
NetDescribe
Member of xantaro group
NetDescribe Use Case
Visibilität mit Splunk IT Service Intelligence
mit Splunk Enterprise
www.netdescribe.com

1. Die Ausgangssituation

In unserem UseCase beleuchten wir den Status der zentralen Protokollierung und die Herausforderungen der Ursachenanalyse.

Unser Kunde hat die Aufgabe, leistungsfähige und zukunftsorientierte E-Government-Anwendungen sowie zentrale Infrastrukturen für den Betrieb von IT-Systemen für Verwaltung und Gerichte zur Verfügung zu stellen.

Im bestehenden IT-Betrieb wurde eine zentrale Logging-Infrastruktur erfolgreich mit Splunk Enterprise implementiert. Sämtliche relevanten Komponenten, die zur Erbringung des zentralen Kunden-Use-Cases – der Bereitstellung von Webdiensten – beitragen, liefern ihre Protokolldaten an diese Plattform. Dazu zählen Betriebssystem-Logs (Windows, Linux), Webserver-Protokolle (Apache, IIS, NGINX), Netzwerk-Logs (Firewall, Proxy), Datenbanklogs (z. B. SQL Server), sowie Applikationsprotokolle (Exchange, Active Directory, kundenspezifische Anwendungen).

Diese umfassende Datenbasis bietet grundsätzlich die Möglichkeit, Root-Cause-Analysen bei Systemstörungen oder Vorfällen durchzuführen. Jedoch gestaltet sich die Ursachenforschung oftmals als aufwendig und komplex, da ein tiefes Verständnis der technischen Hierarchien, Systemzusammenhänge und betrieblichen Abläufe erforderlich ist, um die Logdaten korrekt zu korrelieren und interpretieren.

Ein wiederkehrendes Problem besteht in der Reaktivität der Fehlererkennung: Es treten regelmäßig Störungen auf, die im Vorfeld anhand bestehender Logdaten identifizierbar gewesen wären. Beispiele hierfür sind etwa vollgelaufene Festplatten oder überlastete Systemkomponenten.

Solche Incidents könnten durch eine vorausschauende Analyse (Predictive Monitoring) oder intelligente Alarmierung bereits im Vorfeld erkannt und vermieden werden.

Trotz der breiten Datenverfügbarkeit fehlt es aktuell an einer systematischen, proaktiven Auswertung und Priorisierung potenzieller Risiken.

Die vorhandene Infrastruktur wird primär zur nachgelagerten Fehleranalyse genutzt, anstatt potenzielle Schwachstellen frühzeitig zu identifizieren.

Eine Optimierung in Richtung präventiver Wartung und intelligenter Alerting-Strategien wäre ein logischer nächster Schritt zur Erhöhung der Betriebssicherheit und Effizienz.

NetDescribe BUSINESS BONUS

NetDescribe bietet **zusätzlich zum reinen Produkteinsatz** den entscheidenden Mehrwert durch die Umsetzung proaktiver Monitoring-Lösungen, die Probleme frühzeitig erkennen, bevor sie geschäftskritisch werden.

Wir unterstützen bei der Übersetzung technischer Daten in nutzbare Informationen, die zielgruppenorientiert aufbereitet und operativ verwertbar sind – was intern oft nur mit erheblichem Zeit- und Ressourcenaufwand möglich wäre.

2. Anforderungsanalyse

Die angestrebte Lösung soll die Durchführung von **Root-Cause-Analysen** wesentlich vereinfachen und strukturieren.

Ziel ist es, dass nicht nur Experten, sondern auch Mitarbeitende im 1st- und 2nd-Level-Support in der Lage sind, Störungen eigenständig zu analysieren – **ohne tiefgehendes Spezialwissen über alle beteiligten Applikationen und Services** voraussetzen zu müssen.

Dazu ist eine Lösung erforderlich, die durch **intuitive Visualisierung, geführte Analyseschritte** und **automatisierte Korrelation** von Ereignissen unterstützt. Ergänzend soll ein **Machine-Learning gestütztes Anomalie-Erkennungs-System** integriert sein, das ungewöhnliche Muster frühzeitig identifiziert und automatisch präventive Alarmierungen auslöst – noch bevor es zu einer Beeinträchtigung des Betriebs kommt.

So entsteht ein System, das nicht nur reaktive Fehlerbehebung ermöglicht, sondern einen entscheidenden Beitrag zur **Proaktivität und Stabilität im IT-Betrieb** leistet.

Splunk Service Intelligence

Splunk IT Service Intelligence (ITSI) ist eine leistungsstarke Monitoring- und Analyseplattform für den IT-Betrieb, die auf der Splunk-Technologie basiert. ITSI ermöglicht eine ganzheitliche Sicht auf die Gesundheit und Performance von IT-Services durch die Kombination von Echtzeit-Datenanalyse, Service-Korrelation und intelligenter Alarmierung.

Die Lösung bietet **transparente Einblicke in komplexe IT-Umgebungen**, indem sie technische Metriken, Logs und Events zu geschäftsrelevanten Services zusammenführt. Durch die Nutzung von Machine Learning erkennt ITSI Anomalien automatisch, bewertet Servicezustände anhand definierter KPIs (Key Performance Indicators) und priorisiert Vorfälle basierend auf ihrer Auswirkung auf den Geschäftsbetrieb.

Zudem unterstützt ITSI bei der Root-Cause-Analyse, reduziert die Mean-Time-to-Resolution (MTTR) und fördert die Proaktivität im IT-Betrieb, indem es frühzeitig auf potenzielle Störungen hinweist. Dashboards, Glas-Cockpits und vordefinierte Use-Cases ermöglichen auch weniger spezialisierten Support-Teams eine effektive Überwachung und Fehleranalyse.

Insgesamt bietet Splunk ITSI eine zentrale, intelligente Steuerungsplattform zur Optimierung der Servicequalität und zur Stärkung der operativen Stabilität in modernen, dynamischen IT-Landschaften.

Weitere Informationen finden Sie im Product Brief zu **Splunk IT Service Intelligence**.

3. Die Lösung

Um den gestellten Anforderungen gerecht zu werden und sowohl Transparenz als auch Proaktivität im IT-Betrieb zu gewährleisten, musste eine geeignete Technologie gefunden werden.

Die Lösung von NetDescribe

Die Nutzung von ITSI als zentrale Plattform für serviceorientiertes Monitoring.

Splunk ITSI bietet eine leistungsfähige Lösung zur übergreifenden Überwachung und Bewertung von IT-Services mithilfe eines hierarchisch strukturierten Service- und KPI-Modells, das in sogenannten Glass Tables visualisiert wird.

Kernstück der Lösung ist die Definition und Messung von Key Performance Indicators (KPIs), die in Echtzeit den Zustand einzelner Systemkomponenten und deren Einfluss auf übergeordnete Services widerspiegeln.

Die KPIs sind hierarchisch aufgebaut, sodass sich Störungen auf unteren Ebenen – beispielsweise bei einem Speichermodul oder einer Webserver-Komponente – bis hin zur Gesamtsicht auf geschäftskritische Services wie Exchange oder Datenbankplattformen durchschlagen können.

Diese Struktur ermöglicht eine schnelle Identifikation der Ursache und Bewertung der Auswirkungen auf den operativen Betrieb.

ITSI verfügt über integrierte Machine-Learning-Funktionen, insbesondere für Anomalieerkennung, und bietet eine Vielzahl vortrainierter Modelle zur automatisierten Analyse und Abweichungs-erkennung.

Dadurch lassen sich Unregelmäßigkeiten frühzeitig erkennen und proaktiv adressieren.

Für viele Standardservices – etwa Microsoft Exchange – existieren vorgefertigte Integrationen und KPI-Sets, die eine schnelle Implementierung und hohe Aussagekraft ermöglichen.

Darüber hinaus lässt sich ITSI flexibel erweitern: Neben klassischem Operations-Monitoring wurde die Plattform beispielsweise auch um Security-spezifische Use-Cases ergänzt. Hierbei werden sicherheitsrelevante KPIs (z. B. SQL-Injection-Versuche, Cross-Site-Scripting, Brute-Force-Angriffe) definiert, visualisiert und in die Gesamtsicht integriert, um IT-Security und IT-Betrieb auf einer gemeinsamen Plattform zusammenzuführen.

Damit stellt ITSI eine ganzheitliche Lösung dar, die sowohl die technische Stabilität als auch die Sicherheitslage von IT-Services transparent und steuerbar macht – und das in einer für Support und Management gleichermaßen verständlichen Form.

Microsoft Exchange Executive Overview Dashboard*

Das Microsoft Exchange Executive Overview Dashboard ist ein Glas Table innerhalb des Content Packs für Microsoft Exchange. Es bietet wichtige Betriebsmetriken, Trends und Sicherheitsübersichten in einer einzigen Ansicht, die es Unternehmensleitern, CIOs/CTOs und IT-Operations erleichtert, den Gesamtzustand und die Leistung ihrer Microsoft Exchange-Dienste zu verstehen. Es enthält wichtige Metriken und KPIs für vier Exchange-Komponenten: Mailbox, Client Access, Transport und Legacy.

Die Experten von NetDescribe - Ihre Lösung bei fehlenden Inhouse-Ressourcen

Unsere Experten verstehen nicht nur die technischen Möglichkeiten von Splunk, sondern auch die geschäftlichen Anforderungen und Prioritäten Ihres Unternehmens. Dadurch können sie Dashboards entwickeln, die zielgerichtet, benutzerfreundlich und auf Ihre konkreten Use-Cases zugeschnitten sind – etwa für IT-Betrieb, Management, Sicherheit oder Compliance.
Konkret bedeutet das:

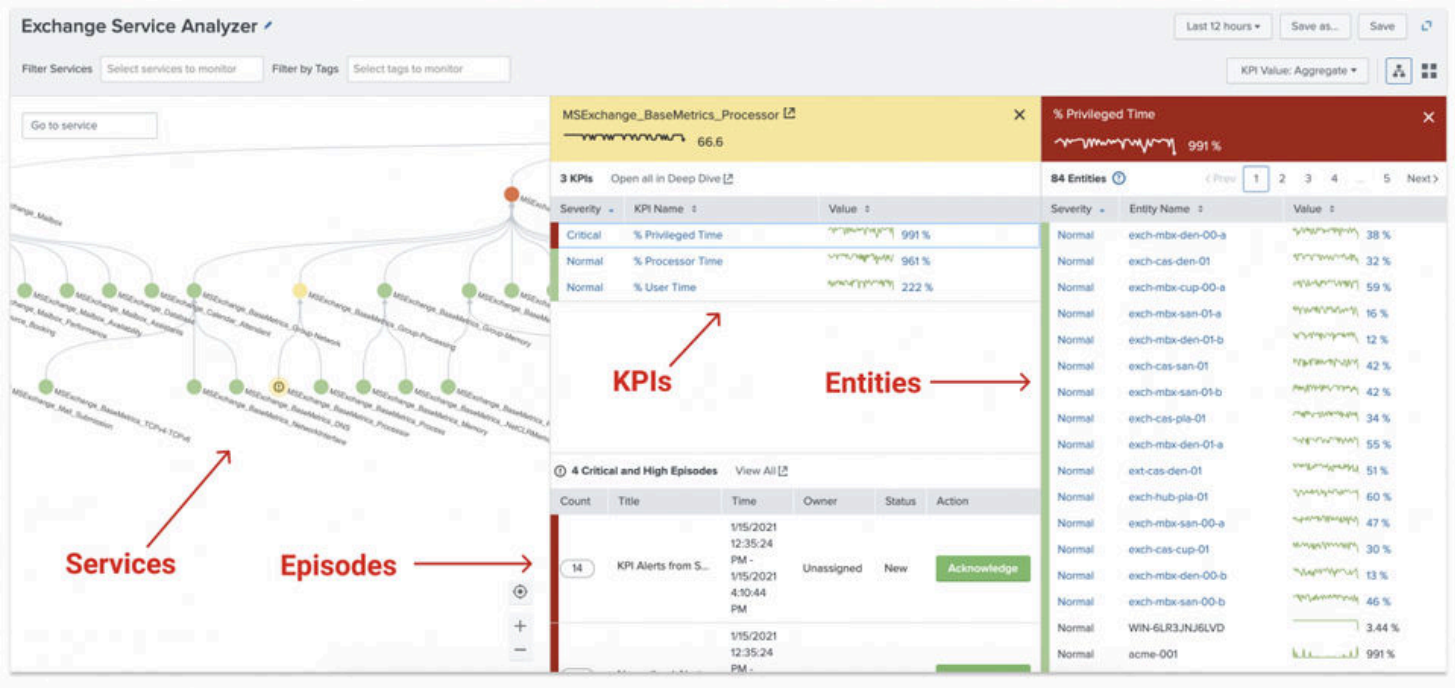
- Relevante KPIs und Metriken werden gezielt identifiziert und sinnvoll visualisiert.
- Komplexe Zusammenhänge (z. B. zwischen Infrastruktur, Applikationen und Services) werden verständlich und intuitiv abgebildet.
- Automatisierung und Dynamisierung (z. B. durch Lookups, Drilldowns, adaptive Filter) steigern die Effizienz und Aussagekraft.
- Dashboards werden so gestaltet, dass sie konkret in Entscheidungen und Maßnahmen münden, statt nur Daten darzustellen.

*Quelle: Splunk

Splunk ITSI Service Insights ermöglicht die Erstellung von vier Arten von Dashboards: Infrastructure Overview, Service Analyzer, Deep Dives und Predictive Analytics.

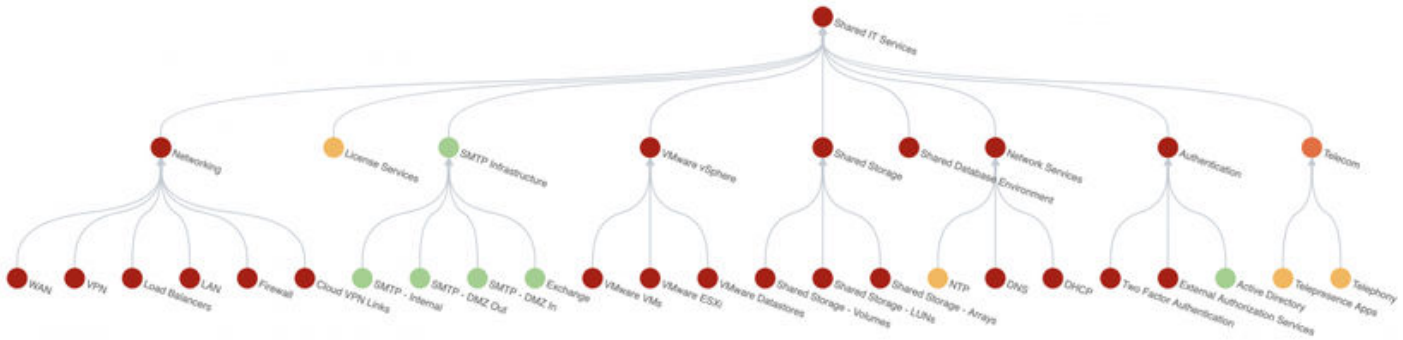
Infrastructure Overview Dashboards bieten einen konsolidierten Überblick über alle Datenintegrationen und Untersuchungstools. Service Analyzer Dashboards helfen bei der Darstellung von Abhängigkeiten zwischen Geräten und Anwendungen.

Exchange Service Analyzer*



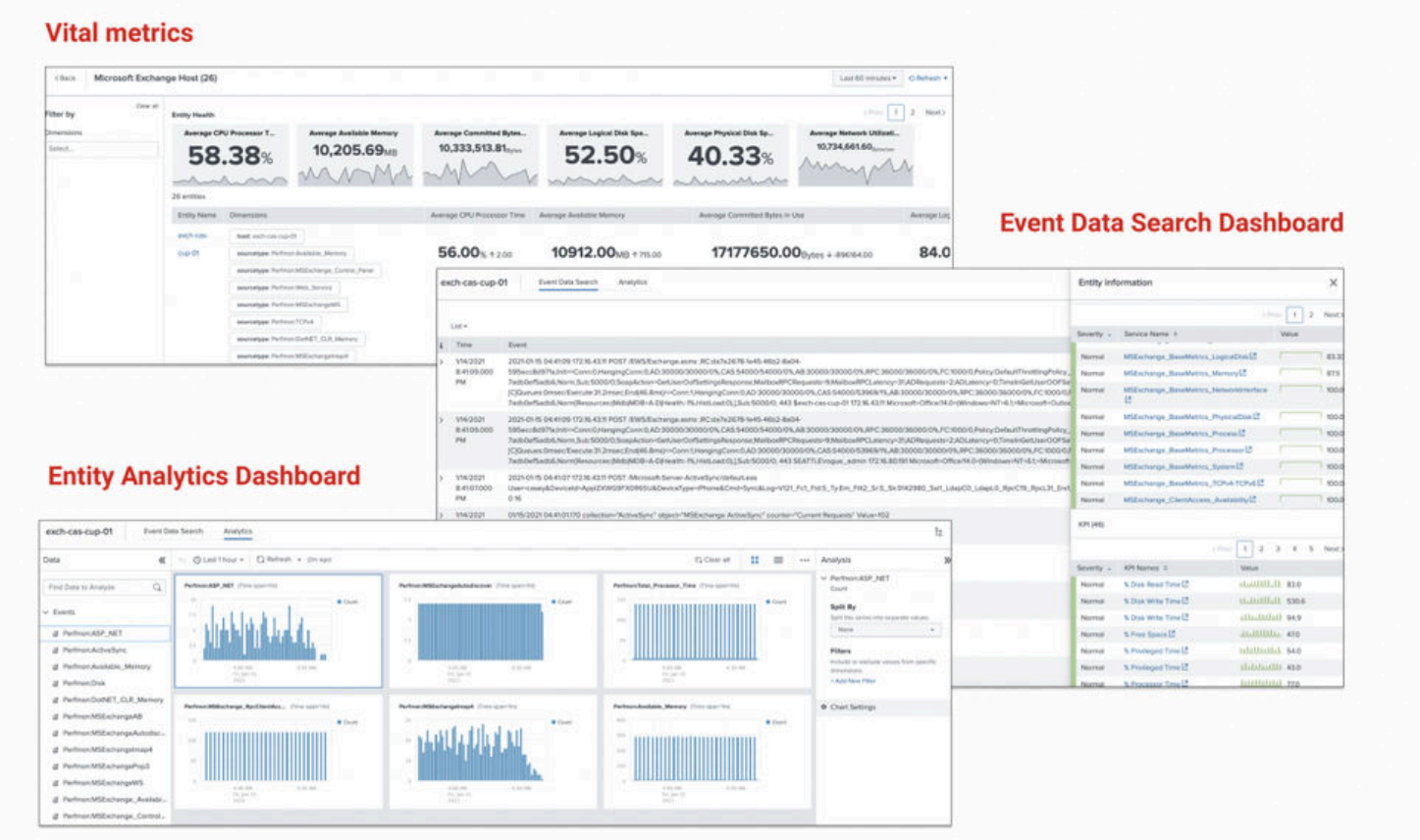
Der Exchange Service Analyzer ist eine vorkonfigurierte Ansicht im Content Pack für Microsoft Exchange, die eine visuelle Darstellung der Microsoft Exchange-Dienste und ihrer Abhängigkeiten bietet. Er ermöglicht es Benutzern, zugehörige KPIs, Entitäten und kritische Episoden zu sehen und erleichtert so die Ursachenanalyse und Fehlerbehebung. Diese Funktion hilft bei der Überwachung des Zustands und der Leistung von Microsoft Exchange-Diensten wie Edge- und Hub-Transport-Servern, Client-Access-Servern und Mailbox-Speicher.

Services Dashboard*



*Quelle: Splunk

Dashboards*



Vital Metrics in Splunk ITSI (IT Service Intelligence) stellen statistische Berechnungen auf der Grundlage von SPL-Suchen dar, die den Gesamtzustand von Entitäten, wie z. B. APM-Entitätstypen von Drittanbietern, anzeigen und Metriken wie die durchschnittliche Verfügbarkeitszeit, die durchschnittliche Antwortzeit und die durchschnittliche Fehlerrate umfassen. Diese Metriken können auf der Seite Entity Health in ITSI eingesehen werden.

Das Dashboard **Ereignisdatensuche** ermöglicht es Benutzern, Ereignisdaten in ihrer Organisation zu suchen und anzuzeigen. Um auf das Dashboard Ereignisdatensuche zugreifen zu können, müssen Benutzer über Standardindizes in ihrer Rolle verfügen, z. B. itoa_user, die Indizes wie itsi_tracked_alerts und itsi_grouped_alerts enthalten. Zusätzliche Indizes können bei Bedarf zu Benutzerrollen hinzugefügt werden.

Mit dem Dashboard **Entity Analytics** können Sie Metriken und Protokolle für bestimmte Entitäten in ITSI analysieren. Sie können das Dashboard mit Metriken und Protokollen entsprechend den Analysedatenfiltern auffüllen, die ITSI mit einer bestimmten Entität verknüpft. Dies ermöglicht eine detaillierte Untersuchung der Entitätsleistung und des Zustands. Das Dashboard ist für verschiedene Entitätstypen verfügbar, einschließlich der Entitäten von Splunk AppDynamics und Microsoft Exchange.

*Quelle: Splunk

4. Business Benefits

- Durch den Einsatz von Splunk ITSI wurde eine transparente Sicht auf die IT-Services geschaffen – inklusive klarer Abhängigkeiten und Zustände.
- Die Kombination aus Glass Tables und dem Service Analyzer ermöglicht eine zielgerichtete und schnelle Root-Cause-Analyse, selbst in komplexen Umgebungen – ohne tiefes Fachwissen im gesamten Service-Stack.
- Trotz fehlender CMDB konnten die erforderlichen Verknüpfungen zwischen Datenquellen, Entitäten und KPIs mithilfe von Splunk Lookups und dynamischen, geplanten Suchen automatisiert abgebildet werden. So werden KPIs kontinuierlich korrekt konfiguriert, ohne manuellen Aufwand.
- Die in ITSI integrierte Anomaly Detection auf Basis von Machine Learning identifiziert Abweichungen im Systemverhalten automatisiert – ein entscheidender Vorteil bei großen Eventmengen.
- Zusätzlich ermöglicht das Machine Learning Toolkit eine proaktive Kapazitätsplanung, z. B. durch Vorhersage von Festplattennutzung, was frühzeitige Alarmierung und risikobasierte Maßnahmen erlaubt.
- Insgesamt führt dies zu höherer Betriebssicherheit, geringeren Reaktionszeiten und einer deutlichen Entlastung des operativen IT-Teams.

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.

“Zentrale Überwachung aller Maschinendaten”
Martin Liebelt, Splunk®-Experte bei 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