automatisch bekannten Angreifern zu. Detaillierte Angreiferprofile unterstützen proaktive Schutzmaßnahmen, falls einer dieser Akteure in einer Umgebung gefunden werden sollte.

Falcon kann die Malware-Analyse automatisieren und fundierte Informationen und benutzerdefinierte Gefährdungsindikatoren bereitstellen, die speziell den Bedrohungen zugeordnet sind, die an den Endgeräten eines Unternehmens oder einer Institution erkannt werden. Dank dieses Automatisierungsgrads können Sicherheitsverantwortliche sehr schnell priorisieren, welche Bedrohungen sie zuerst analysieren müssen. Das macht wertvolle Ressourcen für die Abwehr frei.

Falcon kombiniert die Tools, die von erstklassigen Spezialisten für Cyber-Bedrohung verwendet werden, in einer umfassenden Lösung und führt Untersuchungen automatisch durch. Diese enge und automatische Integration zwischen Falcon und der Bedrohungsaufklärung versetzt alle Teams, unabhängig von Größe und Expertise, in die Lage, Vorfälle besser zu verstehen, schneller darauf zu reagieren und den Angreifern stets einen Schritt voraus zu sein.

Die sofortige Analyse von Bedrohungen, denen die Endgeräte ausgesetzt sind, kombiniert mit der Expertise des globalen CrowdStrike Falcon Intelligence™ Teams, ermöglicht es den Sicherheitsverantwortlichen, in Unternehmen und Institutionen für prädiktive Sicherheit zu sorgen, und zwar unabhängig von Größe und Kenntnisstand.

ENTSCHEIDENDES ELEMENT FÜNF: EINSATZBEREITSCHAFT

VORBEREITUNG AUF DEN ANGRIFF MIT SCHWACHSTELLENBEWERTUNG UND IT-HYGIENE

Warum Schwachstellenanalyse und IT-Hygiene so wichtig sind

Sicherheit beginnt damit, Lücken zu schließen, um die Angriffsfläche zu verkleinern und besser auf Bedrohungen vorbereitet zu sein. Dies setzt das Wissen darüber voraus, welche Systeme und Anwendungen verwundbar sind und wer und was in der eigenen Umgebung aktiv ist. Deshalb sind Schwachstellenanalyse und IT-Hygiene die grundlegenden Bausteine einer effizienten Sicherheitspraxis und sollten Teil jeder robusten Lösung für den Endgeräteschutz sein. Beide Bausteine sorgen für Transparenz und fundierte Informationen. Genau diese werden von den Sicherheits- und IT-Teams benötigt, um vorbeugende Maßnahmen ergreifen zu können und für die komplexen Bedrohungen von heute vorbereitet zu sein.

Schwachstellenanalyse und IT-Hygiene können sehr viel bewirken. So sind beispielsweise veraltete und nicht gepatchte Anwendungen nach wie vor ein wichtiger Einstiegspunkt für Angriffe auf die IT-Umgebung von Unternehmen und Institutionen. Die Fähigkeit, gefährdete Anwendungen in der eigenen Umgebung zu erkennen, zu patchen und zu aktualisieren, verschafft Anwendern einen handfesten Vorteil gegenüber Angreifern.

Wer genau weiß, welche Systeme im eigenen Netzwerk laufen, kann Lücken in der Sicherheitsarchitektur proaktiv schließen. Die IT-Hygiene verleiht die Fähigkeit, nicht verwaltete Systeme oder solche, die ein Risiko für das Netzwerk darstellen könnten, zu identifizieren, wie beispielsweise ungeschützte BYOD- oder Drittsysteme.

Der Diebstahl von Zugangsdaten ist für Angreifer nach wie vor ein weiterer beliebter und effizienter Weg. Die Überwachung und Sichtbarmachung des Anmeldeverhaltens (Aktivitäten/Dauer) in der eigenen Umgebung überall dort, wo Zugangsdaten verwendet und Administrator-Zugangsdaten erstellt werden, ermöglicht es Sicherheitsverantwortlichen, den Missbrauch von Zugangsdaten sowie Angriffe mit gestohlenen Zugangsdaten zu erkennen und zu verhindern.

Schwachstellenanalyse und IT-Hygiene liefern die nötigen Informationen, um eine effiziente, proaktive Abwehr aufzubauen, die Sicherheitslage insgesamt zu verbessern und sich erfolgreich gegen Angreifer zu verteidigen.

Die folgende Tabelle soll bei der Bewertung der Schwachstellenanalyse und IT-Hygienefunktionen einer Endgeräteschutzlösung helfen.

IT-HYGIENE- UND SCHWACHSTELLENBEWERTUNG: ANWENDUNGSFÄLLE UND WESENTLICHE LEISTUNGSMERKMALE

Offenlegung von Schwachstellen	**Erforderliche Merkmale** ■ Fähigkeit zur Erstellung einer Liste von anfälligen Hosts und anderen in der Umgebung vorhandenen Schwachstellen ■ Fähigkeit zur Überprüfung von Anwendungen auf Schwachstellen ■ Differenzierung zwischen installierten Patches und erfolgreich installierten Patches ■ Keine Beeinträchtigung der Endgeräte (kein Scannen)
	Evaluierungskriterien ● Beeinträchtigung der Endgeräte ● Genauigkeit der Informationen (relevant, aktuell, vollständig usw.)
	Relevante Fragen ● Benötigt dieses Leistungsmerkmal einen zusätzlichen Agenten? ● Kann das Produkt installierte Patches von bereitgestellten Patches unterscheiden? ● Sind die Informationen aktuell oder ist ein Scan erforderlich, um auf den neuesten Stand zu gelangen?

Überwachung der Konten und der Nutzung privilegierter Konten	**Erforderliche Merkmale** ■ Identifizierung von Trends in der Kontennutzung: Hosts, an denen sich der Benutzer anmeldet, durchschnittliche Sitzungsdauer, Sitzungsdauer an jedem Host, Zeiten, zu denen der Benutzer typischerweise angemeldet ist, und Art der Registrierung (Batch, Remote) ■ Bereitstellung detaillierter Informationen zur Nutzung des lokalen und des Domänen-Administrationskontos ■ Anzeige der Hosts, die von einem Benutzerkonto verwendet wurden
	Evaluierungskriterien ● Bewertung des Dashboards und der bereitgestellten Berichte zur Kontennutzung
	Relevante Fragen ● Benötigt dieses Leistungsmerkmal einen zusätzlichen Agenten? ● Wie werden diese Informationen gesammelt? ● Wie ist dieses Leistungsmerkmal in die Lösung zum Endgeräteschutz integriert?
Identifikation ungeschützter Systeme und Auffinden nicht verwalteter gefährlicher („rogue“) Systeme	**Erforderliche Merkmale** ■ Echtzeitdarstellung der Assets in der Umgebung ■ Differenzierung zwischen verwalteten, nicht verwalteten und nicht unterstützten Assets, einschließlich Druckern, Kameras usw. ■ Kein Netzwerkscan erforderlich ■ Keine zusätzlichen Agenten erforderlich
	Evaluierungskriterien ● Bewertung des Dashboards und der Berichte mit den bereitgestellten Informationen
	Relevante Fragen ● Benötigt dieses Leistungsmerkmal einen zusätzlichen Agenten? ● Wie werden diese Informationen gesammelt? ● Wie ist dieses Leistungsmerkmal in die Lösung zum Endgeräteschutz integriert?
Überwachung der in der eigenen Umgebung ausgeführten Programme	**Erforderliche Merkmale** ■ Auflistung aller Anwendungen, die auf einem Endgerät und über alle Endgeräte in der Umgebung hinweg genutzt werden ■ Identifikation und Suche nach Anwendungen, die auf einem bestimmten Host oder von bestimmten Benutzern verwendet werden
	Evaluierungskriterien ● Bewertung des Dashboards und der Berichte mit den bereitgestellten Anwendungsinformationen
	Relevante Fragen ● Benötigt dieses Leistungsmerkmal einen zusätzlichen Agenten? ● Wie werden diese Informationen gesammelt? ● Wie ist dieses Leistungsmerkmal in die Lösung zum Endgeräteschutz integriert?

DAS KONZEPT VON CROWDSTRIKE

CrowdStrike Falcon Discover™ und Falcon Spotlight™ ermöglichen es Unternehmen, Sicherheitslücken zu schließen und sich besser auf Bedrohungen vorzubereiten. Das Sicherheitsbewusstsein wird gestärkt und die sicherheitsrelevanten Bereiche einer Infrastruktur werden sichtbar gemacht. Die Lösungen machen vorhandene Schwachstellen deutlich und zeigen die in einer Umgebung verwendeten Assets, Anwendungen und Konten auf. Der Agent von Falcon meldet Schwachstellen in Echtzeit, ohne Endgeräte zu scannen, und stellt fest, ob ein Patch nicht nur bereitgestellt, sondern auch erfolgreich angewendet wurde. So wird in Echtzeit sichtbar, was oder wer sich im Netzwerk befindet. Gefährliche, ungeschützte und nicht verwaltete Systeme, wie private Geräte (BYOD) oder Drittsysteme, werden identifiziert.

Über ein benutzerfreundliches Dashboard mit Drill-Down-Optionen zeigt das Anwendungsinventar in Echtzeit eine Ansicht aller in der Umgebung ausgeführten Anwendungen. So können Sicherheitsverantwortliche ohne Beeinträchtigung der Endgeräte sofort sehen, welche Anwendungen auf welchen Hosts derzeit ausgeführt werden. Sie können zudem ermitteln, wann die Anwendung ursprünglich gestartet wurde, und zu anderen Endgeräten mit derselben Anwendung wechseln und somit weiteren Kontext erhalten, beispielsweise zur Nutzung pro Anwendung oder pro Host.

Falcon überwacht das Anmeldeverhalten (Aktivitäten/Dauer) in der eigenen Umgebung überall dort, wo Zugangsdaten verwendet und Administrator-Zugangsdaten erstellt werden. So können Sicherheitsverantwortliche den Missbrauch von Zugangsdaten sowie Angriffe mit gestohlenen Zugangsdaten erkennen und verhindern.

Unter dem Strich bietet Falcon die erforderliche Schwachstellenanalyse und IT-Hygiene, mit der Sicherheitsverantwortliche die Sicherheitslage verbessern und sich auf die Abwehr von Angriffen besser vorbereiten können.

Der Sensor von Falcon hat praktisch keine Auswirkung auf das Endgerät und ist daher eine ausgezeichnete Wahl für virtuelle Umgebungen.

EINE CLOUD-BASIERTE ARCHITEKTUR FÜR DIE ENTSCHEIDENDEN ELEMENTE IN DER ENDGERÄTESICHERHEIT

Wenn Unternehmen wachsen und mehr verteilte Endgeräte installieren, können vor Ort installierte Lösungen schnell sehr komplex werden. Bis zur vollen Funktionsfähigkeit können Monate vergehen. Schon nach kurzer Zeit muss die gesamte Infrastruktur aktualisiert werden, um das jeweils höchste Schutzniveau zu gewährleisten. Oder es muss eine andere Komponente zum Schutz vor einer neuen Art von Bedrohung hinzugefügt werden. Der gesamte Implementierungsprozess muss dann oft erneut aufgesetzt werden. Bis zum Abschluss der Implementierung ist der Schutz dann nur lückenhaft.

Im Unterschied dazu ermöglicht eine Cloud-basierte Lösung einen dauerhaften Schutz über die gesamte Umgebung hinweg, und dies schneller, kostengünstiger und mit weniger Verwaltungsaufwand bei gleichzeitig mehr Leistung, Agilität und Skalierbarkeit.

Dadurch, dass keine Hardware und zusätzliche Software beschafft, bereitgestellt, verwaltet und aktualisiert werden muss, lässt sich die Endgerätesicherheit aus der Cloud schnell und einfach ausrollen. Während die vollständige Einführung von Systemen vor Ort bis zu einem Jahr dauern kann, können Cloud-basierte Lösungen in Umgebungen mit Zehntausenden von Hosts innerhalb weniger Stunden erfolgreich bereitgestellt werden. In der Cloud erfolgen die Aktualisierungen der Infrastruktur unverzüglich durch den Anbieter und verlangen vom Anwender keine monatelange Planung, die die Ressourcen des eigenen IT-Teams überfordern kann, sodass letztlich kein lückenloser Schutz gewährleistet ist.

Ein Cloud-basiertes Modell bietet zudem den Vorteil, umfangreiche Daten in Echtzeit sammeln und nach Bedarf skalieren zu können, wodurch große Datenmengen im Petabyte-Bereich monatelang gespeichert und in Sekundenschnelle analysiert werden können, ohne die Leistung der Endgeräte zu beeinträchtigen. Derart anspruchsvolle und komplexe Aufgaben können lokale Installationen kaum leisten. Und schließlich sind Cloud-Modelle unverzichtbar für den Schutz entfernter Systeme außerhalb des Netzwerks oder außerhalb des VPN.

Eine gut durchdachte Cloud-Architektur sollte folgende Leistungsmerkmale aufweisen:

1. Sofortige Einsatzbereitschaft, ohne dass vor der Bereitstellung eine Infrastruktur aufgebaut werden muss
2. Nahtlose Skalierung von Endgeräten und Ereignissen, ohne dass der Anwender eingreifen muss
3. Minimierung der Endgerätebelastung (z. B. sollten auf dem Endgerät keine Datenbanken zur Speicherung von Ereignisdaten erforderlich sein und für Suche und Analyse keine Endgeräteressourcen verbraucht werden)
4. Schnelle Analyse großer Datenmengen bei Lieferung genauer Ergebnisse

Die folgenden Fragen helfen, die wirklichen Fähigkeiten einer Endpoint Protection-Lösung mit Cloud-Architektur zu ermitteln:

- Wie lange dauert es, bis die Lösung voll einsatzbereit ist?
- Welche zusätzliche Hard- und Software (Server – physische oder virtuelle – Appliances, Datenbanklizenzen usw.) sind für die Implementierung der Lösung erforderlich?
- Handelt es sich um eine echte Cloud-Architektur oder eine virtualisierte Appliance, die in der Cloud gehostet wird?
- Muss der Anwender aktiv werden, wenn die Anzahl der Endgeräte wächst oder wenn der Umgebung zusätzliche Standorte hinzugefügt werden?
- Wie wirkt sich die Lösung auf Endgeräte, Festplattenspeicher, CPU-Auslastung und RAM-Nutzung aus?
- Wie wirken sich Suchvorgänge und die Ereigniserfassung auf die Endgeräte aus?
- Wie viele Ereignisse pro Sekunde kann die Cloud-Infrastruktur verarbeiten?
- Wie viele Endgeräte unterstützt die Architektur?

Die Cloud-basierte Architektur von CrowdStrike Falcon wurde von Anfang an mit dem Ziel entwickelt und implementiert, die Leistung und Skalierbarkeit der Cloud zu nutzen. Dadurch bietet CrowdStrike eine sofortige Time-to-Value. Unternehmen und Institutionen sind innerhalb weniger Stunden voll einsatzbereit, im Gegensatz zu Wochen oder Monaten, die für den Aufbau lokaler Systeme normalerweise erforderlich sind.

Dieser 100-prozentige Cloud-basierte Ansatz ermöglicht es zudem, Kosten zu senken und gleichzeitig Geschwindigkeit, Effizienz und automatische Skalierbarkeit zu erhöhen.

Die speziell entwickelte Cloud-Architektur von CrowdStrike unterstützt nicht nur eine schnelle und einfache Implementierung bei extrem niedrigen Wartungs- und Erweiterungskosten, sondern überzeugt auch durch eine Reihe von Alleinstellungsmerkmalen.

Die Falcon-Plattform von CrowdStrike ist die perfekte Lösung für Kunden, die Endgeräte schützen möchten, die auf einer Cloud-Plattform gehostet werden. Die Lösung eignet sich ideal für Anwender, die Endgeräte in einer hybriden Umgebung schützen müssen, unabhängig davon, ob diese sich innerhalb oder außerhalb des Netzwerks befinden oder in einer Cloud gehostet werden.

Dank dieser Architektur kann CrowdStrike über eine Billion Ereignisse pro Woche sammeln, analysieren und speichern, was mit einer lokalen Architektur kaum zu erreichen ist. Das Cloud-Modell von CrowdStrike beruht auf einer Graph-Datenbank für Bedrohungen und ist für die Speicherung eines großen und ständig wachsenden Datenvolumens ausgelegt. Diese Daten können über einen längeren Zeitraum verfügbar sein und die Architektur skaliert automatisch, um neue Daten aufzunehmen. Die Architektur macht die gründliche und schnelle Analyse dieser großen Datenmenge möglich und liefert innerhalb von Sekunden Antworten auf Suchanfragen – sogar bei Datenvolumen im Petabyte-Bereich.

Und schließlich werden die Daten in der Cloud über mehrere Umgebungen hinweg aggregiert, wodurch die Intelligenz und das Know-how aller Beteiligten ausgeschöpft werden können. Somit können alle CrowdStrike-Kunden vor neuen Bedrohungen geschützt werden, die in einer bestimmten Umgebung eines Kunden ermittelt werden, bevor sie sich weiter verbreiten.

Die Cloud-basierte Architektur von CrowdStrike Falcon wurde von Anfang an mit dem Ziel entwickelt und implementiert, die Leistung und Skalierbarkeit der Cloud zu nutzen.

FAZIT

Die Auswahl einer Lösung für den Endgeräteschutz kann eine Herausforderung darstellen, da der Endgerätemarkt durch Hunderte von Optionen gekennzeichnet ist. Jedes Produkt hat seine eigenen Leistungsmerkmale und Technologien. Die Unterschiede sind oft nicht leicht zu erkennen. Zur Vereinfachung und Verdeutlichung der Lage fasst CrowdStrike die Anforderungen an eine umfassende und effiziente Lösung für den Endgeräteschutz unter fünf entscheidenden Elementen zusammen, die in diesem Leitfaden eingehend erläutert wurden:

1. Prävention zur Abwehr von so vielen bösartigen Elementen wie möglich
2. Erkennung zum Auffinden und Ausschließen von Angreifern
3. Verwaltete Bedrohungssuche zur Verbesserung der Erkennung über die Automatisierung hinaus
4. Integrierte Bedrohungsaufklärung zum besseren Verständnis der Lage und zur Wahrung eines Vorsprungs gegenüber potenziellen Angreifern
5. IT-Hygiene und Schwachstellenbewertung zur Vorbereitung und Stärkung der Umgebung gegen Bedrohungen und Angriffe

Darüber hinaus müssen diese fünf Leistungsmerkmale über eine Cloud-basierte Architektur bereitgestellt werden. Nur so lässt sich die Geschwindigkeit, Flexibilität und Leistung erreichen, die zur Abwehr versierter Angreifer erforderlich sind.

Die Plattform CrowdStrike Falcon zum Schutz von Endgeräten wurde konsequent mit dem Ziel entwickelt, versierte Angreifer abzuwehren und Sicherheitsverletzungen zu stoppen. Die Lösung arbeitet mit einem einzigen schlanken Agenten für Prävention, Erkennung, Bedrohungssuche, Reaktion, Behebung, Schwachstellenanalyse und IT-Hygiene. Darüber hinaus besteht optional die Möglichkeit, mit Falcon Complete™ die Verwaltung rund um die Uhr in die Hände der Sicherheitsexperten von CrowdStrike zu legen. Diese Option ist mit einer Garantie von bis zu 1 Million US-Dollar verbunden.

Die Falcon-Plattform zum Schutz von Endgeräten wurde in der Cloud entwickelt und erstellt. Sie nutzt eine hochmoderne Graph-Datenbanktechnologie als Grundlage für die Falcon-Endgeräte-Agenten, die künstliche Intelligenz von CrowdStrike sowie alle sonstigen Komponenten der Falcon-Plattform. Wenn neue Sicherheitsanforderungen auftreten, wird die Plattform nahtlos erweitert und bietet somit den CrowdStrike-Kunden einen ultimativen Endgeräteschutz. Und dies alles über einen einzigen schlanken Agenten.

Wir stoppen Sicherheitsverletzungen.
Erfahren Sie mehr unter: www.crowdstrike.de

Folgen Sie uns: Blog |Twitter

ÜBER CROWDSTRIKE

CrowdStrike ist der führende Anbieter von cloudbasiertem Endgeräteschutz. Die Plattform CrowdStrike Falcon® sorgt mithilfe von künstlicher Intelligenz (KI) für sofortige Transparenz und Schutz im gesamten Unternehmen und verhindert Angriffe auf Endgeräte innerhalb und außerhalb des Netzwerks. CrowdStrike Falcon ist innerhalb von Minuten einsatzbereit. Vom ersten Tag an stehen damit fundierte Analysedaten für den Echtzeitschutz zur Verfügung. Die Lösung vereint nahtlosen Virenschutz der nächsten Generation mit erstklassiger Endgeräteerkennung und Reaktion (EDR) – unterstützt durch eine verwaltete Bedrohungssuche rund um die Uhr. Cloud-Infrastruktur und Single-Agent-Architektur minimieren die Komplexität bei gleichzeitiger Verbesserung der Skalierbarkeit, Administrierbarkeit und Schnelligkeit.

CrowdStrike Falcon schützt Kunden vor allen denkbaren Cyberangriffen mithilfe einer signaturlosen Bedrohungsabwehr anhand von Angriffsindikatoren (IOA) auf Basis hochentwickelter künstlicher Intelligenz und maschinellem Lernen. So werden bekannte und unbekannte Bedrohungen in Echtzeit gestoppt. Auf Basis von CrowdStrike Threat Graph™ korreliert Falcon auf Anhieb täglich mehr als 100 Milliarden Sicherheitsereignisse weltweit und kann so Bedrohungen sofort erkennen und abwehren.