

# Splunk® Cloud™

Die branchenweit führende SaaS-Plattform für Operational Intelligence

## BESONDERE MERKMALE

- **Schnell:** Schneller Testbeginn mit [Splunk Cloud Trial](#). Schnelle Umwandlung von Test- in Produktivsystem.
- **Sicher:** Erfolgreiche Auditprüfung nach SOC2 Type 2\*. Dedizierte Cloud-Umgebung für jeden Kunden.
- **Zuverlässig:** SLA mit 100% Betriebszeit Alle Funktionen von Splunk Enterprise einschließlich Apps, APIs, SDKs. Skalierbar auf über 10 TB pro Tag
- **Hybrid:** Zentrale Transparenz über Splunk Cloud- (SaaS) und Splunk Enterprise-Verteilungen (Software)

## Splunk Cloud – Übersicht

**Splunk Cloud liefert Operational Intelligence als Cloud-Service.** Sie können damit die wertvollen Maschinendaten, die von der Technologieinfrastruktur Ihres Unternehmens erzeugt werden, leicht und schnell analysieren und profitieren gleichzeitig von den Vorteilen des SaaS-Konzepts (Software as a Service).

Maschinendaten sind einer der am schnellsten wachsenden, komplexesten und wertvollsten Bereiche von Big Data. Die von IT-Systemen, Anwendungen, technischen Geräten, Sensoren usw. erzeugten Maschinendaten umfassen kategorische Aufzeichnungen zu Benutzertransaktionen, Kundenaktivitäten, Systemverhalten, Sicherheitsbedrohungen und Vielem mehr.

Mit Splunk Cloud können Sie Ihre sämtlichen Echtzeit- oder historischen Maschinendaten durchsuchen, überwachen, in Berichten darstellen und analysieren. Lösen Sie Probleme, untersuchen Sie Sicherheitsvorfälle und überwachen Sie Ihre End-to-End-Infrastruktur, um Dienstbeeinträchtigungen oder -ausfälle zu vermeiden. Verschaffen Sie sich Echtzeittransparenz und kritische Einblicke in Kundenerlebnis, Kundentransaktionen und andere unternehmerische Schlüsselmetriken. Splunk Cloud wird als Cloud-Dienst angeboten und macht Ihre Maschinendaten besser verfügbar, besser verwertbar und wertvoller für das gesamte Unternehmen.

Legen Sie gleich mit der kostenlosen [Splunk Cloud Trial](#) los und sorgen Sie für zentrale Einblicke aus der gesamten Technologieinfrastruktur Ihres Unternehmens, ob physisch, virtuell oder in der Cloud.

## Dienst auf Unternehmensniveau

**Ausgelegt auf Betriebszeit und Performance:** Splunk Cloud ist auf 100 Prozent Betriebszeit und zuverlässige Performance ausgelegt. Jeder Kunde wird als dedizierte Cloud-Umgebung angelegt, um sicherzustellen, dass die Performance nicht durch die Aktionen anderer Kunden beeinträchtigt wird. Darüber hinaus nutzt Splunk Cloud Clustering und Datenreplikation, um die Betriebszeit und Verfügbarkeit sicherzustellen. Dies wird durch unser SLA mit 100% Betriebszeit garantiert.

**Skalierbarkeit und Flexibilität:** Splunk Cloud bietet Flexibilität durch bis zu 10-faches Bursting bei unerwarteten Anstiegen des Datenvolumens und lässt sich auf über 10 TB/Tag skalieren.

**Robuste Sicherheit:** Durch dedizierte Cloud-Umgebungen für jeden Kunden stellt Splunk Cloud sicher, dass Ihre Daten niemals mit Daten anderer Kunden vermischt werden. Zudem bietet Splunk Cloud rollenbasierte Zugriffssteuerung, Überprüfbarkeit und Datenverschlüsselung bei Übertragung und Speicherung. Splunk Cloud hat Auditprüfungen nach SOC2 Type 1 und SOC2 Type 2\* bestanden. Weitere Informationen finden Sie in unserer technischen Beschreibung: [Schutz von Kundendaten in Splunk Cloud](#).

## Umfassende SaaS-Plattform für Operational Intelligence

**Alle Funktionen von Splunk Enterprise PLUS alle Vorteile von SaaS:** Splunk Cloud bietet den gesamten Funktionsumfang der preisgekrönten Splunk Enterprise-Plattform und gibt Zugriff auf Splunk-Apps wie die Splunk App für Enterprise Security.

**Hybride Suche:** Splunk Cloud bietet zentrale Sichtbarkeit über Splunk Enterprise- und Splunk Cloud-Verteilungen hinweg, sodass Kunden entsprechend ihren Geschäftsanforderungen Splunk als Software oder SaaS verteilen können, ohne auf die zentrale Transparenz verzichten zu müssen.

**Sammeln und Indizieren beliebiger Maschinendaten:** Sie können damit beliebige Maschinendaten aus praktisch jeder Datenquelle, in jedem Format und von jedem Speicherort in Echtzeit sammeln und indizieren. Dazu gehört das Datenstreaming aus Standard- und angepassten Anwendungen, App-Servern, Webservern, Datenbanken, Netzwerken, Übertragungsdaten aus Netzwerken, Virtual Machines, Telekommunikationsgeräten, Betriebssystemen, Sensoren und Vielem mehr. Sie müssen die Daten dazu noch nicht einmal verstehen. Senden Sie Ihre Daten einfach an Splunk Cloud und der Dienst beginnt sofort mit dem Sammeln und Indizieren, sodass Sie gleich mit der Datensuche und -analyse loslegen können. Beheben Sie Fehler in Anwendungen, untersuchen Sie Sicherheitsvorfälle, überwachen Sie Netzwerke und Performance, stellen Sie die Compliance sicher und analysieren Sie neue Produkte und Dienste.

**Suchen und Untersuchen:** Ganz egal, ob Sie für Betrieb, Sicherung und Auditing von IT, Anwendungsentwicklung oder Bereitstellung von Unternehmensanalysen zuständig sind – die Suchfunktion ist in jedem Fall der Ausgangspunkt für die Erschließung unzähliger neuer Möglichkeiten aus Ihren Daten. Die in Splunk Cloud enthaltene,

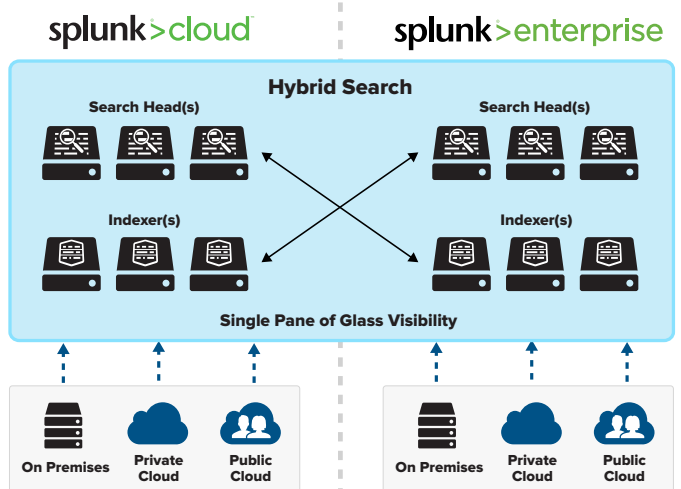


Abbildung 1: Die hybride Suche ermöglicht zentrale Sichtbarkeit.

leistungsfähige Suchsprache (SPL™) ist einfach genug für Anfänger und gleichzeitig leistungsfähig genug für erfahrene Analysten. Gewinnen Sie durch die Interaktion mit Ihren Daten aussagekräftige neue Einblicke. Sie können entlang einer Zeitachse mehr oder weniger Details anzeigen, um Trends, Spitzen und Anomalien zu erkennen. Führen Sie ein Drilldown auf Ihre Ergebnisse durch und entfernen Sie störende Daten, um zur so genannten Nadel im Heuhaufen zu gelangen; korrelieren, analysieren und reagieren Sie auf Echtzeitergebnisse. Verwenden Sie spezifische Begriffe oder Ausdrücke, Boolesche Operatoren und leistungsfähige Statistik- und Reporting-Befehle.

**Hinzufügen von Feldern:** Splunk Cloud extrahiert beim Suchen automatisch Informationen aus Ihren Maschinendaten, sodass Sie sofort mit der Nutzung neuer Datenquellen beginnen können. Sie können Ihre Maschinendaten in Kontext setzen und noch aussagekräftiger machen, indem Sie Felder und Datenpunkte identifizieren, benennen und mit Tags versehen. Sie haben sogar die Möglichkeit, Informationen aus externen Inventarverwaltungsdatenbanken, Konfigurationsmanagementsystemen und Benutzerverzeichnissen hinzuzufügen, und das System damit noch wertvoller für die Benutzer zu machen.

**Überwachen und Benachrichtigen:** Sie können Suchvorgänge in Echtzeitbenachrichtigungen umwandeln, um Schwellenwertbedingungen rund um die Uhr zu überwachen. Legen Sie fest, dass bei der Erfüllung einer Bedingung automatisch Aktionen ausgelöst werden, also beispielsweise E-Mails gesendet, Skripte mit Korrekturmaßnahmen ausgeführt oder Beiträge an RSS-Feeds übermittelt werden sollen. Sie können für Benachrichtigungen eine beliebige Granularitätsstufe festlegen und sie von verschiedenen Schwellenwerten, trendbasierten Bedingungen und komplexen Mustern wie etwa abgebrochene Einkaufsvorgänge, Brute Force-Angriffe und Betrugsszenarien abhängig machen.

**Berichten und Analysieren:** Erstellen Sie im Handumdrehen anspruchsvolle Diagramme, Grafiken und Dashboards, die wichtige Trends, Hochs und Tiefs, Zusammenfassungen von Top-Werten und Häufigkeit des Auftretens zeigen. Erstellen Sie ganz neue, stabile und aussagekräftige Berichte, ohne die Suchsprache lernen zu müssen. Führen Sie von einem beliebigen Punkt in einem Diagramm ein Drilldown zu den zugrunde liegenden Ereignissen durch. Speichern Sie Berichte, integrieren Sie sie in Dashboards und zeigen Sie sie auf Ihrem Desktop-Computer oder auf dem Mobilgerät an. Erstellen Sie in regelmäßigen Intervallen PDF-Dokumente für die Verteilung an Führungskräfte, Business-Benutzer oder andere IT-Entscheidungssträger.

**Benutzerdefinierte Dashboards und Ansichten:** Fassen Sie mehrere Ansichten ganz einfach mit dem Dashboard-Editor in interaktiven Dashboards zusammen. Dashboards können mehrere Diagramme und Ansichten Ihrer Echtzeitdaten beinhalten und so an die Bedürfnisse verschiedener Benutzer angepasst werden, z. B. für Führungskräfte, Business- oder Sicherheitsanalysten, Auditoren, Entwickler und Systemadministratoren. Benutzer können Dashboards mit einer einfachen Drag & Drop-Oberfläche bearbeiten und die Diagrammtypen ad-hoc anhand von integrierten Diagrammsteuerelementen ändern.

**Splunk-Apps:** Splunk Cloud unterstützt Splunk-Apps und andere Inhalte. Splunk-Apps bieten ein gezielt zugeschnittenes Benutzererlebnis für unterschiedliche Rollen, Anwendungsfälle und Unternehmenstechnologien. Diese Apps können Ihnen helfen, neue Möglichkeiten für die Visualisierung von Daten zu finden, und stellen vordefinierte Ansichten mit führenden Technologien wie Linux, Windows, VMware etc. bereit.

**Umfassende Entwicklungsumgebung:** Geben Sie Entwicklern die Möglichkeit, Daten und Funktionalität aus Splunk Cloud in Anwendungen innerhalb des gesamten Unternehmens zu integrieren. Dazu werden SDKs (Software Development Kits) für Java, JavaScript, C#, Python, PHP und Ruby zur Verfügung gestellt.

\* SOC2 Type 2 Auditprüfung bestanden für Splunk Cloud Kundenumgebungen für Datenvolumina über 50GB/Tag

## Kundenerfolge mit Splunk Cloud

**FINRA**, die größte unabhängige Regulierungsbehörde für Wertpapierhäuser in den USA, verwendet Splunk Cloud dazu, Sicherheit und Compliance sicherzustellen. Darüber hinaus setzt die FINRA Splunk Cloud mit der Splunk App for AWS ein.



"Splunk Cloud bietet Ihnen Anwendungen, mit denen Sie riesigen Nutzen aus Ihren Daten ziehen können."

**MindTouch**, ein führender Anbieter für cloud-basierte Customer Success-Software, nutzt Splunk Cloud für Echtzeittransparenz und -analysen innerhalb des gesamten Unternehmens. MindTouch setzt Splunk Cloud für das Echtzeit-Monitoring seiner cloud-basierten Software ein und stellt seinen Kunden wertvolle Geschäftsanalysen zur Verfügung, die zu mehr Kundenzufriedenheit, proaktiver Problembefehung und effizienteren Geschäftsprozessen führen.



"MindTouch hat mehrere Dienste für die Maschinendatenanalyse ausprobiert und außer Splunk Cloud erfüllte keiner die hohen Anforderungen des Unternehmens", erklärte Aaron Fulkerson, Gründer und CEO von MindTouch. "Unsere Produkte sind unternehmenskritisch für unsere Kunden. Da Splunk Cloud 100% Betriebszeit sicherstellt, können wir leichter die Erwartungen unserer Kunden erfüllen, durchgängig online zu sein. Dank Splunk Cloud können wir zuverlässige 24x7-Verfügbarkeit bieten."

**Backupify**, der führende Anbieter von Cloud-to-Cloud-Backupsoftware, nutzt Splunk Cloud für die Ereigniskorrelation über völlig verschiedene Datenquellen hinweg und das Monitoring seiner Produktivsysteme. Mit Splunk Cloud konnte Backupify die Zeit vom ersten Verkaufskontakt bis zum Produktivstart ganz ohne operativen Aufwand auf weniger als eine Woche verkürzen.



"Splunk Cloud ersparte uns Monate an Entwicklungsarbeit", sagte Eugene Gorelik, Director of DevOps bei Backupify. "Darüber hinaus konnten wir die Fehlerbehebungszeit bei Produktivsystemen um ca. 60-70 Prozent senken."

### Gleich loslegen

Die Gebühren für Splunk Cloud basieren auf Jahresabonnements, die für Datenvolumen bis mehr als 10 TB/Tag angeboten werden. Sie können gleich loslegen. Tragen Sie sich hier für das [Splunk Cloud Trial](#) ein oder kontaktieren Sie uns per Email an [dach\\_sales@splunk.com](mailto:dach_sales@splunk.com).