Splunk

Softwarehersteller · Web: splunk.com

Über den Anbieter

Splunk ist ein Softwarehersteller für Datenplattformen im Bereich Security und Observability. Das Unternehmen bietet Lösungen zur Echtzeit-Analyse großer Datenmengen, zur Bedrohungserkennung und zur IT-Infrastrukturüberwachung. Die Plattform ermöglicht es Organisationen, Daten in konkrete Geschäftsergebnisse umzuwandeln und die digitale Resilienz zu erhöhen. Splunk wurde 2024 von Cisco übernommen und ist bekannt für seine SIEM-, Observability- und AIOps-Lösungen, die sowohl cloud-basiert als auch on-premise verfügbar sind.

Schwerpunkte & Spezialisierung

Splunk spezialisiert sich auf die Kombination von Security Operations (SIEM, SOAR, UEBA) und IT Observability (Monitoring, APM, Digital Experience Analytics) auf einer einheitlichen Datenplattform. Besonderheit ist die Integration von KI und agentengestützten Operationen (Agentic Operations und Agentic SOC) zur Automatisierung und intelligenten Analyse.

Stammdaten

Anbieter-Typ	Softwarehersteller
Mutterkonzern	Cisco
Weitere Länder	USA, Vereinigtes Königreich, Australien, Japan, Südkorea, China
Website	splunk.com

Leistungen

Cybersecurity · Daten & Analytics · IT-Infrastruktur · Künstliche Intelligenz (KI)
Security Information and Event Management (SIEM), Security Orchestration (SOAR), Managed Detection & Response (MDR), Security Operations Center (SOC), Threat Intelligence, Incident Response, Monitoring, Big Data, Echtzeit-Analytics (Streaming), Dashboarding, Data Engineering, Anomalieerkennung, Predictive Analytics, Machine Learning

Eigenschaften

BETRIEB & SUPPORT

Cloud / SaaS	**ja**
On-Premise möglich	**ja**
Managed Service	k. A.
24/7-Support	k. A.
Deutschsprachiger Support	k. A.

DATENSCHUTZ & HOSTING

Serverstandort Deutschland	k. A.
Serverstandort EU	k. A.
DSGVO-konform / EU-Standardvertrag	k. A.

Auftragsverarbeitung (AVV)	k. A.

ZERTIFIZIERUNGEN & QUALIFIZIERUNGEN

ISO 27001	k. A.
BSI IT-Grundschutz	k. A.
BSI C5-Testat	k. A.
TISAX	k. A.
BSI APT-Response-Dienstleister (qualifiziert)	k. A.
ISO 27017 (Cloud-Sicherheit)	k. A.
ISO 27018 (Cloud-Datenschutz)	k. A.
ISO 27701 (Datenschutz / PIMS)	k. A.
ISO 9001 (Qualitätsmanagement)	k. A.
ISO 20000-1 (IT-Service-Management)	k. A.
ISO 22301 (Notfallmanagement / BCM)	k. A.
SOC 2 (Type II)	k. A.
IDW PS 951 (Typ 2)	k. A.
CISIS12	k. A.
VdS 10000	k. A.
KRITIS-Nachweis (§ 8a BSIG)	k. A.

Branchen

Finanzwesen / Banken / Versicherungen, Gesundheitswesen / Kliniken, Industrie & Fertigung, Telekommunikation & Medien, Verteidigung & öffentliche Sicherheit, Öffentliche Verwaltung / Behörden, Energie- & Wasserversorgung (KRITIS), Bildung / Hochschulen / Forschung

Typische Use-Cases

- Zentrale Überwachung von IT-Infrastruktur und Diensten zur Früherkennung von Ausfällen
- Automatisierte Sicherheitsanalysen und Incident Response in Echtzeit zur Bedrohungserkennung
- Konsolidierte Datenanalyse aus heterogenen Systemen für bessere Geschäftsentscheidungen
- Monitoring von Anwendungsperformance und Endnutzererfahrung in Cloud- und On-Premises-Umgebungen
- Compliance-Reporting und Audit-Trail-Verwaltung für regulatorische Anforderungen
- Kostenkontrolle durch Optimierung von Datenmengen und Speicherverbrauch im Monitoring
- Anomalieerkennung bei Benutzer- und Entitaetsverhalten für Sicherheitsanalysen
- Debuggen von Microservices-Problemen durch korrelierte Log- und Metrik-Daten

Häufige Fragen

Welche Splunk-Produkte sind für öffentliche Auftraggeber verfügbar?
Splunk bietet Splunk Cloud Platform (SaaS) und Splunk Enterprise (On-Premise) an. Beide können für SIEM, Observability und IT-Service-Management eingesetzt werden. Die Produktauswahl richtet sich nach den spezifischen Anforderungen des Auftraggebers (Sicherheit, Monitoring, Compliance).

Welche Bereitstellungsmodelle unterstützt Splunk?
Splunk stellt seine Plattform in drei Modellen bereit: Cloud-basiert (Splunk Cloud), On-Premise (Splunk Enterprise) und Hybrid-Lösungen. Die Preismodelle sind flexibel und können an die Datenmengen und genutzten Services

angepasst werden.

Ist Splunk DSGVO-konform und für deutsche Behörden zertifiziert?
Splunk wird von Cisco betrieben. Zu konkreten Zertifizierungen (BSI C5, TISAX, deutschlandweit gehostete Infrastruktur) liegen keine öffentlich dokumentierten Nachweise vor. Anforderungen zur DSGVO-Konformität und Datenverarbeitung sollten mit dem Anbieter spezifisch geklärt werden.

Welche Use Cases werden für öffentliche Auftraggeber unterstützt?
Splunk adressiert Sicherheitsüberwachung (SIEM, Threat Detection), IT-Betrieb (IT Service Health, Monitoring), Compliance-Anforderungen und Notfallmanagement. Der Einsatz ist dokumentiert in Krankenkassen, Energieversorger und weitere kritische Infrastrukturen.

Bietet Splunk Schulung und Zertifizierung an?
Splunk bietet Training und Zertifizierungsprogramme (Training and Certification) sowie Dokumentation, Produkttouren und die Splunk-Community zur Wissensvermittlung an.