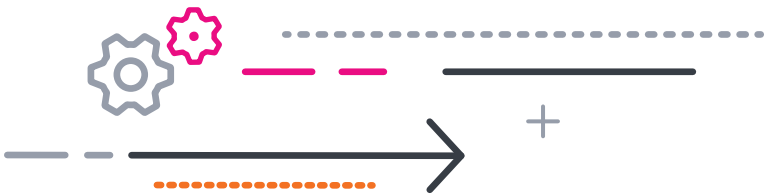
3 Must-Haves für das Management von Multi-Cloud-Komplexität

Ein Leitfaden für CIOs, CTOs und CISOs
auf ihrem Weg in die Cloud

splunk>
turn data into doing™



In zu vielen Unternehmen stehen Cybersecurity-, IT- und DevOps-Teams heute vor einem Dilemma: Sie haben eine Multi-Cloud- oder Hybrid-Cloud-Umgebung aufgesetzt, doch die unterstützenden Systeme, die sicherstellen, dass diese Technologieumgebungen beim Erreichen der Unternehmensziele helfen, haben mit dieser Entwicklung nicht Schritt gehalten. Wie ist diese Situation entstanden und was können sie jetzt tun?

Heute arbeiten praktisch alle Unternehmen mit einer Multi-Cloud- oder Hybrid-Cloud-Umgebung. Laut einer Befragung der IDC setzen 93 % der Unternehmen auf mehrere Clouds. Die Entscheidung für mehrere Clouds kann z. B. aus dem Wunsch heraus getroffen worden sein, Kosten zu sparen und die Bindung an einen bestimmten Anbieter zu vermeiden, die Ausfallsicherheit zu erhöhen, oder vielleicht haben Unternehmen aufgrund von Entscheidungen verschiedener Teams nun mehrere Clouds. Die Realität ist, dass sich nur sehr wenige Unternehmen zuerst fragen, wie sie ihre Technologie sichern und überwachen können, bevor sie diese strategischen Technologieentscheidungen treffen.

Doch nachdem die Entscheidung für eine Multi-Cloud- oder Hybrid-Cloud-Umgebung gefallen ist, stellen die Security-, IT- und DevOps-Teams in diesen Unternehmen fest, dass diese Umgebungen besondere Herausforderungen mit sich bringen. Es lässt sich nur schwer der Überblick über alle Cloud-Dienste in einem Unternehmen behalten, da die Einrichtung einer neuen Cloud-Infrastruktur heute so einfach ist wie ein Online-Einkauf. Gleichzeitig steigt die Komplexität, da sich die Abläufe über eine verteilte Technologielandschaft erstrecken. Durch die immer größer werdende Angriffsfläche wird es schwieriger, die Sicherheit aller Teilsysteme zu gewährleisten: Security-Teams müssen neue Bedrohungen abwehren und gleichzeitig Cloud-Services und -Tools verwalten, die bei keinen zwei Anbietern gleich sind. Darüber hinaus steigt das Potenzial für redundante Kosten, da die Teams innerhalb eines Unternehmens ihre eigenen Tools einsetzen und Funktionen manchmal doppelt in Anspruch genommen werden. Wird die Komplexität aufgrund mangelnder Transparenz und fehlender Kontrolle nicht bewältigt, führt dies zu verpassten Chancen und potenziell kostspieligen Fehlern.

Gleichzeitig stellen die Security-, IT- und DevOps-Teams in diesen Unternehmen fest, dass ihre bisherigen Ansätze für Monitoring und Troubleshooting nicht ausreichen für die neue, komplexere Cloud-Landschaft. Untersuchungen zeigen, dass nur 11 % der Entscheidungsträger mit ihren Monitoring-Tools zufrieden sind. Ältere Technologien wurden für lokale Infrastrukturen und monolithische Anwendungen entwickelt. In der damaligen Welt waren Batch-Processing und Aktualisierungen alle paar Minuten genug. In einer Container-basierten, Cloud-nativen Umgebung führt die Kurzlebigkeit der Aktivierung und Deaktivierung von Diensten jedoch dazu, dass eine Stapelverarbeitung nicht geeignet ist. Doch Tools, die speziell für die Cloud-native Welt entwickelt wurden, reichen möglicherweise nicht aus, da die große Mehrheit der Unternehmen ihre Systeme über alte und neue Generationen hinweg verteilt hat. Folglich ist Transparenz ebenso von zentraler Bedeutung wie die Möglichkeit, in verschiedenen Umgebungen Maßnahmen ergreifen zu können. Und wie verhält es sich mit den nativen Tools der Anbieter von Cloud-Diensten? Sie haben zwar deutliche Fortschritte gemacht, sind aber in erster Linie auf Transparenz für ihre eigenen Dienste ausgerichtet.

Unternehmen, die auf Multi-Cloud und Hybrid-Cloud umgestiegen sind und festgestellt haben, dass sie die Art und Weise, wie sie ihre Umgebungen verwalten, ändern müssen, benötigen einen Daten-Backbone, um ihren Erfolg sicherzustellen. Ein solcher Daten-Backbone für moderne Technologielandschaften erfordert Tools, die IT- und DevOps-Mitarbeitern Monitoring-Funktionen und Sicherheitsexperten eine End-to-End-Ansicht bieten, damit sie untersuchen, überwachen, analysieren und nach diesen Erkenntnissen handeln können.

Unternehmen müssen die traditionellen Monitoring-Ansätze hinter sich lassen und die Observability verbessern. Monitoring und Observabilty gehen zwar Hand in Hand, aber während das Monitoring zeigt, ob das System funktioniert, können Unternehmen mithilfe von Observabilty fragen, warum genau es nicht funktioniert. Anders ausgedrückt: Das Monitoring schlägt bei vorhersehbaren Ausfällen Alarm, während die Observabilty einen Einblick in alle möglichen Kombinationen vollständiger und teilweiser Ausfälle ermöglicht. Für Unternehmen ist es von entscheidender Bedeutung, ihre Systeme beobachtbar zu gestalten, damit sie in der Multi-Cloud- und Hybrid-Cloud-Landschaft den Überblick behalten können. Im Bereich der Sicherheit benötigen Unternehmen vor allem Transparenz und Kontrolle, um die Komplexität moderner Infrastrukturen zu verwalten. Eine einzige Ansicht aller Systeme zur Normalisierung und Verwaltung von Daten in der gesamten Hybrid-Infrastruktur hilft Sicherheitsanalysten bei der Zentralisierung von Ergebnissen, der Priorisierung von Warnungen und der Rationalisierung von Untersuchungen.

3 Must-Haves für den Erfolg von Multi-Cloud- und Hybrid-Cloud-Umgebungen

Jedes Security-, IT- und DevOps-Team benötigt für den Betrieb seines Daten-Backbone die folgenden Fähigkeiten:

1. **Analyse beliebiger Daten aus beliebigen Quellen und in beliebigem Umfang:** Die Teams müssen in der Lage sein, alle Daten in den Clouds und vor Ort zu nutzen, um proaktiv eine Erkennung, Warnung und Untersuchung einleiten zu können. David Linthicum, Vordenker in Sachen Cloud, drückt es wie folgt aus: „Tatsache ist, dass man ohne eine solide Abstraktionsebene, die für operative Einfachheit und Observability sorgt, nicht erfolgreich sein kann."
2. **Echtzeit-Erkenntnisse:** Aufgrund der kurzlebigen Natur des containerisierten Betriebs und der „as-a-Service"-Funktionen haben Unternehmen nicht minutenlang Zeit, um herauszufinden, ob Probleme mit der Infrastruktur bestehen. Nur eine skalierbare Streaming-Architektur kann Daten schnell genug erfassen, analysieren und melden, um so Probleme zu erkennen, zu untersuchen und zu verhindern, dass Kunden dadurch beeinträchtigt werden.
3. **Analysen, die Teams zum Handeln befähigen:** Da Multi-Cloud- und Hybrid-Cloud-Strategien nicht nur von einem einzelnen Team verfolgt werden, müssen Unternehmen in der Lage sein, Daten teamintern und teamübergreifend zu analysieren, um zeitnah Entscheidungen treffen und Maßnahmen ergreifen zu können. Bei der Förderung und Sicherung der Cloud-Transformation spielen insbesondere IT-, DevOps- und Sicherheitsteams eine entscheidende Rolle. Sie müssen analysieren und aufgrund dieser Analysen handeln und dabei stets auf die aktuellsten Daten zurückgreifen können.

Mit diesen drei Fähigkeiten sind Unternehmen auf einem guten Weg, ihre Multi-Cloud- und Hybrid-Cloud-Umgebungen erfolgreich sichern, betreiben und weiterentwickeln zu können.

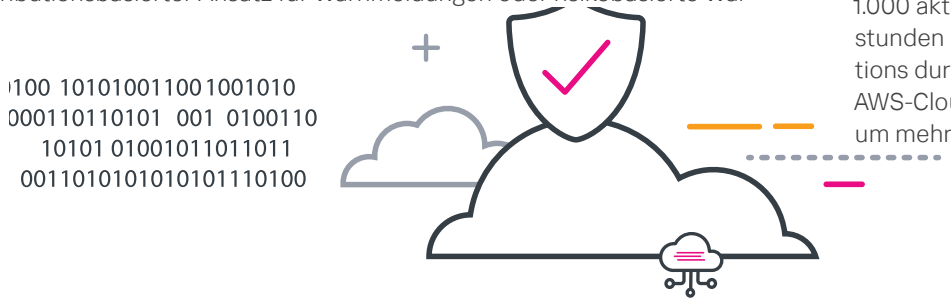
Sicherheit

Jüngste Attacken zeigen, wie wichtig es ist, die Sichtbarkeit aller Daten in Clouds und lokalen Infrastrukturen sowie in den Bereichen zwischen diesen Umgebungen zu gewährleisten, wenn Daten von einem Dienst zum anderen fließen. Die durchschnittliche Verweildauer von Sicherheitsbedrohungen beträgt weltweit 56 Tage – mehr als genug Zeit für Hacker, um erheblichen Schaden anzurichten. Die MITRE Cloud ATT&CK Matrix dokumentiert, dass Cyberkriminelle immer vielfältigere Taktiken und Techniken gegen Cloud-basierte Unternehmensdienste einsetzen.

Vor diesem Hintergrund ist es von entscheidender Bedeutung, die erste oben erwähnte Fähigkeit im Bereich der Sicherheit zu etablieren: Unternehmen müssen in der Lage sein, alle Daten aus jeder Quelle und in großem Umfang zu erfassen. Durch die Erfassung aller Daten – und deren ordnungsgemäße Analyse und Priorisierung – werden blinde Flecken in verteilten Ökosystemen beseitigt, die zu Sicherheitslücken führen und sowohl die Durchführung von Untersuchungen als auch die Ermittlung von Lösungen behindern können. Mit End-to-End-Transparenz ist es Unternehmen möglich, Bedrohungen von einer einzigen Stelle aus zu überwachen, was ihre Sicherheitslage vereinfacht und stärkt.

> Durch die Erfassung aller Daten werden blinde Flecken in verteilten Ökosystemen beseitigt.

Unternehmen benötigen außerdem Echtzeiteinblicke in diese Daten und sie müssen in der Lage sein, ihren gesamten Technologiestack in kürzester Zeit zu untersuchen. Schnelle Untersuchungen führen zu kurzen Reaktionszeiten und minimieren die Auswirkungen von Sicherheitsbedrohungen. In Anbetracht der Tatsache, dass die Security-Teams von heute oft unterbesetzt und von der Menge der Warnmeldungen überfordert sind, reichen Echtzeiteinblicke allein jedoch nicht aus. Ein attributionsbasierter Ansatz für Warnmeldungen oder risikobasierte Warnungen tragen dazu bei, die Menge an Alarmen drastisch zu reduzieren, sodass die Analysten mehr Zeit haben, sich auf echte Bedrohungen zu konzentrieren. Darüber hinaus sind Automatisierung und Orchestrierung wichtige Sicherheitsfunktionen, die Analysten dabei helfen, Warnungen schneller zu erkennen, zu untersuchen und auf sie zu reagieren. So können Sicherheitsteams beispielsweise automatisierte Playbooks nutzen, um SIEM-Warnungmeldungen zu sortieren, verdächtige Aktivitäten zu blockieren oder Sicherheitsvorfälle in Maschinengeschwindigkeit vollständig zu beheben. Mit diesen Tools können Security-Teams ihre Reaktionszeit verkürzen und sich auf das Wesentliche konzentrieren.



Ein Beispiel für die Ergebnisse, die Unternehmen mit der Implementierung einer datengesteuerten Multi-Cloud- und Hybrid-Cloud-Sicherheitsstrategie erzielen können, stammt von einem großen europäischen multinationalen Hersteller. Dieses Unternehmen war in seiner komplexen Umgebung mit einer großen Anzahl blinder Flecke konfrontiert. Um dieses Problem zu beheben, setzte es auf Splunk als einzige Sicherheitsplattform weltweit für 350 Anwendungsfälle im Security Operations Center (SOC). Nach 18 Monaten erreichte das Unternehmen eine 40-fache Steigerung der im Monitoring befindlichen Assets und eine Verachtfachung der täglich analysierten Datenmenge. Auch die Automatisierung konnte deutlich gesteigert werden: 80 % der Warnmeldungen der Stufe 1 und 50 % der Warnmeldungen der Stufe 2 wurden automatisch beantwortet, was den 1.000 aktiven Nutzern, die die Plattform jeden Monat nutzen, unzählige Arbeitsstunden einspart. Darüber hinaus konnte die Abteilung Cloud Security Operations durch einen datengesteuerten Ansatz die Compliance-Abweichungen von AWS-Cloud-Ressourcen gegenüber den Unternehmensstandards und -richtlinien um mehr als 50 % reduzieren.

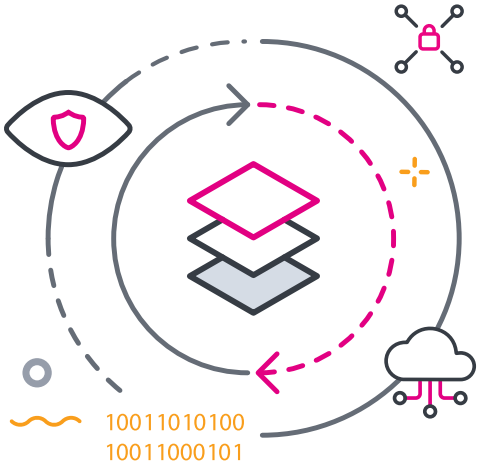
> … nach 18 Monaten konnten sie eine 40-fache Steigerung der überwachten Assets und eine Verachtfachung der täglich analysierten Datenmenge feststellen.

Betrieb

Der Multi-Cloud- und Hybrid-Cloud-Stack erschwert den Überblick über die gesamte IT-Landschaft. Datensilos führen dazu, dass es länger dauert, um Probleme zu erkennen und zu lösen. Außerdem sind Cloud-native Technologien wie Container und serverlose Funktionen oft nur Sekunden oder Minuten in Betrieb, sodass Unternehmen in der Lage sein müssen, das Monitoring und Ergreifen von Maßnahmen in Echtzeit zu gewährleisten. Diese Herausforderungen entstehen vor dem Hintergrund immer höherer Erwartungen von Kunden und Mitarbeitern an eine jederzeit reibungslose digitale Erfahrung, ohne Ausfälle oder andere Leistungsprobleme.

> Um diese Herausforderungen zu bewältigen, müssen Unternehmen dazu übergehen, alle ihre Systeme beobachtbar zu gestalten.

Um diese Herausforderungen zu bewältigen, müssen Unternehmen dazu übergehen, alle ihre Systeme beobachtbar zu gestalten. Sie müssen sowohl die Transparenz als auch die Kontrolle über die gesamte IT-Landschaft gewährleisten und alle Daten in Clouds und vor Ort nutzen, um proaktiv Probleme zu erkennen, Warnhinweise auszugeben, Untersuchungen durchzuführen und Leistungsprobleme zu reduzieren. Diese Transparenz schafft darüber hinaus neue Möglichkeiten zur Optimierung und Kostensenkung, z. B. durch die Identifizierung von Überversorgungen mit Ressourcen. Zudem erfordern Cloud-native Technologien Monitoring und Untersuchungen in Echtzeit – etwas, das herkömmliche Monitoring-Tools nicht leisten können. Und schließlich können integrierte KI/ML-gestützte Analysen bei all den Vorfällen, mit denen ITOps- und DevOps-Teams konfrontiert sind, dazu beitragen, Untersuchungen zu beschleunigen, Workflows zu optimieren und zukünftige Leistungseinbußen und Ausfälle zu antizipieren.



Der japanische Anbieter von Kreditkartenzahlungs- und Marketingdiensten Vesca konnte durch die Aktualisierung seiner Technologien während der COVID-19-Pandemie eine Reihe dieser operativen Vorteile für sich nutzen. Vesca verzeichnete aufgrund der gestiegenen Nachfrage nach E-Commerce und bargeldlosem Zahlungsverkehr mit über zehn Millionen monatlichen Kreditkartenzahlungen ein starkes Wachstum seiner Geschäftsaktivitäten. In der Vergangenheit kam es oft vor, dass zwei oder drei Personen einen ganzen Tag damit beschäftigt waren, einen einzigen Systemfehler zu beheben. Trotz des zusätzlichen Geschäftsvolumens war das Unternehmen dank Splunk in der Lage, selbst mit dem durch die Pandemie begrenzten Personalbestand ein reibungsloses Monitoring seiner Cloud-Architektur zu gewährleisten. Vesca verzeichnete nach der Implementierung von Splunk eine 99 %-ige Verringerung des Workloads bei der Incident Response und kann dadurch Probleme automatisch in wenigen Minuten statt in einem ganzen Tag erkennen.

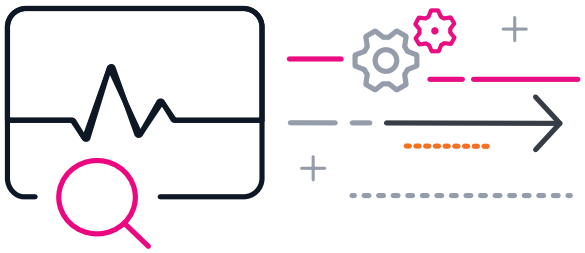
> Vesca verzeichnete nach der Implementierung von Splunk einen Rückgang des Incident-Response-Workloads um 99 %.

Innovation

Es kann eine große Herausforderung darstellen, das richtige Gleichgewicht zu finden zwischen der Freiheit für Entwickler und andere Teams, ihre eigenen Cloud-Dienste zu wählen, und dem Etablieren strenger Richtlinien zur Vermeidung von Schatten-IT. Unternehmen haben oft Schwierigkeiten, alle Cloud-Dienste zu erfassen, für die sie bezahlen und die sie überwachen und sichern müssen. Darüber hinaus bereitet die fehlende Transparenz der Infrastruktur DevOps-Teams Kopfzerbrechen, da sie die Ursache von Problemen nur schwer ausfindig machen können.

Multi-Cloud wird zwar oft als Mittel zur Kostenoptimierung oder zur Erhöhung der Ausfallsicherheit betrachtet, doch wenn sie richtig eingesetzt wird, fördert eine Multi-Cloud-Strategie auch die Innovationskraft in Unternehmen, indem sie durch Auswahl, Flexibilität und Dynamik zum Experimentieren anregt. Entwickler-, IT- und Architektenteams können die Dienste auswählen, die für das jeweilige Problem am besten geeignet sind, anstatt durch eine begrenzte Anzahl von Funktionen Einschränkungen zu erfahren. Multi-Cloud gibt Unternehmen die Möglichkeit, die besten Lösungen für jedes Problem zu finden, und kann dadurch letztlich das Geschäftsergebnis verbessern. Eine Umgebung mit handverlesenen Best-of-Breed-Tools, die ihre Geschäftsergebnisse optimieren, ist für Unternehmen heute nicht mehr nur eine Wunschvorstellung. Sie sind in der Lage, aus den besten Optionen Lösungen zu verwenden und zu erstellen, um die effektivsten Benutzererfahrungen und Geschäftsergebnisse zu erreichen.

> Multi-Cloud gibt Unternehmen die Möglichkeit, die besten Lösungen für jedes Problem zu finden, und kann dadurch letztlich das Geschäftsergebnis verbessern.



Dank Observabilty kann diese Vision Wirklichkeit werden. Führungskräfte können Transparenz gewährleisten und die Kontrolle über ihre Umgebung behalten, unabhängig davon, wie die Entwickler sie nutzen. Mit anderen Worten: Es gibt keine Schatten-IT mehr, da Unternehmen über vollständige Transparenz all ihrer Cloud-Dienste verfügen. Durch die Analyse aller Daten aus einer beliebigen Anzahl von Quellen in Echtzeit sind Unternehmen in der Lage, all ihre Cloud-Dienste zu erkennen, zu überwachen und zu warten und diese Informationen im gesamten Unternehmen zu verbreiten – für ITOps, DevOps, Sicherheit, Business-Bereiche und darüber hinaus.

> Splunk unterstützt Nasdaq dabei, die Lücke zwischen seinen Cloud- und On-Premises-Ökosystemen zu schließen und Zeit für Teams freizusetzen, die neue Produkte für Kunden entwickeln.

Die Nutzung all ihrer Daten hilft den Teams auch dabei, sicherzustellen, dass die Infrastruktur über den gesamten Technologiestack hinweg und vom Frontend bis zum Backend ordnungsgemäß funktioniert. Entwickler können Leistungsprobleme reduzieren und sicherstellen, dass die Infrastruktur mit den Anforderungen des Unternehmens skaliert, sodass sie mehr Zeit für Innovationen aufwenden können.

Nasdaq ist ein Paradebeispiel für die Notwendigkeit, in einem heterogenen Umfeld innovativ aufzutreten. Das Unternehmen setzt auf Splunk für das Monitoring und das Troubleshooting seiner Infrastrukturen, Anwendungen und Betriebssysteme in seinem Hybrid-Cloud-Stack. Dadurch kann Nasdaq das tun, was es am besten kann – spezialisierte Anwendungen für Kapitalmärkte, Handel und Marktdaten entwickeln. Da Splunk die Untersuchung beliebiger Daten aus beliebigen Quellen ermöglicht, unterstützt es Nasdaq dabei, die Lücke zwischen seinen Cloud- und On-Premises-Ökosystemen zu schließen und Zeit für Teams freizusetzen, die neue Produkte für Kunden entwickeln. Weitere Informationen über die Erfahrungen des CIO/CTO von Nasdaq erhalten Sie hier.

Ein Daten-Backbone neue Technologielandschaften

Angesichts der Herausforderungen und Chancen einer Multi-Cloud- und Hybrid-Cloud-Umgebung benötigen Unternehmen eine einzige, einheitliche Lösung, um alle ihre Daten zu zentralisieren, Einblicke in Echtzeit zu erhalten und Maßnahmen auf der Grundlage von Analysen zu fördern.

Splunk ist der Daten-Backbone für die neue Technologielandschaft und beschleunigt die Cloud-Transformation, indem es umfassende Datenstrategien für IT-, DevOps- und Security-Teams fördert, damit diese über Multi-Cloud- und Hybrid-Cloud-Umgebungen hinweg eine verbesserte Sicherheit, einen schnelleren Betrieb und mehr Innovationen gewährleisten können.

Mit der leistungsstarken Kombination aus der führenden Datenplattform und speziell entwickelten Lösungen hilft Splunk Unternehmen, die Komplexität zu überwinden und die Vorteile der Cloud-Transformation zu nutzen: mehr Flexibilität, optimierte Kosten, Sicherung der wichtigsten Assets und Reduzierung der Ausfallzeiten.

91 der Fortune-100-Unternehmen setzen auf Splunk. Es wird also auch in Ihrem Unternehmen wahrscheinlich heute bereits eingesetzt. Sprechen Sie mit Ihrem Team darüber, wie Sie die Splunk-Plattform nutzen können, um die Multi-Cloud- und Hybrid-Cloud-Erfahrung zu verbessern.

Erfahren Sie mehr.

Besuchen Sie splunk.de, um mehr darüber zu erfahren, wie Sie Ihre Cloud-Transformation in Ihrer Multi-Cloud- und/oder Hybrid-Umgebung mit der branchenführenden Datenplattform und Best-in-Class-Lösungen beschleunigen können.

21-18311-3 Must-Haves for Managing Multicloud Complexity-LS-114_DE

splunk>
turn data into doing™