WHITEPAPER

Warum Ihre Security in der Cloud nur noch stärker wird

Die wichtigsten Vorteile einer Sicherheitsanalyseplattform in der Cloud

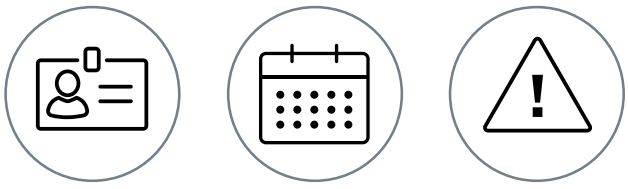
splunk> turn data into doing™

Moderne Sicherheitsbedrohungen zu entdecken, wird immer schwieriger, denn Hacker werden immer raffinierter. Gleichzeitig bieten sich immer mehr und immer komplexere Tools zur Abwehr von Cyberangriffen an. Darüber hinaus sind Unternehmen mit der Herausforderung konfrontiert, dass ihnen nicht genügend qualifiziertes Sicherheitspersonal zur Verfügung steht, um die Angreifer in Schach zu halten.

Cyberkriminelle | **Böswillige Insider** | **Nationalstaaten**

Die Lösung dieser Probleme muss jetzt angegangen werden – und nicht erst wenn der Kampf gegen eine komplexe Bedrohung bereits entbrannt oder die Untersuchung einer potenziellen Sicherheitsverletzung im Gange ist. Zeit ist ein knappes Gut, und Sicherheitsteams können es sich einfach nicht leisten, zu viel davon mit der Suche nach qualifizierten Mitarbeitern, Hardware oder Bereitstellungsmöglichkeiten zu vertun, schon gar nicht dann, wenn sie gerade eine potenzielle Bedrohung untersuchen müssen.

Damit sie Angreifern und komplexen Bedrohungen immer einen Schritt voraus sind, müssen Sicherheitsteams Ad-hoc-Analysen aller Daten durchführen können, die in der Cloud oder lokal gespeichert sind – im Netzwerk, an den Endpunkten, bei Identitäten, zu Erkenntnissen zum Hintergrund einer Bedrohung sowie Informationen, die nicht zu den üblichen Security-Daten zählen – und das praktisch in Echtzeit.



100 % der böswillig genutzten Logins sind gestohlene Account-Daten

99 Tage dauert es im Durchschnitt bis zur Erkennung (Median)

67 % der Opfer werden von Dritten aufmerksam gemacht

Außerdem müssen Unternehmen in der Lage sein, Bedrohungen, Angriffe und andere anormale Aktivitäten bei allen sicherheitsrelevanten Daten mit Business-Bezug in Echtzeit zu überwachen und in Berichte zu fassen. Erst mit hochentwickelten Analysefunktionen werden Bedrohungserkennung und Vorfallreaktion im gesamten Security-Ökosystem schnell genug.

Auf in die Cloud!

Die Situation erscheint düster, doch zum Glück besteht Hoffnung. Vielmehr bietet sich den Sicherheitsteams sogar die Chance, ihre Prozesse zugleich bei Sicherheit und Intelligence zu verbessern: mit einer Cloud-basierten, analysegestützten Sicherheitslösung, die sowohl Cloud-Workloads als auch die Systeme vor Ort schützt.

Eine Cloud-basierte, analysegestützte Sicherheitslösung ist eine Plattform, mit der Unternehmen den sich ständig verändernden Cyberbedrohungen immer einen Schritt voraus sind und Sicherheitsverletzungen rasch begegnen können, ohne dass sie ihre geschäftskritischen Prozesse vernachlässigen müssten.

Weil Cloud-Lösungen sehr flexibel sind, ist eine solche analysegestützte Sicherheitslösung eine Option für Unternehmen aller Größen. Und weil man weder zusätzliche Mitarbeiter einstellen noch teure Hardware anschaffen muss, spart sie sogar Kosten.

Eine Cloud-basierte, analysegestützte Sicherheitslösung ist stufenlos skalierbar und sorgt dafür, dass der Umstieg in die Cloud sicher verläuft und sicher bleibt. Darüber hinaus zeigt die Lösung detailgenau an, was im Security-Ökosystem und seinen Anwendungen vorgeht, egal ob hybrid oder rein in der Cloud. So können Unternehmen oft schon binnen Stunden nach der Cloud-Migration neuen Mehrwert schaffen.

Im Einzelnen können Unternehmen mit einer analysegestützten Sicherheitslösung in der Cloud fortschrittliche Malware erkennen, komplexe Bedrohungen untersuchen und darauf in Rekordzeit reagieren.

Außerdem verhilft eine Cloud-basierte Lösung Unternehmen dazu, dass sie die einschlägigen Compliance-Vorschriften rasch umsetzen und verlässlich einhalten können. Sie schützt das geistige Eigentum der Firma ebenso wie sensible Daten und kritische Assets.

Die Cloud bringt entscheidende Vorteile mit sich

Manche zweifeln noch immer, ob eine Sicherheitslösung in der Cloud wirklich unbedenklich ist. Doch deren Schutz unterscheidet sich nicht von dem vieler anderer SaaS-Lösungen (Software-as-a-Service), die schon jetzt zum Unternehmensalltag gehören. Eine Cloud-basierte Sicherheitslösung kann Informations- und Wissenslücken schließen, die viele Unternehmen bezüglich ihrer eigenen Sicherheitslage haben.

Bevor Sie eine Cloud-basierte Sicherheitslösung verwerfen, sollten Sie sich vor Augen führen, dass die Sicherheitsverfahren und -technologien bei den großen Cloud-Services in der Regel sehr viel ausgereifter sind als bei den allermeisten Unternehmen.

SaaS wird bereits flächendeckend bei CRM, HR, ERP, Business Analytics und anderen geschäftskritischen Systeme eingesetzt. Auch für die Bereitstellung weit verbreiteter Software wie Microsoft Office 365, Salesforce, Okta, Box, ServiceNow und AWS ist SaaS ein gängiges Modell.

Aus den gleichen Gründen, aus denen SaaS für Unternehmensanwendungen sinnvoll ist – schnelle, komfortable Bereitstellung, geringer Overhead, automatische Updates, nutzungsabhängige Abrechnung und skalierbare, gehärtete Infrastruktur – ist die Cloud hervorragend für Sicherheitslösungen geeignet.

Cloud-basierte Sicherheitslösungen bieten die Flexibilität, die nötig ist, um die ganze Vielfalt der Datensets aus sowohl Cloud- als auch Vor-Ort-Systemen zu nutzen. Und weil immer mehr Unternehmen ihre Workloads auf IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) und SaaS verlagern, beweist die Einfachheit der Integration mit Drittsystemen, die enorme Sinnhaftigkeit einer Sicherheitslösung in der Cloud.

Zu den wichtigsten Vorteilen einer in die Cloud verlagerten analysegestützten Sicherheitslösung gehören die Flexibilität einer hybriden Architektur, automatische Software-Updates und eine vereinfachte Konfiguration, die einsatzfertige, skalierbare Infrastruktur sowie starke Kontrollen und hohe Verfügbarkeit.

Flexible, hybride Architektur

Die Wirtschaft setzt mittlerweile verstärkt auf Cloud-Services, und viele Unternehmen arbeiten bereits in hybriden Umgebungen mit Daten und Anwendungen in der Cloud und on premises. Deshalb muss eine Sicherheitslösung – ganz gleich, wo sie angesiedelt ist – in der Lage sein, Daten aus beiden Umgebungen zu erfassen.

In Deutschland ist die Cloud weiterhin auf Wachstumskurs, dem Cloud Monitor 2020 zufolge nutzen bereits 76 % der Unternehmen Rechenleistungen aus der Cloud, und die Pandemie dürfte diese Entwicklung noch beschleunigt haben. Deloitte rechnet ab 2021 mit einem weltweiten Cloud-Wachstum von über 30 % jährlich. Dort, wo die Cloud-Migration weniger fortgeschritten ist, müssen die Firmen unverhältnismäßig viel in den Erhalt der Bestandssysteme investieren, was die IT-Budgets mit teils enormen Kosten belastet.

Mit einer Sicherheitslösung in der Cloud gewinnen Unternehmen vor allem größere Flexibilität: Bei einer Hybrid-Cloud-Implementierung kann die Sicherheitslösung aus dem eigenen Rechenzentrum des Unternehmens bereitgestellt werden, aber trotzdem Daten sowohl aus lokalen als auch aus den Cloud-Diensten aggregieren. Und sie kann ebenso als Cloud-Service fungieren, der Security-Daten von allen Seiten her abrufen kann.

Robuste, skalierbare Infrastruktur

Dabei ist zu bedenken, dass Bereitstellung und Betrieb der Infrastruktur für eine Sicherheitslösung vor Ort viel Zeit und operativen Aufwand erfordern.

Sicherheitssysteme müssen sowohl an die wachsenden Datenmengen als auch an die zunehmende Vielfalt der Quellen anpassbar sein. Eine analysegestützte Sicherheitslösung in der Cloud kann sofort bereitgestellt werden und ist problemlos skalierbar. Sie konsolidiert alle relevanten Sicherheitsinformationen in einem einzigen Repository, wo sie geschützt, indiziert und analysiert werden – damit fallen sämtliche Entscheidungen in Sachen Security deutlich leichter.

Hochverfügbarkeit und starke Kontrollen

Enterprise-Lösungen müssen grundsätzlich die Anforderungen erfüllen, die Unternehmen in puncto Sicherheit, Kontrolle und Performance an Cloud-Services stellen. Dazu gehören unter anderem folgende:

Daten- und Systemsicherheit: SaaS läuft meist auf AWS, der Google Cloud Platform, Microsoft Azure oder einer anderen der führenden IaaS-Plattformen. Diese großen Cloud-Provider betreiben Rechenzentren mit auditierten Sicherheitskonzepten, die Zertifizierungen nach SOC 2 Type II und ISO 27001 erreichen.

Zu den Best Practices für Sicherheitsservices zählt die logische Separierung der Kundendaten durch Zuweisung dedizierter virtueller Server und kundenspezifischer Speicher. Bei der Übertragung müssen die Kundendaten mit SSL und optional in der Ablage mit AES 256 Bit verschlüsselt werden, und zwar mit eindeutigen Schlüsseln, die regelmäßig rotiert werden.

Datenhoheit und die Standortfrage: Eine Hybrid-Cloud-Architektur ist eine gute Option für Sicherheitslösungen, weil Daten, deren Verarbeitung besonderen Datenschutzvorgaben oder gesetzlichen Anforderungen gerecht werden muss, entweder direkt vor Ort oder in der passenden Region eines IaaS-Anbieters bleiben können. Unternehmen, die ihre Lösung bei einem großen IaaS-Anbieter hosten lassen, haben die Möglichkeit, zwischen Regionen auf der ganzen Welt auszuwählen. In Europa gibt es sowohl große als auch regionale Provider, die auf hochsichere, DSGVO-konforme Dienste spezialisiert sind.

Kontrolle und Anpassung der Services: Die Migration in die Cloud darf nicht mit dem Verlust der Kontrolle über wichtige Anwendungseinstellungen und Sicherheitsrichtlinien einhergehen. Eine Cloud-basierte Sicherheitslösung muss Usern einerseits die volle Steuerungskontrolle auf Anwendungsebene geben,

sie andererseits aber vor den Details auf Infrastrukturebene verschonen. Dann können Unternehmen ihre Lösungen passgenau einrichten, während sie interne und externe Anforderungen problemlos erfüllen.

Performance und Verfügbarkeit: Wenn die Sicherheitslösung bei einem der großen IaaS-Provider wie AWS läuft, bekommt man erstklassige Systemverfügbarkeit zu einem vernünftigen Preis. Zum Beispiel kann der Security-Service so eingerichtet werden, dass er mehrere Verfügbarkeitszonen oder -regionen umfasst; damit bleibt er auch dann noch verfügbar, wenn ein einzelnes Rechenzentrum offline geht.

Und jetzt kommt Splunk

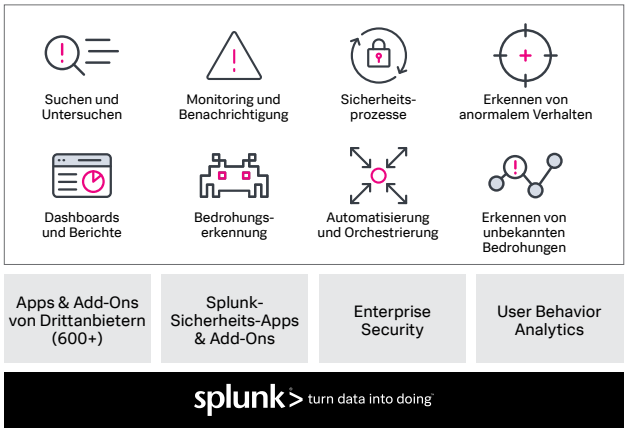
Das Portfolio Cloud-basierter, analysegestützter Sicherheitslösungen von Splunk besteht aus Splunk Enterprise (die SaaS-Entsprechung heißt Splunk Cloud), Splunk Enterprise Security (ES) und Splunk User Behavior Analytics (UBA). Damit führen Unternehmen mehrere IT-Bereiche zusammen, erleichtern die Zusammenarbeit und implementieren Best Practices zur Abwehr moderner Cyberbedrohungen.

Splunk Enterprise wird auf AWS bereitgestellt. Es handelt sich um ein in sich geschlossenes Softwarepaket, das leicht auf EC2-Instances verteilt und horizontal skaliert werden kann. Damit eignet sich die Lösung optimal für eine AWS-Bereitstellung.

Mit der Splunk-Plattform als Schaltzentrale können Security-Teams statistische, visuelle, verhaltensbasierte und explorative Analysen starten, um neue Erkenntnisse zu gewinnen, Entscheidungen zu erleichtern und erforderliche Maßnahmen abzusichern.

Big Data und Cloud-basierte Sicherheit – ein Kraftpaket

Eine Sicherheitslösung, die in der Cloud läuft, hat viele Vorteile – und noch mehr in Kombination mit einer Big-Data-Analyseplattform wie Splunk, die Log-Analysen und Berichte zu sämtlichen System- und Anwendungsmetriken liefert. Eine solches Doppel bietet durchgängiges End-to-End-Anwendungsmonitoring, schnelle Fehlersuche und intelligente Sicherheitsanalyse vereint mit einer umfassenden, analysegestützten Sicherheitslösung.



Die besten Sicherheitsanalyseplattformen sind darauf ausgelegt, Log-Einträge aus zahllosen Systemen zu erfassen, zu sammeln und auszuwerten. Es handelt sich um bewährte Lösungen, die in großen und kleinen Unternehmen gleichermaßen eingesetzt werden. Diese Plattformen bieten Datenerfassung in Echtzeit, ein Suche in allen Daten mithilfe einer leistungsstarken Abfragesprache sowie Funktionen zur Datenvisualisierung und statistische Analysen mit Echtzeiteinspeisung in übersichtliche Dashboards.

Die Kombination von Sicherheitslösung und Big-Data-Plattform ermöglicht Datenabfragen aus beliebigen Systemen und gibt Unternehmen eine zentrale, einheitliche Übersicht über die wichtigsten Metriken aus dem operativen Bereich, der Anwendungsperformance und der Sicherheit. Durch die Bereitstellung als Cloud-Service profitieren Unternehmen sofort von sämtlichen Vorteilen – ohne Lehrgeld und langwierige Einrichtung, ohne große Anfangsinvestitionen.Stattdessen können sie sofort Daten aus allen Umgebungen sammeln und analysieren, sowohl aus Clouds als auch aus lokalen Systemen.

Ein Cloud-Service ist die perfekte Lösung für Security-Bereitstellungen, weil die Quellen sicherheitsrelevanter Informationen laufend mehr werden und das Datenvolumen insgesamt rasant ansteigt. Wer seine Sicherheitslösung auf einer bewährten Data-to-Everything Plattform wie Splunk aufsetzt, kann deren leistungsstarke Funktionen, die ursprünglich zur Optimierung der IT-Abläufe entwickelt wurden, dann auch für ein besseres, schärferes und reaktionsschnelleres Security-Management nutzen.

Testen Sie jetzt Splunk Enterprise Security! Überzeugen Sie sich von der Leistungsfähigkeit von Splunk Enterprise Security – ganz ohne Downloads, Hardware-Einrichtung und Konfiguration. Mit der Online-Sandbox für Splunk Enterprise Security bekommen Sie 7 Tage lang Zugriff auf eine Testumgebung mit realitätsnahen Daten in der Cloud, die Sie durchsuchen, visualisieren und analysieren können; ebenso können Sie dort Vorfälle aus verschiedensten Sicherheitsbereichen eingehend untersuchen. Sie können aber auch die Schritt-für-Schritt-Anleitung durchgehen und so die leistungsfähigen Visualisierungen und Analysen der Splunk-Software kennenlernen. Jetzt mehr erfahren.

splunk>

Weitere Informationen: www.splunk.de/asksales

www.splunk.de

20-16126-Why You Should Take Security in the Cloud-A4-102-WP_GER