

SECURITY UND DATEN-WORKLOAD-TRANSFORMATION: SPLUNK WORKLOADS IN AWS MIGRIEREN UND OPTIMIEREN MIT COMPUTACENTER

Autoren:

Archana Venkatraman

Duncan Brown

Februar 2021

Gesponsert von



Security und Daten-Workload-Transformation: Splunk Workloads in AWS migrieren und optimieren mit Computacenter

Einleitung

Wir stehen an der Schwelle zu einem neuen Zeitalter der digitalen Wirtschaft: Bis 2022 werden 65 % des globalen BIP durch die Produkte und Dienstleistungen digital transformierter Unternehmen erwirtschaftet.

Das bedeutet: Digitale Unternehmen müssen dynamisch, widerstandsfähig und agil sein. Um diese Ziele zu unterstützen, müssen Verantwortliche in Unternehmen sicherstellen, dass ihre IT genauso agil, digital und dynamisch aufgestellt ist. Die Cloud wird dabei zur De-facto-Grundlage für eine digitale Infrastruktur: Laut einer Studie von IDC nennen 40 % der europäischen Unternehmen Innovation als Hauptgrund für die Einführung der Nutzung einer Public Cloud.

Dabei zeichnet sich schon jetzt ab, dass der durch die globale Pandemie ausgelöste Handlungsdruck die digitale Transformation und damit auch die Nutzung der Cloud enorm beschleunigen wird. Bis Ende 2021 werden 80 % der Unternehmen entsprechende Prozesse einrichten, um doppelt so schnell wie vor der Pandemie auf eine Cloud-zentrierte digitale Infrastruktur umzustellen.

Unternehmen, die ihre Cloud- Nutzung erhöhen, ziehen gleichzeitig in Betracht, ihre Security Workloads zu modernisieren und zu optimieren. Bisherige Bedenken zur Realisierung von zentralen Workloads, wie Security Information and Event Management (SIEM) in Public Clouds, wurden durch COVID-19 relativiert. Viele erkennen, dass der Wechsel zu einer Cloud-basierten Sicherheitsarchitektur moderne Funktionen, bessere Skalierbarkeit und wirtschaftliche Vorteile mit sich bringt und somit den Weg zu einem Cloud-zentrierten und für die digitale Transformation notwendigen Geschäftsmodell ebnet. Da immer mehr Anwendungen und Daten in die Cloud verlagert werden, steht die Migration von SIEM-Workloads in die Cloud im Einklang mit übergeordneten Hybrid-Cloud- und modernen Sicherheitsstrategien.

Auf einen Blick

Wenn uns die Pandemie eines gelehrt hat, dann, dass die digitale Transformation (DX) nicht nur eine Priorität, sondern ein *Muss* für die Resilienz, Anpassungsfähigkeit und agile Innovation von Unternehmen ist.

Unternehmen treiben ihre DX-Reise voran. Dafür erhöhen sie ihre Investitionen in die Cloud, die Modernisierung von Security- und Daten-Workloads, die Einführung neuer agiler Entwicklungsmethoden, die Implementierung flexibler oder as-a-Service-Geschäftsmodelle und fokussieren sich auf datengesteuerte Erkenntnisse.

Die Transformation und Migration von Security- und Daten-Workloads, wie von Splunk in die Cloud, erfordert jedoch Expertise in:

- » Cloud- und Workload-Bewertung
- » Transformations- und Migrationsplanung
- » kontinuierlicher Optimierung von Infrastruktur-Ressourcen
- » der Fähigkeit, Innovationen aus Daten zu generieren

Mit gebündelten Splunk- und AWS-Fachkenntnissen unterstützt und begleitet Computacenter seine Kunden auf deren Reise hin zu einem intelligenten, digitalen Unternehmen.

SIEM-Workloads wie Splunk Enterprise Security bilden wichtige Säulen in den Sicherheitsstrategien von Unternehmen, um auf Sicherheitsvorfälle zu reagieren. Damit sind sie das Herzstück eines Security Operations Centers (SOC). Diese Workloads können jedoch komplex, datenintensiv und damit kostspielig werden.

Die Cloud-Flexibilität, hinsichtlich der Preisgestaltung, und -Agilität bietet dabei die Möglichkeit, kritische Security-Workloads zu modernisieren und zu optimieren. Laut der *COVID-19 Impact Survey* von IDC (Wave 5, Mai 2020) planen etwa 58 % der Unternehmen, Security-Workloads in die Cloud zu verlagern.

Für europäische Unternehmen wird eine Infrastrukturalternative immer beliebter – die Ausführung von Splunk auf AWS. Folglich bietet dies die Nutzung von Splunk Cloud, gehostet auf AWS, oder die Ausführung von Splunk Enterprise direkt auf AWS. AWS ist der führende IaaS-Anbieter in Westeuropa mit einem Marktanteil von mehr als 53 % im Jahr 2019 (IDC Public Cloud Tracker, Oktober 2020).

Splunk Workloads sind für viele Unternehmen zu einem geschäftskritischen Service geworden, mit dem sie aus ihren Daten Antworten auf wichtige Geschäftsfragen ableiten und Planungsstrategien erhalten können. Die Transformation und Migration dieser Splunk Workloads kann aufgrund der zusätzlichen Funktionen in der Cloud, wie zum Beispiel Large-Scale-Analysen, einen besseren ROI erzielen. IDCs Multicloud Survey aus dem Jahr 2020 hat ergeben, dass nur 23 % der Migrationen von zentralen Workloads in die Cloud erfolgreich sind. Schlechte Public-Cloud-Konfigurationen, wenn sie eigenständig auf AWS verwaltet werden, Fachkräftemangel, Kostenkontrolle und Leistungsprobleme sind dabei die Hauptgründe, weshalb Cloud-Migrationen scheitern. Um wichtige Security- und Daten-Workloads wie von Splunk erfolgreich in der Public Cloud zu betreiben, sollten Unternehmen in die folgenden Bereiche investieren:

- Cloud- und Workload-Bewertung
- Transformations- und Migrationsplanung
- kontinuierliche Optimierung der On-Premises-Infrastruktur-Ressourcen im Falle hybrider Szenarien unter Verwendung von On-Premises Splunk und Splunk auf AWS
- Nutzung von datengetriebenen Innovationen und neuen Use Cases

Die Rolle eines Technologiepartners wie Computacenter, mit dediziertem Engineering und qualifizierten Fachexperten sowie einer langfristigen Partnerschaft mit Splunk und AWS, kann das Risiko von kostspieligen Fehlern bei einer Splunk-Cloud-Migration erheblich verringern. Mit seinen Integrations-, Re-Engineering-, Support- und Cloud-Migrationsprogrammen kann Computacenter Kunden dabei helfen, SIEM- und Daten-Workloads zu modernisieren, die Cloud besser zu nutzen, Management-Overheads zu eliminieren und fehlendes Fachwissen auszugleichen. Somit können sich Unternehmen auf ihre Kernkompetenzen und digitale Innovationen konzentrieren, um Information-Security-Programme schnell auf- und auszubauen. Auf Basis der Security der nächsten Generation können Unternehmen ihre Datenstrategien vorantreiben, einen transparenten Überblick über vorhandene Daten entwickeln, Echtzeit-Analysen erstellen und Maßnahmen ebenfalls in Echtzeit ergreifen.

Inhalt des Partner Spotlights

Dieses IDC Partner Spotlight analysiert die Trends in der europäischen Unternehmens-IT und der digitalen Transformation. Dabei liegt der Fokus auf der Frage, wie Unternehmen das Beste aus Splunk-Umgebungen herausholen, die Komplexität der IT auflösen und Kosten letztlich besser verwalten können.

Zudem werden Vorteile herausgestellt, die die Modernisierung von Splunk-Workloads auf eine der erfolgreichsten Cloud-Plattformen, AWS, mit sich bringt. Darüber hinaus wird Computacenter als wichtiger Technologiepartner vorgestellt, der die gesamte Klaviatur abdecken kann – von der Splunk-Modernisierung, über die Cloud-Migration, die Cloud-Optimierung und -Automatisierung bis hin zur anschließenden datengesteuerten Transformation. Dieses Partner Spotlight beleuchtet außerdem die Expertise, die Fähigkeiten, die Unterscheidungsmerkmale und die Zusammenarbeit von Computacenter mit Splunk und AWS, um Splunk-Lösungen in AWS zu implementieren und gleichzeitig kontinuierlich zu optimieren.

Situationsüberblick

Die Cloud ist der Motor für Innovationen in Unternehmen. Wir bewegen uns unumgänglich auf eine Ära zu, in der die Cloud-First-Strategie unabdingbar und alltäglich wird. Unternehmen evaluieren die Public Cloud nicht nur für die Entwicklung neuer Cloud-nativer Anwendungen, sondern auch für die Modernisierung von Kern-Workloads wie ERP-Workloads, Datenbanken und SIEM-Workloads, um die Vorteile der Cloud zu nutzen.

41 % der Unternehmen nutzen bereits oder planen die Nutzung der Cloud für SOC-, SVM- und SIEM-Funktionen – so das Ergebnis des European IT Security Survey von IDC, Juni 2020.

Darüber hinaus betreiben laut IDCs *Multicloud Survey* von 2020 nur 14 % der europäischen Unternehmen ihre Workloads ausschließlich vor Ort oder in Colocation, während 86 % in unterschiedlichen Ausprägungen einen Hybrid-Cloud-Ansatz verfolgen. Etwa 14 % dieser Unternehmen richten sich sogar nach einem Public-Cloud-First- oder Public-Cloud-Only-Ansatz.

Die Public Cloud, insbesondere AWS, entwickelt sich für europäische Unternehmen zu einem wichtigen Bestandteil ihrer Cloud-zentrierten Infrastrukturstrategien. Basierend auf Daten des IDC Public Cloud Tracker verzeichnete AWS im Jahr 2019 ein Wachstum von 38 % im IaaS-Markt in Westeuropa und konnte damit weit mehr als die Hälfte des gesamten IaaS-Marktes einnehmen. Im *European Tech and Industry Pulse Survey, 2019-2020* von IDC, nannten die Befragten AWS als einen der Top-5-Anbieter, der die digitale Transformation (DX) ermöglicht.

Es wird deutlich, dass mittlerweile so gut wie alle Workloads – bei entsprechender Optimierung – in der Public Cloud laufen können.

Die *COVID-19 Impact Survey* von IDC ergab, dass 94 % der Unternehmen planen, ihre langfristige IT-Strategie zu ändern. Zu den wichtigsten Änderungen gehören:

- offensiverer Vorstoß in die Cloud

- höhere Investitionen in das Risikomanagement (Disaster Recovery, Security)
- umfassendere Strategie zur Automatisierung

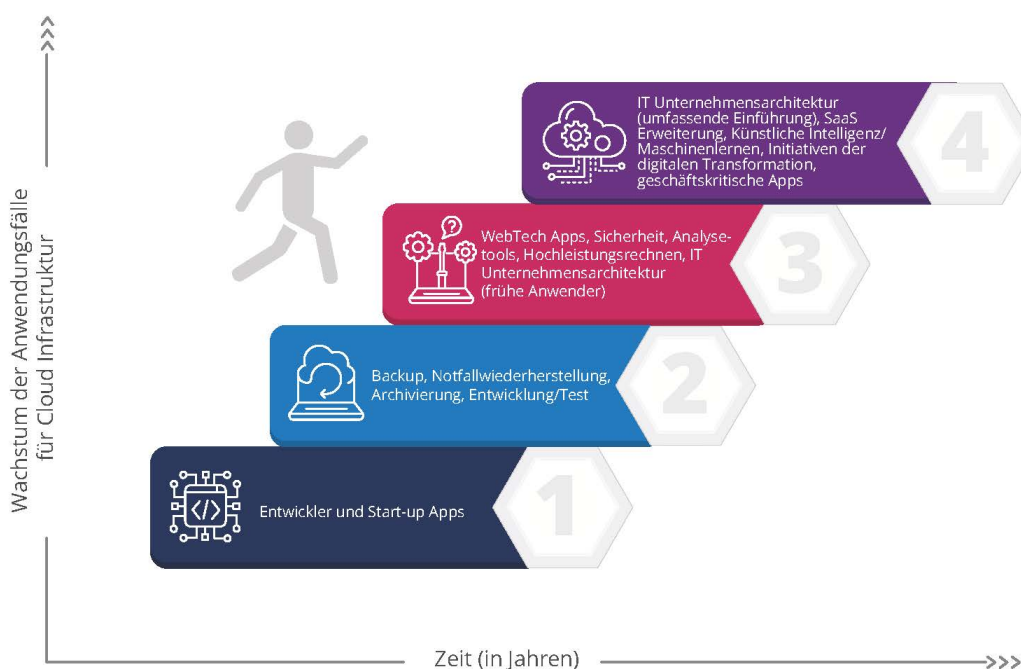
Die Gründe für eine offensivere Cloud-Einführung sind Geschäftskontinuität, Anpassungsfähigkeit, die Entwicklung zu flexiblen Preismodellen und Resilienz.

Splunk SIEM-Workloads sind bereit für die Cloud-Migration

Die Einführung der Cloud ist ein mehrjähriges Vorhaben. Kunden beginnen mit einfach zu migrierenden, weniger kritischen Workloads wie Backup, Archivierung und Disaster Recovery, um von der Effizienz der Cloud zu profitieren und Erfahrungen zu sammeln, um die Cloud für weitere Workloads nutzen zu können (siehe Abbildung 1). Einschätzungen von IDC zufolge werden – neben den Backup- und DR-Workloads – auch Web-Apps, HPC-Workloads, Security- und Analytics-Workloads zur nächsten Welle von Anwendungen gehören, die in die Public Cloud verlagert werden.

ABBILDUNG 1

Die nächsten Workloads, die in die Cloud verlagert werden – Hochleistungsrechnen, Analysetools und Sicherheit



Quelle: IDC, 2021

Die Verbesserung von Sicherheits- und Compliance-Aspekten hat für europäische Unternehmen, die an unserer Multi-Cloud-Befragung teilgenommen haben, oberste Priorität – dies macht die Modernisierung der SIEM-Umgebung unabdingbar. Dabei ist Splunk unter den Top 5 der Marktanteilsinhaber. IDC schätzt, dass der Umsatz von Splunk mit SIEM in Westeuropa im Jahr 2019 um 28,6 % gewachsen ist.

Der Druck auf IT- und Business-Führungskräfte, ihre Cloud-Migrationsstrategien erfolgreich zu gestalten, steigt kontinuierlich. Diejenigen, die bereits in der Cloud sind, stehen ebenfalls unter Druck, ihre Cloud-basierten Workloads stetig zu optimieren.

Doch hinter der Cloud verbirgt sich eine dynamische Infrastruktur mit schnelleren Updates sowie Veränderungen und stellt daher für viele Unternehmen einen Paradigmenwechsel dar. Folglich muss sie kontinuierlich gemanagt und optimiert werden. Dies erfordert, dass Unternehmen ein hohes Maß an Fachwissen aufbauen, um das Beste aus der Cloud herauszuholen. Da die meisten Unternehmen in Multi-Cloud-Umgebungen arbeiten (fast 89 % der von uns befragten europäischen Unternehmen), ist es wenig effizient und praktikabel, ein tiefes und umfangreiches Fachwissen für jede einzelne Cloud zu entwickeln.

An dieser Stelle können Lösungsanbieter wie Computacenter eine entscheidende Rolle spielen.

Da sich Leistung und Kosten in Cloud-Umgebungen im Laufe der Zeit verändern können, ist das Management von Workloads über verschiedene Cloud-Umgebungen hinweg ebenso entscheidend, wie die kontinuierliche Optimierung, wo diese ausgeführt werden. Davon hängt einerseits ab, ob die Applikationen den Erwartungen der Nutzer gerecht werden und andererseits, ob die IT-Abteilung die Kosten im Griff hat. Das Cloud-Betriebsmodell ist ein dynamisches Modell und Unternehmen müssen ihre Angebote regelmäßig mit neuen Preismodellen überprüfen, um den richtigen Weg in die Cloud zu finden.

Überlegungen zur erfolgreichen Migration von Splunk SIEM Workloads auf AWS

Wie Abbildung 2 zeigt, erfordert der erfolgreiche Betrieb moderner Splunk-Lösungen auf AWS einen stufenweisen Ansatz, der Folgendes umfasst:

- Cloud- und Workload-Bewertung
- effektive Transformations- und Migrationsplanung
- kontinuierliche Optimierung von Technologieressourcen und Funktionen in der Cloud
- fortlaufende Fähigkeit, die Data-to-Action-Funktionen von Splunk besser zu nutzen

ABBILDUNG 2

Überlegungen für die erfolgreiche Migration von datenintensiven Workloads in die Cloud



Quelle: IDC, 2021

In jeder dieser Phasen erfolgreich zu sein, kann jedoch in der Praxis schwierig werden. Zu den typischen Herausforderungen für Kunden gehören:

- begrenztes Splunk-Fachwissen und -Expertise
- begrenzte Cloud-Kenntnisse
- fehlende Automatisierung, die für einen reibungslosen Rollout und Upgrades erforderlich ist (nicht erforderlich für Splunk Cloud, da der SaaS Service von Splunk durchgeführt wird)
- Silos in der Kundenorganisation und kulturelle Barrieren
- die Schwierigkeit sowie die Kosten für das Management und für die Gewährleistung einer sicheren Migration großer Datenmengen in die Cloud
- begrenztes Fachwissen zur Optimierung der Umgebung für den Umzug in die Cloud
- Bedenken hinsichtlich Datenhoheit und Datensicherheit

Wie in Abbildung 3 zu sehen ist, gehören zu den Top-5-Gründen, weshalb Cloud-Migrationen in der Praxis scheitern, Fachwissen, Security- und Netzwerk-Fehlkonfigurationen sowie Zuverlässigkeitsprobleme.

ABBILDUNG 3

Weshalb Cloud-Migrationen scheitern



Quelle: IDC's 2020 Annual Multicloud and Next-Generation Infrastructure Survey, n = 613

Infolgedessen entscheiden sich einige Kunden dafür, Unterstützung bei der Migration und für ihren Weg in die Cloud von Splunk oder anderen Partnern anzufordern.

Warum Computacenter?

Computacenter bietet maßgeschneiderte Splunk Enterprise-on-AWS-Services über alle vier Modernisierungsphasen hinweg – und zwar End-to-End für eine durchgängige Security-Transformation.

- **Technologiebeschaffung** – Verstehen und Bewerten der Lizenzbeschaffung von Splunk, der Splunk- und AWS-Infrastrukturservices und Preisoptionen, z. B. für verschiedene Storage-Arten; Umstellung auf ein Cloud-ähnliches, Workload-basiertes Preismodell – im Gegensatz zu historischen Datennutzungsbasierten Angeboten.

- **Architektur des Splunk-Workloads für die Cloud-Optimierung** – Design und Engineering einer modernen Cloud-fähigen Splunk-Umgebung; Neuarchitektur oder Neuformatierung bestehender On-Premises-Splunk-Umgebungen für Splunk Cloud und Splunk Enterprise auf AWS; Sicherstellung, dass das Design der neuen Splunk-Umgebung mit der langfristigen Hybrid-Cloud-Strategie übereinstimmt und alle Compliance-Anforderungen erfüllt.
- **Erfolgreiche Bereitstellung in der Cloud** – Entwerfen des Business Case und der Migrations-Roadmap; Durchführung der Splunk-Migration zu Splunk Cloud oder Splunk Enterprise auf AWS mit minimalen Unterbrechungen und Sicherheitsrisiken, Unterstützung bei der Transformation von Geschäftsprozessen, Kultur und Geschäftsergebnis-Metriken zur Messung des Erfolgs.
- **Sicherstellung eines konsistenten Betriebs, Wartung und Managements** – Optimierung, Integration und inkrementelle Entwicklung der bestehenden Bereitstellung in der Cloud, Bewertung und Nutzung der ergänzenden Funktionen und Services von AWS, um einen Wettbewerbsvorteil aufzubauen.
- **Innovation** – Ausrichten der Splunk-Workload-Modernisierung auf eine breitere Cloud-Einführung, Security der nächsten Generation, Resilienz, Kosteneffizienz, kontinuierliche Effizienz und Cloud-zentrierte digitale Transformation.
- **Datenschutz** – Unterstützung der Kunden beim Verständnis der rechtlichen und technischen Umgebung und bei der Festlegung geeigneter Prozesse und Architekturen, die sowohl die rechtlichen Rahmenbedingungen als auch die Einstellung des Unternehmens zu Risiken und Sicherheit erfüllen, wie z. B. der Entwurf von Datenschutzbewertungen, Richtlinien zur rechtmäßigen Nutzung usw.

Computacenter – Unternehmensprofil

Der globale Technologiepartner Computacenter mit Hauptsitz in UK unterstützt Unternehmen bei der Beschaffung, Transformation und dem Management ihrer IT-Infrastruktur, um digitale Geschäftsergebnisse zu erzielen. Das Portfolio der Technologielösungen von Computacenter umfasst Infrastruktur-Services (Security, Netzwerk, Hybrid Cloud, On-Premises), Lösungen für den digitalen Arbeitsplatz und Produktivität, geschäftsspezifische IT-Lösungen, Managed-IT-Services sowie Support- und Maintenance Services.

Im Rahmen seines AWS- und Splunk-Angebots nutzt Computacenter sein globales Splunk Center of Excellence und seine umfangreichen AWS Professional Services, um Splunk-Implementierungen zu reparieren und zu verbessern. Computacenter ist seit 2016 Splunk-Partner und hat seine Fähigkeiten im Markt mit zahlreichen Splunk-Engineer- und Architect-Zertifizierungen, einer vollständigen Palette des Splunk-Produktportfolios und akkreditierten Consultants für die Bereitstellung von Lösungen im großen Maßstab etabliert. Computacenter zählt außerdem zu den AWS Advanced Consulting Partnern, wodurch Kunden ihre AWS-Reise über vier Fokusbereiche hinweg beschleunigen können: AWS Marketplace Services, AWS Foundation Services, Massenmigration und VMware Cloud on AWS.

Der Technologieanbieter kombiniert seine Splunk- und AWS-Fähigkeiten, um Kunden dabei zu helfen, ihre Splunk-Implementierungen zu optimieren sowie zu vereinfachen und die Workloads

in die Public Cloud zu migrieren. Kunden profitieren von einer verbesserten Skalierbarkeit und Kosteneffizienz der Public Cloud sowie von einer modernen, belastbaren Splunk-Plattform. Mit dieser können sie die digitale Grundlage für ihre Compliance-, moderne Security- und digitale Vertrauensstrategien legen.

Eine AWS-Splunk-Lösung bündelt das Wissen von Computacenter hinsichtlich Beratung, Transformation und Optimierung von Splunk Enterprise Workloads und AWS auf einer einzigen Plattform.

Viele Szenarien – viele Möglichkeiten zur Optimierung

IDC vertritt die Meinung, dass sich das AWS- und Splunk-Know-how von Computacenter hervorragend eignet, um Unternehmen dabei zu unterstützen, ihre Security- und Cloud-Möglichkeiten voll auszuschöpfen – unabhängig davon, wo sich diese auf ihrer Reise in die Cloud gerade befinden. Ein wesentlicher Vorteil einer maßgeschneiderten Lösung liegt in der damit verbundenen Antwort auf zu geringe Kenntnisse rund um Splunk-Workload, Workload-Redesign sowie Cloud-Migration und -Optimierung.

- **Szenario 1:** Kunden, die Splunk On-Premises betreiben. In Gesprächen mit IDC haben Unternehmen, die SIEM-Workloads wie Splunk On-Premises bereits in Betrieb haben, berichtet, dass sie unter Druck stehen, neue Daten zu erhalten, stärker auf Analytics zu setzen und sich auf die Prozessautomatisierung durch Playbooks in Security Operations Centern zu konzentrieren. Indem neben Infrastrukturkosten (z. B. für Storage) und Lizenzkosten der Betriebsaufwand gesenkt wird, erhalten Teams mehr Freiraum, sich auf höherwertige Aufgaben zu konzentrieren. Während On-Premises-Implementierungen die Security-Anforderungen des letzten Jahrzehnts erfüllen, werden sie der dynamischen Skalierung, Flexibilität, Automatisierung und Effizienz moderner dynamischer Cloud-basierter Umgebungen nicht gerecht. On-Premises-Implementierungen schränken Unternehmen zudem in der Fähigkeit ein, enorme Datenmengen schnell zu vereinheitlichen und zu verarbeiten, um Bedrohungen, die vorübergehend mehr Dateneinblicke erfordern, effektiv zu bewerten. Diese Kunden benötigen Services und technischen Support, um erfolgreich in die Cloud zu migrieren und eine umfassende, von der Cloud getriebene Transformation anzustoßen.
- **Szenario 2:** Kunden, die bereits Cloud-Erfahrung haben, aber ihre Workloads optimieren und die Stärken der Cloud besser nutzen müssen. Auch wenn diese Unternehmen die Cloud bereits für sich nutzen, suchen sie nach Beratungsleistungen, wie sich die Splunk-Modernisierung an den Geschäftszielen ausrichten lässt. Gleichzeitig sollen die richtigen Workloads klassifiziert und in die Cloud verlagert werden können, um das Tempo der Cloud zu erreichen.
- **Szenario 3:** Greenfield-Deployment. Diese Kunden möchten Splunk Cloud innerhalb weniger Tage nutzen, um ihre digitale Security- und Incident-Response-Strategie umzusetzen. Für sie ist es ausschlaggebend schnelle Antworten auf ihre dringendsten Security-Fragen zu erhalten, anstatt Wochen damit zu verbringen herauszufinden, welche Module, Lizenzen und Betriebsmodelloptionen für sie am besten geeignet sind.

In allen skizzierten Szenarien profitieren Unternehmen von der Plattform, indem sie Splunk Cloud einsetzen, um Kosten zu reduzieren und die Skalierung zu erhöhen. Die Plattform hilft dabei, eine moderne Splunk-Lösung zu entwerfen, um mehr Use Cases zu bedienen, effizientere Benutzererfahrungen zu ermöglichen und Engpässe bei AWS- oder Splunk-Expertise zu überwinden.

Vorteile der Migration von Splunk Enterprise auf AWS für verschiedene Stakeholder

Derzeit fokussieren sich IT-Abteilungen sehr stark auf die Generierung von Mehrwert für das Business, Kosteneffizienz und Erhöhung des Sicherheitsniveaus, um eine vertrauenswürdige Digitalisierung umzusetzen. Die Frage danach, wie sich die Auswirkungen von Security- und Datenvorfällen minimieren und Compliance und Resilienz sicherstellen lassen, hat für viele Chefetagen oberste Priorität. Darüber hinaus hat Splunk seine ‚Data to Everything‘-Plattform mit neuen Funktionen erweitert, um die Produktivität, Einblicke und Administration für verschiedene Bereiche wie IT-, Security- und DevOps-Teams zu verbessern. Um in der Ära der Intelligenz und Analytik erfolgreich zu sein, sollten Unternehmen diese modernen, Cloud-nahen Funktionen nutzen.

Fest steht: COVID-19 hat den Status quo für bisherige IT-Strategien in Frage gestellt. Die Pandemie bietet den Unternehmen damit die Möglichkeit und den An Schub zugleich, ihre Splunk-Workloads mit Public-Cloud-Funktionen zu modernisieren. Unternehmen, die dies erfolgreich umsetzen, können die Potenziale der digitalen Wirtschaft für sich nutzen und haben so die Chance, sich auch in Zukunft als digitale, vertrauenswürdige Marke zu positionieren. Splunk Enterprise zu modernisieren und diese auf AWS auszuführen, kann für Unternehmen weitreichende geschäftliche Vorteile haben und gleichzeitig die Anforderungen einer Vielzahl von Personen erfüllen. Dazu zählen:

Manager mit Schwerpunkt auf Unternehmens- und Digitalstrategie:

- eine belastbarere und reaktionsfähigere Splunk-Plattform
- die Möglichkeit zur Skalierung von Splunk für den Einsatz in weiteren Bereichen des Unternehmens, um bessere Einblicke und Analysen zu liefern
- Zugang zu komplexeren und aufschlussreicheren Security-Anwendungsfällen, um komplexere Security-Bedrohungen und -Schwachstellen rascher zu erkennen
- Klarheit über die zukünftige Roadmap für Splunk und wie es weitere Einblicke und Daten zur Unterstützung des Geschäftswachstums liefern kann
- Unterstützung der größeren Innovationsagenda und der digitalen Transformationsstrategie mit einer erfolgreichen Cloud-Migration

Betriebsleiter, Security-Verantwortliche und Center of Excellence-Teams:

- Zugang zu Fähigkeiten und Expertise, um die Splunk-Leistung im Blick zu behalten und Alternativen für mehr Effizienz und Leistung zu entwickeln
- Hilfe bei der Erstellung des Business Case zur Unterstützung der Migration
- Hilfe bei der Planung und Verwaltung der Cloud-Migration

- Zugriff auf vorgefertigte Use Cases, die einfach implementiert werden können, um bessere Security-Insights zu erhalten

Technologieexperten:

- profitieren von der Möglichkeit eines kostengünstigeren Betriebs von Splunk
- schnelles Modernisieren und Betreiben von Splunk in viel größerem Umfang
- neue Möglichkeiten, mehr Daten für Analytics und Einblicke zu speichern
- Zugang zu einer widerstandsfähigeren und stabileren Plattform

Für IDC steht fest: Werden datenintensive Workloads wie Splunk in die Cloud verlagert, bringt das eine ganze Reihe an Vorteilen mit sich. Unternehmen können damit ihre Kosten optimieren, unmittelbar auf Echtzeit-Intelligenz zugreifen, das Nutzererlebnis deutlich verbessern, Komplexitäten minimieren sowie standardisierte Architekturen entwickeln. Der vielleicht wichtigste Vorteil besteht darin, dass damit der Weg für eine langfristige Cloud-Migration, höhere Automatisierung und Innovationen im Security-Bereich geebnet ist.

Ausblick und Zukunftsperspektiven

Es besteht kein Zweifel, dass Cloud-Reife und -Erfolg unmittelbar mit dem digitalen Fortschritt verbunden sind.

„Digital Leaders – die Top 25 % der Unternehmen, die am stärksten in fortschrittliche IT-Infrastrukturtechnologien wie Public Cloud, KI, Automatisierung, intelligentes Monitoring usw. investieren – verzeichneten ein größeres Umsatzwachstum im Vergleich zu den sog. Digital Followers, die in Sachen Digitalisierung noch Aufholpotenzial haben. 44 % der Digital Leaders sahen 2019 ein Umsatzwachstum von bis zu 10 % im Vergleich zu 26 % der Digital Followers.“

Der Glaube, dass mindestens 15 % der Public-Cloud-Ausgaben verschwendet werden, wird viele Unternehmen im Jahr 2021 mehr in das Public-Cloud-Kostenmanagement investieren lassen, mit dem Ziel, diese Verschwendung zu halbieren. An dieser Stelle bietet sich wieder ein großer Anknüpfungspunkt für Technologiepartner wie Computacenter, die als integraler Teil ihres Lösungspaketes auch Services zur Kostenoptimierung anbieten.

IDC ist davon überzeugt, dass Unternehmen, die ihre Cloud und ihre Workloads optimieren, sich einen erheblichen Wettbewerbsvorteil verschaffen werden. Dabei lässt sich ein wachsender Trend beobachten, bei dem Unternehmen die vollständige Kontrolle über Daten, Geschäftslogiken und ihre IP behalten wollen, jedoch den täglichen Betrieb, das Management und die Wartung an Technologieanbieter auslagern möchten, um unnötige Managementkosten und Ausfallrisiken zu vermeiden und gleichzeitig die „best-of-breed“ Funktionen zu nutzen.

Lösungsanbieter mit End-to-End-Fähigkeiten, die von der Technologiebeschaffung und -lizenzierung bis hin zur Implementierung und dem kontinuierlichen Support alles abdecken, sind daher gut positioniert, um den Anforderungen der Splunk-Migration gerecht zu werden.

Herausforderungen für Computacenter

Eine der größten Herausforderungen für Technologiepartner, die den Wechsel in die Public Cloud ermöglichen, liegt darin, dass europäische Unternehmen durchaus sehr unterschiedliche Einstellungen und Ansichten gegenüber der Cloud-Thematik vertreten. Die Cloud-Akzeptanz ist in Europa nuanciert, wobei verschiedene Regionen unterschiedliche ‚Anker-Clouds‘ haben – eine primäre Public Cloud, zu der sie in ihrer Multi-Cloud-Strategie tendieren.

Bedenken über die Zukunft des Datenschutzes, europäische Vorschriften wie die DSGVO und Compliance, können sich dabei durchaus als potenzielle Verhinderer entpuppen. Daher sollte Computacenter aufzeigen, wie die Security- und Compliance-Anforderungen der Kunden mit den Lösungen und Services abgedeckt und erfüllt werden können. IDC prognostiziert, dass bis Ende 2021 mehr als 90 % der Unternehmen, die Cloud-Services für datenschutzsensible Workloads evaluieren, die Aufrechterhaltung der Datenhoheit und Datenkontrollfunktionen über geografische Grenzen hinweg fordern werden.

Darüber hinaus werden Hybrid- und Multi-Cloud-Strategien zur Norm – und Technologiepartner wie Computacenter müssen großen Unternehmenskunden damit versichern, dass die Splunk-Workloads so umgestaltet werden können, dass sie ihren hybriden Multi-Cloud-Anforderungen gerecht werden.

IDC ist der Meinung, dass Computacenter seine Expertise über mehrere Plattformen hinweg weiter ausbauen sollte. Darüber hinaus sollte das Splunk-AWS-Solution-Team mit den Teams zusammenarbeiten, die ‚VMware Cloud on AWS‘ oder den Geschäftsbereich On-Premises managen, um eine Einbahnstraße zwischen Public Cloud und On-Premises oder Private Cloud zu verhindern. Zudem sollte für Einfachheit und Transparenz rund um die Vorteile des Betriebs von Splunk Enterprise auf AWS oder auf Splunk Cloud gesorgt werden, um sicherzustellen, dass die Kunden der Public Cloud zugewandt bleiben.

Fazit

Security in einen Wettbewerbsvorteil zu verwandeln und den Aufbau von Digital Trust aktiv voranzutreiben, ist in der heutigen Zeit zur absoluten Notwendigkeit geworden. Um dem Veränderungstempo der digitalen Wirtschaft standzuhalten, müssen Unternehmen sicherstellen, dass ihre SIEM-Workloads wie Splunk-Umgebungen aktuell, modern und effizient sowie im Einklang mit ihren hybriden Multi-Cloud-Strategien sind.

Hinter dem Konzept der Cloud steckt viel mehr als nur eine reine Technologie oder ein Meilenstein, den ein Unternehmen erreichen möchte. Oft wird sie als grundlegend transformierend oder gar als neue Erfahrung für Unternehmen betitelt.

Aufgrund ihrer Manpower und ihrer Bereitschaft groß zu denken, befinden sich AWS und Splunk in einer guten Ausgangslage, um weiterhin Kundenprobleme in ihren jeweiligen Bereichen der digitalen Wirtschaft zu lösen. Technologiepartner wie Computacenter, die dabei helfen, den Fachkräftemangel aufzufangen und Komplexität zu reduzieren, können die entscheidende Schnittstelle zwischen Unternehmen und Anbietern sein.

Inmitten einer Pandemie wird Vertrauen zum strategischen Imperativ. IDC glaubt, dass Digital Trust einer der wichtigsten wirtschaftlichen Treiber der digitalen Transformationsstrategie sein wird. IDC definiert die Zukunft des Vertrauens mithilfe von fünf Kernelementen: Risiko, Security, Compliance, Datenschutz sowie Ethik und soziale Verantwortung (Quelle: *The Future of Trust: Mitigating Risk and Creating Value*, IDC #US46533320, Juni 2020).

Laut IDCs *2020 CEO Survey* sind Initiativen rund um Digital Trust der wichtigste neue Punkt auf der Agenda der nächsten fünf Jahre. Mit den Auswirkungen der globalen Pandemie im Rückspiegel, wird digitales Vertrauen auch in Zukunft ein kritisches Fokusthema bleiben. Bis 2025 werden zwei Drittel der G2000-Vorstände eine formale Vertrauensinitiative fordern, die eine Roadmap zur Verbesserung der Security, des Datenschutzes und der ethischen Haltung eines Unternehmens umsetzen soll.

Ganz gleich, ob Sie CEO, CIO oder in einer anderen Position für die digitale Transformation im Unternehmen tätig sind: Wenn Sie in Ihrer täglichen Arbeit alles daran setzen, die digitale Transformation Ihres Unternehmens voranzutreiben und seine Strukturen und Prozesse erfolgreich für die digitale Zukunft zu rüsten, sollte die Modernisierung der Security-Architektur und die Nutzung der Cloud ganz oben auf Ihrer IT-Agenda stehen.

MITTEILUNG DES SPONSORS

Computacenter ist ein führender, unabhängiger Technologiepartner, dem große Unternehmen sowie öffentliche Auftraggeber vertrauen. Wir beschaffen, transformieren und managen digitale Technologien, die IT-Anwender und deren Geschäft erfolgreich machen.

Wir helfen unseren Kunden dabei, sich und ihre Unternehmenswerte in der digitalen Transformation umfassend zu schützen. Wir haben die Größe und Erfahrung, um umfangreiche Lösungsangebote zu liefern, indem wir sowohl die Breite unseres Serviceangebots als auch unsere weltweiten Kompetenzen nutzen. Aufgrund unseres End-to-End-Portfolios von Workplace Security bis hin zu Cyber Defence, verfügen wir über vertrauensvolle Beziehungen zu hochrangigen Stakeholdern – vom CIO bis hin zu den Anwendern.

Durch unsere jahrzehntelangen Tätigkeiten und Beziehungen verfügen wir über umfassendes Wissen zu den am Markt aktiven Security-Anbietern und deren Lösungen. Dies bedeutet, dass wir immer passgenaue Lösungen anbieten und in großem Umfang liefern können.

Wir haben fundierte Kenntnisse der klassischen Infrastruktur und moderner Cloud-Strategien gleichermaßen und können diese optimal kombinieren und umsetzen. Wir sind bestens positioniert, um die Cloud-Transformation für unsere Kunden zu beschleunigen und die Cloud zu einem sicheren, effizienten und gut vernetzten Ort zu machen.

Über die Analysten

[Archana Venkatraman](#), Associate Research Director, Cloud Data Management, IDC Europe



Archana Venkatramans Hauptforschungsfeld ist die Verwaltung von Cloud-Daten. Sie forscht in verschiedenen Bereichen, darunter Datenschutz, Edge-to-Cloud-Datentrends, Anwendungs- und Datenverfügbarkeit, Compliance, Datenintegration, intelligente Datenverwaltung, DataOps, Datenqualität, sowie Multicloud-Prioritäten und -Trends. Außerdem ist sie Co-Lead der Cloud Practice und leistet einen aktiven Beitrag zu den DevOps und KI Research Practices von IDC Europe.

[Duncan Brown](#), VP of Enterprise Research Europe, IDC



Duncan Brown leitet IDCs European Research für die Themengebiete Software, Services, Cloud, AccAD und KI/IPA und ist für die Research-Teams zu Kanälen und Ökosystemen verantwortlich. Seine Hauptaufgabe besteht darin, im europäischen Research-Team von IDC „Neues“ zu fördern. Der Fokus seiner Arbeit liegt dabei auf Teamentwicklung und Thought Leadership. Darüber hinaus arbeitet er eng mit Vertrieb, Marketing und Consulting zusammen, um das europäische Geschäft von IDC auszubauen.

Über IDC

International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informations- und Verbrauchertechnologie und der Telekommunikation. IDC analysiert und prognostiziert technologische und branchenbezogene Trends und Potenziale und ermöglicht seinen Kunden so eine fundierte Planung ihrer Geschäftsstrategien sowie ihres IT-Einkaufs. Mehr als 1.100 IDC-Analysten in über 110 Ländern liefern globale, regionale und lokale Erkenntnisse zu technologie- und branchenbezogenen Chancen und Trends. Seit 50 Jahren vertrauen Business-Verantwortliche und IT-Führungskräfte bei der Entscheidungsfindung auf IDC. IDC ist ein Geschäftsbereich von IDG, des weltweit führenden Unternehmens in den Bereichen IT-Publikationen, Research sowie Events.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Global Headquarters

5 Speen Street Framingham, MA
01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com

Copyright und Einschränkungen

Jegliche Verwendung von IDC-Daten oder Verweise auf IDC in der Werbung, in Pressemitteilungen oder im Marketingmaterial bedarf der schriftlichen Vorabgenehmigung durch IDC. Wenn Sie eine Genehmigung zur Verwendung dieser Ressourcen wünschen, wenden Sie sich bitte an IDC Custom Solutions (telefonisch unter 508-988-7610 oder per E-Mail an permissions@idc.com). Für die Übersetzung und/oder Lokalisierung dieses Dokuments ist eine weitere Lizenz von IDC erforderlich. Weitere Informationen zu IDC finden Sie unter www.idc.com. Weitere Informationen zu IDC Custom Solutions finden Sie unter http://www.idc.com/prodserv/custom_solutions/index.jsp.

Copyright 2021 IDC. Die Vervielfältigung ohne Genehmigung ist verboten. Alle Rechte vorbehalten.