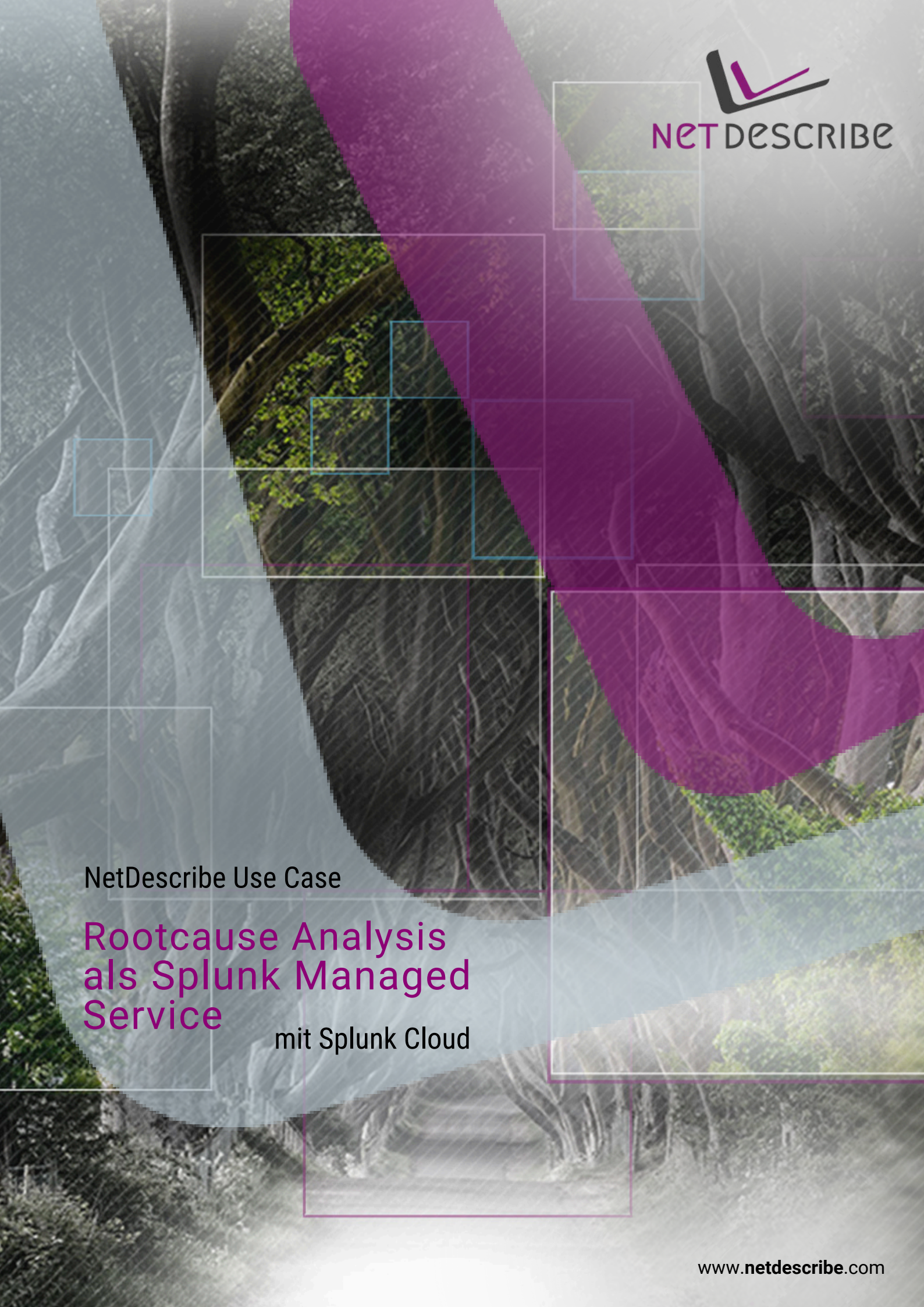


NetDescribe Use Case

Rootcause Analysis als Splunk Managed Service

mit Splunk Cloud

www.**netdescribe**.com

1. Die Ausgangssituation

Beginnen wir mit einem Kundenzitat aus dem ersten Termin: “Unsere Anwender beschweren sich, dass SAP an verschiedenen Standorten so langsam ist. Wir können die Ursache nicht finden und wollen deshalb die Client-Daten analysieren. Kann Splunk das Problem lösen und können Sie uns langfristig bei der Umsetzung des Projekts unterstützen?”

Diese oder ähnliche Fragen haben Sie sich möglicherweise auch schon gestellt.

Sporadisch auftretende Probleme mit der Performance im Netzwerk machen die Mitarbeiter:innen unzufrieden. Eine richtige Fehlerbeschreibung gibt es nicht und alle Untersuchungen laufen ins Leere bzw. ergeben, dass es “eigentlich funktionieren sollte”.

Jedes System für sich: Server, Router, Laptops, Wireless-Komponenten, Applikation und Datenbank sehen super aus - “Alles auf Grün!” Und trotzdem rufen die Anwender an und melden Fehler, lange Antwortzeiten und Ausfälle.

Wie kann zielgerichtetes Troubleshooting Fehlerquellen erkennen und die User Experience steigern?

In den meisten Fällen, fehlt eine übergreifende Analyse und Auswertung der gesammelten Daten über alle im Unternehmen eingesetzten Systeme.

Der Schlüssel: Rootcause Analysis als Splunk Managed Service auf höchstem Niveau!

Die Rootcause Analysis beinhaltet die Erfassung von Fehlern, bewertet diese Daten übergreifend und analysiert deren Ursprung. Daraus leiten sich nicht nur Maßnahmen zur Fehlerreduzierung, sondern auch eine Kostenreduktion ab.

Das sollte Ihnen ein Datenplattform-Service* bieten:

Machine Learning und KI
Vorhersagen und verhindern, anstatt nur zu reagieren! Mit Datenauswertungen in Maschinengeschwindigkeit verbessern Sie sowohl die Sicherheit als auch Ihre Geschäftsergebnisse.

Daten-Streaming
Mithilfe von Stream-Processing in Echtzeit können Sie Daten in Millisekunden erfassen, verarbeiten und an Splunk und andere Ziele verteilen.

Skalierbarer Index
Ihre Daten erfassen und sammeln Sie in Terabyte-Größenordnung aus Tausenden von Quellen – Tendenz steigend.

Collaboration-Tools
Funktionen für Mobile, TV und Augmented Reality sorgen für standortunabhängige Interaktion und Zusammenarbeit.

Föderierte Suche
Unternehmensweite Datenanalyse durch Suchläufe mit korrelierten Resultaten, die Ihr gesamtes Daten-Ökosystem erfassen (lokale und Drittanbieter-Speicher eingeschlossen).

Aussagekräftige Dashboards
Mit eigenen Dashboards, die Sie einfach und intuitiv einrichten, können Sie selbst komplexeste Daten-Storys anschaulich kommunizieren.

*Quelle: splunk.com

2. Der Use Case

Unser Kunde, ein Unternehmen aus Deutschland, stellt innovative Technologien auf Polyurethan-Basis her. Über 300 Mitarbeiter sind auf maßgefertigte Systeme spezialisiert und seit vielen Jahren auf dem europäischen Markt tätig.

Vor kurzem fand eine Umfirmierung statt, bei der die gesamte Infrastruktur neu aufgelegt und in Richtung Cloud und Services entwickelt wurde. Um diese neuen Strukturen zu managen, wurde das NetDescribe S@ND Team eingebunden.

Im Verlauf der Gespräche mit dem Kunden wurde klar, dass alle Versuche, die Performance Probleme zu analysieren gescheitert sind.
Die IT-Abteilung hat Server, Router, Wireless-Komponenten, Applikation und Datenbanken überprüft und keine Fehlerquelle gefunden.
Jedes einzelne System zeigt an, dass alles OK ist.

Da es kein zentrales Überwachungssystem gab, kam es bei der Problemsuche immer wieder zu Verzögerungen.

Die Lösung von NetDescribe

Durchsuchen, analysieren und visualisieren Sie Ihre Daten mit der Splunk Cloud Platform und ergreifen Sie auf dieser Grundlage die richtigen Maßnahmen. Dank der gezielten Verwendung einer Premium App aus der Splunkbase und den Consulting Services von NetDescribe konnte das Problem für den Kunden erfolgreich gelöst werden.

Für die Weiterführung des Projekts wurde der Betrieb und die Entwicklung der Use Cases an das NetDescribe Managed Services Team S@ND outgesourced.

3. Die Umsetzung

Nach einer überzeugenden Splunk Operational-Information-Demo folgte der PoC, der bewusst in der Splunk Cloud durchgeführt wurde. Dieser brachte deutlich mehr Visibilität, zeigte allerdings noch nicht den gewünschten Erfolg.

Erst die Auswahl und Ergänzung einer passgenauen Premium App aus der Splunkbase führte schließlich zur Lösung.
In Teilen des Gebäudes gab es eine nur mangelhafte Abdeckung des WLAN-Signals. Dies konnte letztendlich nur durch die Auswertung der Client Daten nachvollzogen werden.

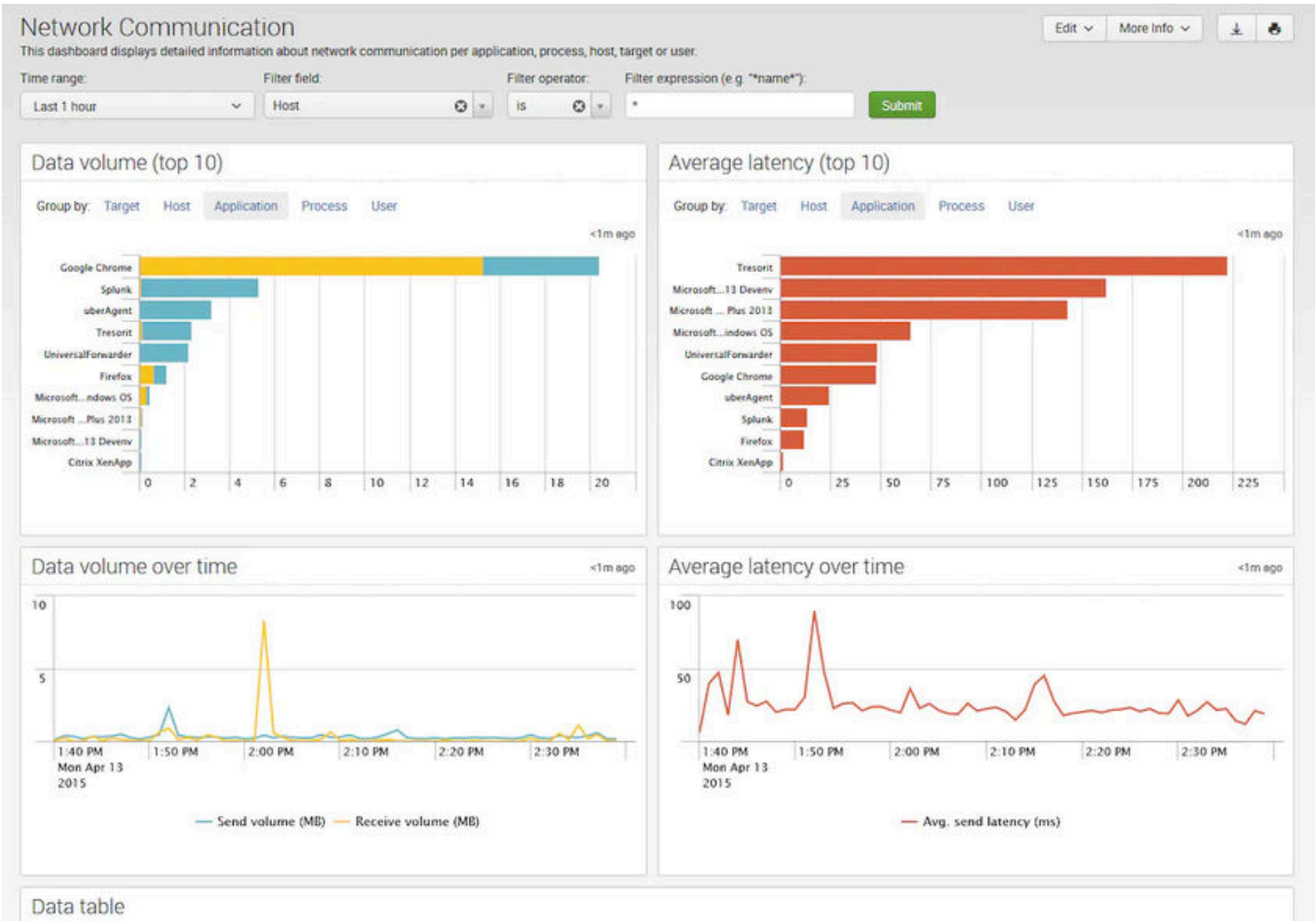
Eine vom Kunden selbst entwickelte Applikation erzeugte ungewöhnlich viele “Reconnects” auf den Clients. Dieser Fehler wurde erkannt, da mit Splunk zum ersten Mal eine historische Analyse der Daten möglich war. Die Ursache konnte problemlos beseitigt werden.
Im nächsten Schritt wurde Splunk Cloud durch die Experten von NetDescribe implementiert.

Nach dem initialen “Quick Win” reduzierten sich die Anrufe der Anwender maßgeblich.
Bei der Übernahme durch das S@ND Team wurde gemeinsam mit dem Kunden entschieden, weitere sicherheitsrelevante Daten (Firewall-Logs, Windows Event Logs, AWS-Logs) in Splunk Cloud zu indizieren und auszuwerten.

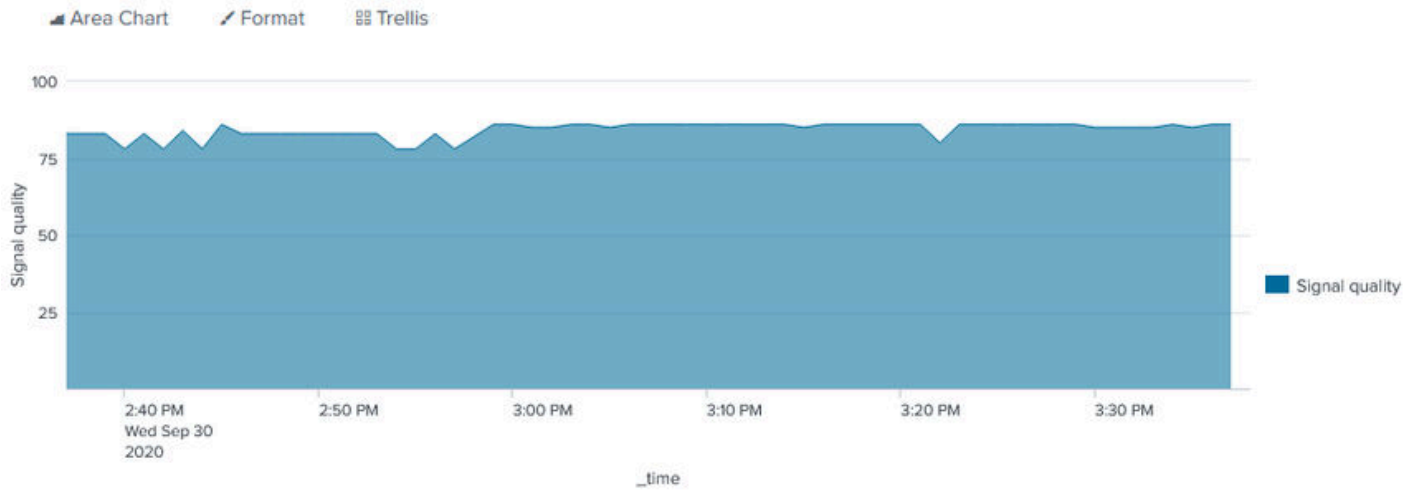
Das Ergebnis: Binnen sechs Monaten vervierfachte sich das Volumen der mit Splunk analysierten Daten und ergab ein umfassendes Bild über die eingesetzten Systeme.

Fazit: Zur vollsten Zufriedenheit des Kunden können Fehlerquellen jederzeit schnell identifiziert und eliminiert werden.
Zusätzlich wird das IT-Team des Kunden durch die S@ND Services erheblich entlastet.

Zentrale Ansichten über alle Anwender*

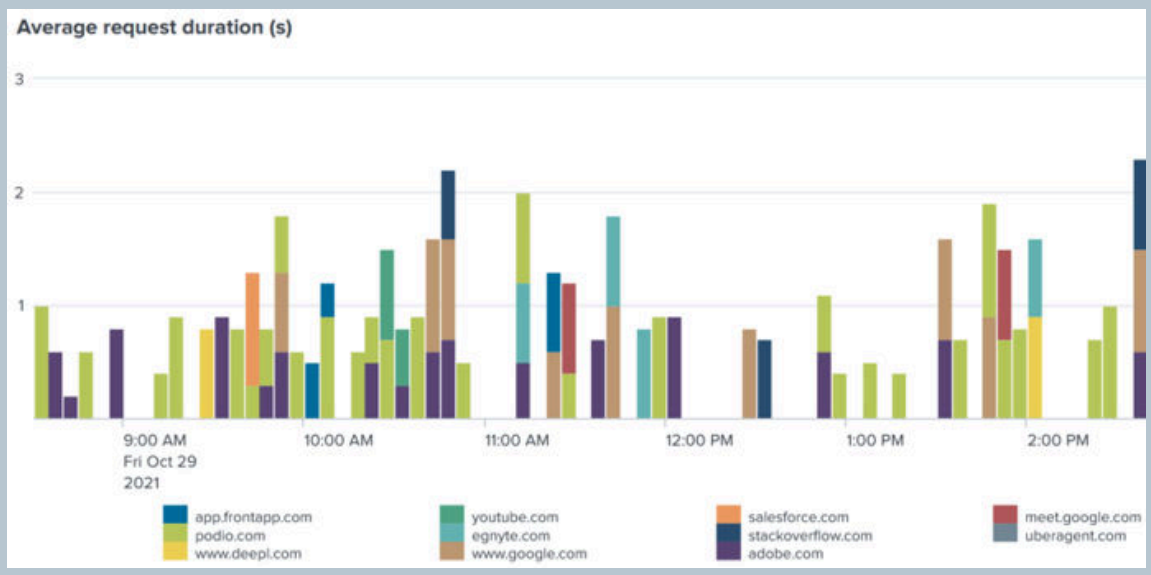


Timechart: WLAN Signalqualität von einem Anwender*

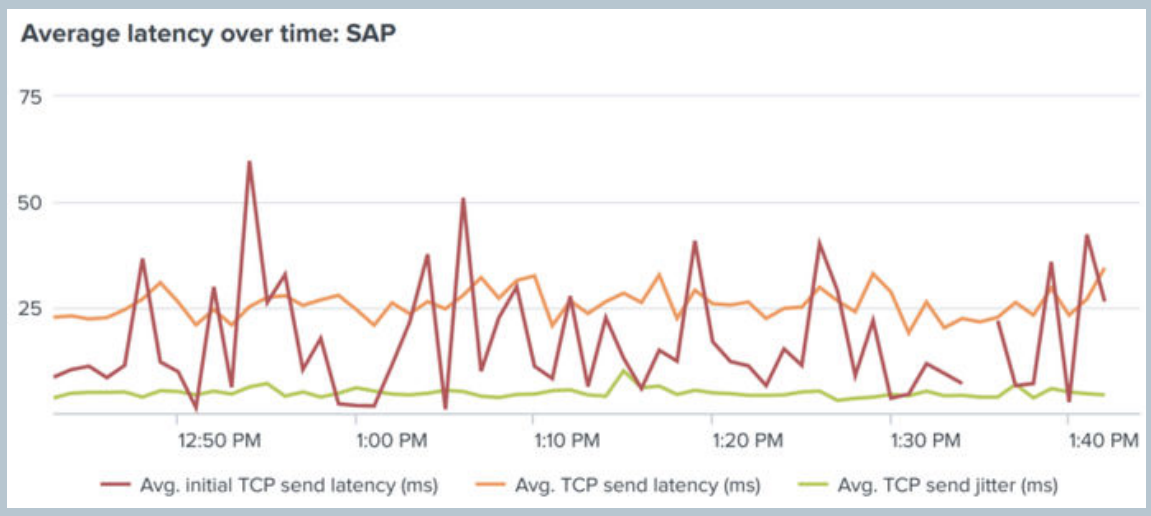


*Quelle: Splunk

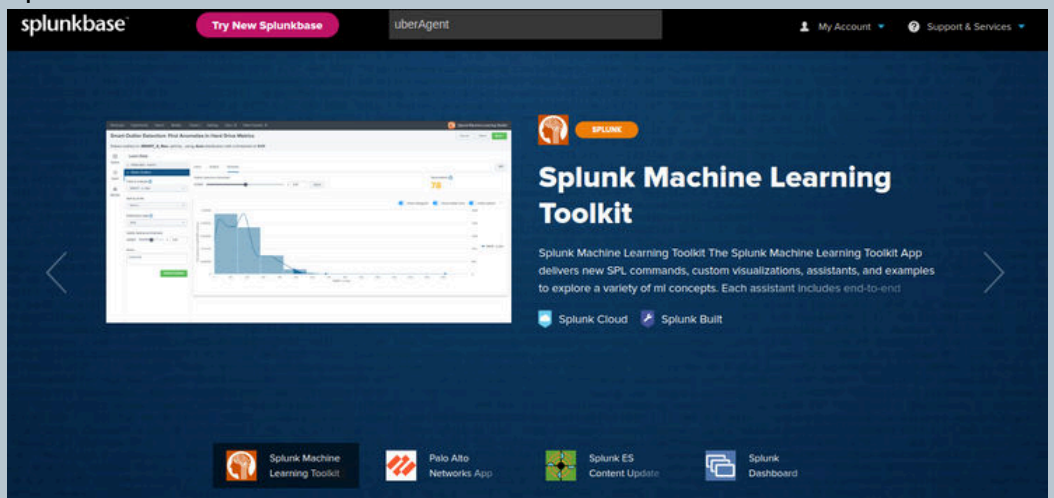
Durchschnittliche Dauer der Anfrage*



Durchschnittliche Latenzzeit*



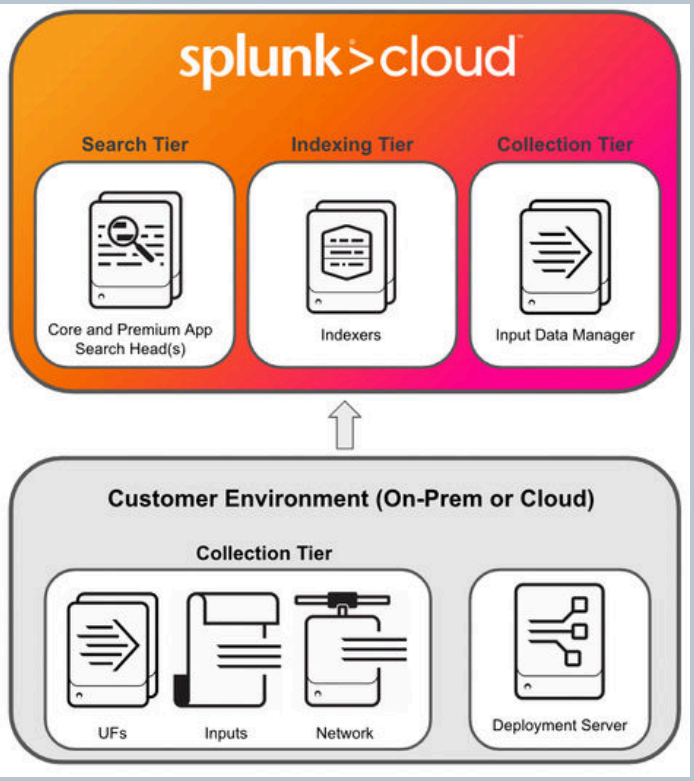
Splunkbase*



Die Splunk Machine Learning Toolkit App liefert neue SPL-Befehle, benutzerdefinierte Visualisierungen, Assistenten und Beispiele, um eine Vielzahl von Machine Learning-Konzepten zu erkunden.

*Quelle: Splunk

Splunk Cloud*



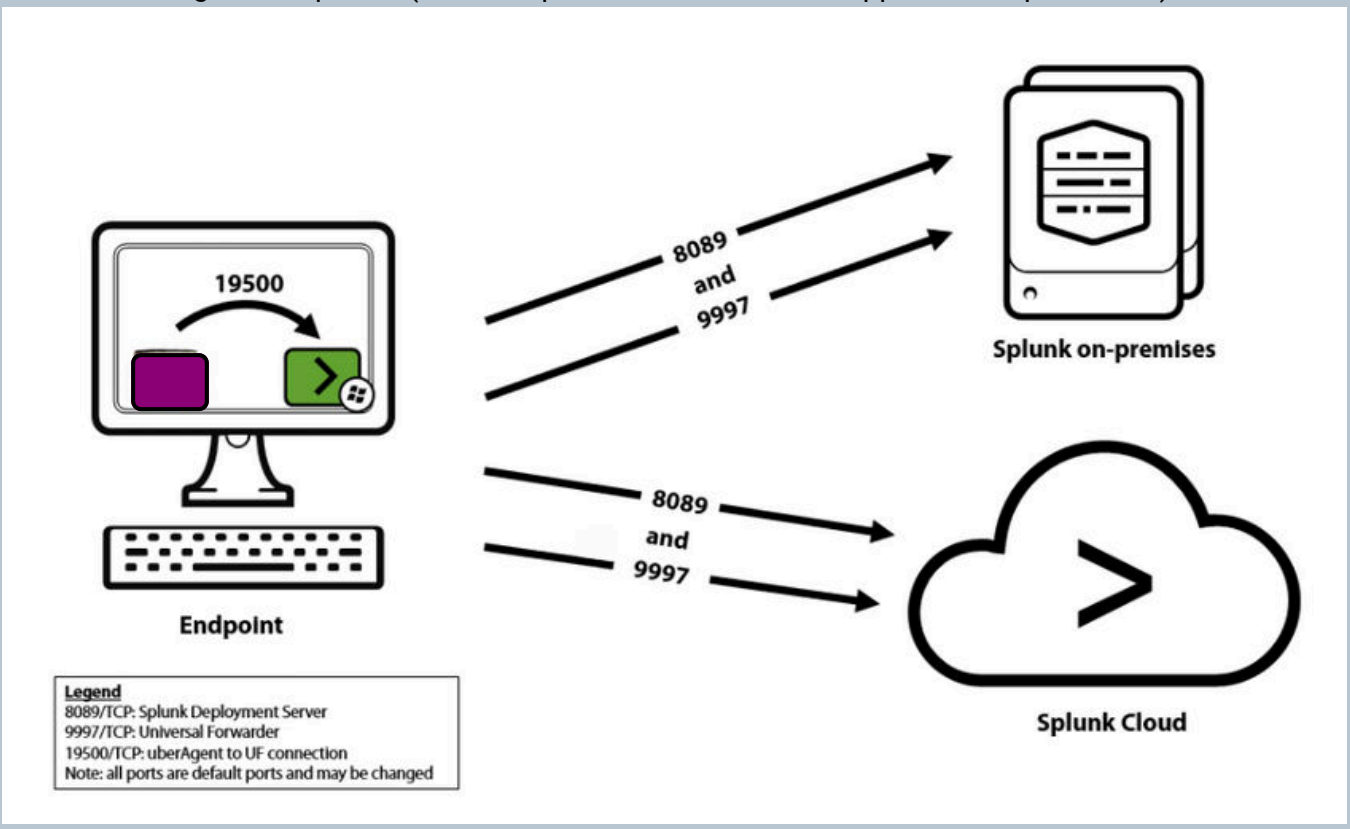
Verwandeln Sie Daten in Antworten - mit Splunk as a Service!

Splunk Cloud ist eine flexible Plattform, um die Daten in Ihrer Cloud-Umgebung zu durchsuchen, zu analysieren und zu visualisieren.

Damit können Sie:

- Daten in Terabyte-Größe erfassen und sammeln, um sie in Splunk und anderen Zielen zu nutzen
- Alle Arten von Daten in Ihrem Ökosystem durchsuchen
- Mittels Machine Learning Sicherheits- und Leistungsprobleme voraussagen und vermeiden
- Mit Dashboards mühelos komplexe Data Storys vermitteln
- Über mobile Geräte und Augmented Reality von überall zusammenarbeiten

Datenerfassung am Endpunkt* (hier mit Splunk UF und Premium App aus der SplunkBase)



*Quelle: Splunk

5. Die Ergebnisse

- Durch die Entscheidung, Splunk Cloud zu nutzen, konnten die initialen Probleme des Kunden innerhalb weniger Tage gelöst werden - ganz ohne die Bereitstellung von neuen Servern.
- Heute ist der Kunde in der Lage, sich alle relevanten Maschinendaten in einer Oberfläche anzeigen zu lassen. Er kann diese nach unterschiedlichsten Aspekten durchsuchen, analysieren und somit zielgerichtete, Daten-basierte Entscheidungen treffen. Die Fehlerkosten sinken und die Kundenzufriedenheit steigt.
- Der Kunde profitiert zum einen von einer hohen Zeitersparnis bei der Ursachenforschung nach Fehlerquellen und zum anderen von einer erheblichen Kostenreduktion.
- Durch permanente Analyse der Daten und die sofortige Alarmierung bei Anomalien, hat der Support jederzeit einen Überblick und kann zielgerichtet agieren.
- Die Splunk Cloud Plattform hilft dem Kunden das gesamte Potential seiner Daten auszuschöpfen. Gleichzeitig werden die gesetzlichen Datenschutzvorgaben und die Compliance Standards erfüllt.
- Ressourcen sparen durch NetDescribe Managed Services:
  Der Kunde kauft mit den externen Services IT-Ressourcen und Expertenwissen ein, ohne dass eigene Mitarbeiter:innen langwierig geschult und von anderen wichtigen Projekten abgezogen werden müssen.
- Security auf höchstem Niveau:
  Gerade kleine und mittelständische Unternehmen profitieren von dem konzentrierten Know-how innerhalb des S@ND Teams. Langjährige Expertise unserer SOC Analysten sorgt für den Schutz Ihrer sensiblen Daten und die Aufrechterhaltung einer starken Cybersicherheitsstruktur.

Das Splunk Portfolio

Splunk Plattform.
Splunk Enterprise sammelt und indiziert in Echtzeit alle Maschinendaten, die in physikalischen, virtuellen oder Cloud-Umgebungen erzeugt werden. Dies können Daten aus Applikationen, Servern, Netzwerken, Sensoren oder Telekommunikationsgeräten sein. Die Lösung korreliert komplexe Ereignisse, ermöglicht aussagekräftige Einblicke in Maschinendaten und vereinfacht Analysen.

Splunk für Sicherheit.
Splunk Enterprise Security verbessert alle Sicherheitsprozesse und gibt Ihnen als analysegestützte SIEM-Lösung (Security Information and Event Management) die ganzheitliche Sicht, um erzeugte Maschinendaten (z. B. Angaben über Netzwerke, Endpunkte, Zugriffe, Schwachstellen und Identitätsdaten) sicher nutzen zu können und um Sicherheitsverstöße zu reduzieren.

Splunk für IT- und Business Services.
Splunk IT Service Intelligence (ITSI) visualisiert als Monitoring- und Analyselösung Zustandsdaten und Key-Performance-Indikatoren (KPIs) von kritischen IT- und Business Services. Splunk ITSI nutzt maschinengetriebene (künstliche) Intelligenz, identifiziert bestehende und potenzielle Probleme, priorisiert die schnelle Wiederherstellung geschäftskritischer Dienste und stellt analytisch betriebene IT-Operations bereit.

Operational Intelligence & Security mit Splunk Enterprise und NetDescribe

Die Splunk-Funktionen auf einen Blick

Sammlung und Indizierung von Maschinendaten
Eventerfassung in Echtzeit, universelle Indizierung, Adapterentfall, Verwendung von Metrikdaten, Zeitstempel für Events

Suche und Überprüfung
Echtzeitsuche, Transaktionssuche, interaktive Ergebnisse

Korrelation und Analyse
Machine-Learning-basierte KI, Korrelation komplexer Events, Ereignisanmerkungen, Mustererkennung

Visualisierung und Reporting
Dashboard-Erstellung, Automatisierung von Berichten

Überwachung und Alarmierung
Monitoring von Ereignissen und KPIs, proaktive Benachrichtigungen

Sicherheit und Verwaltung
Verschlüsselter Zugriff auf Datenströme, gesicherter Benutzerzugriff