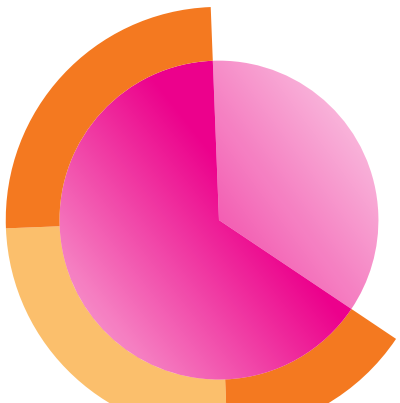
Leitfaden für
Infrastrukturdaten

splunk>
turn data into doing™

Zeitreihendaten. Streaming-Daten. Dark Data.

Es ist kein Geheimnis, dass Daten in den meisten Unternehmen überall auf der Welt immer noch zu wenig genutzt werden und unterschätzt sind. Obwohl ständig von datengestützten Entscheidungen die Rede ist, verfehlen Unternehmen aller Größen nach wie vor das Ziel, die täglich anfallenden Datenmengen effektiv zu erfassen und zu verarbeiten – ganz gleich, ob sie von Benutzern, externen Branchenressourcen oder ihren eigenen vernetzten Geräten stammen. Tatsächlich schätzen die meisten Entscheidungsträger in den Fachbereichen und der IT, dass **55 % ihrer Daten Dark Data** sind, also Informationen, von denen sie nicht wissen, dass sie vorhanden sind oder die sie nicht in der Lage sind, vollständig nutzbar zu machen.

Dadurch wird eine große Chance verpasst. Wichtige Einblicke in die IT, Cyber Security und in Ihr Unternehmen sind in diesen Daten verborgen. Daten enthalten verlässliche Aufzeichnung aller Aktivitäten und Verhaltensweisen ihrer Kunden und Nutzer, Transaktionen, Anwendungen, Server, Netzwerke, Mobilgeräte und von vielem mehr. Bedeutende Informationen zu allen Bereichen – von Konfigurationen, APIs, Nachrichtenwarteschlangen, Diagnoseausgängen, Sensordaten von Industrieanlagen und vielem mehr – stehen Ihnen zur Verfügung. Sie müssen sie sich nur richtig erschließen.



Mit dem richtigen Ansatz erleichtern Daten folgende Aufgaben:

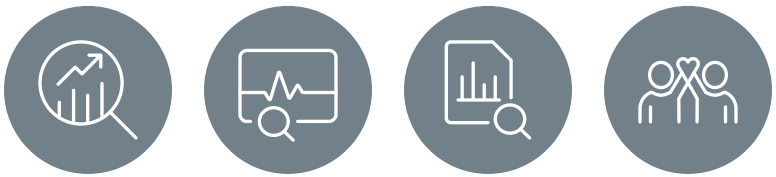
- Das Treffen fundierterer Entscheidungen in allen Unternehmensbereichen
- Eine Effizientere Betriebsführung
- Das Optimieren der Benutzer- und Kundenerfahrung
- Das Erkennen von Hinweisen auf Betrug (bzw. das Vermeiden von Betrug insgesamt)
- Das Erkennen potenzieller Katastrophen, ehe sie eintreten
- Das Ausmachen verborgener Trends, die Ihrem Unternehmen zu einem Wettbewerbsvorsprung verhelfen
- Jeden, der sie nutzt, wie einen Experten aussehen lassen
- … und vieles mehr

Die Herausforderung bei der Nutzung der riesigen Datenmengen, die die meisten Unternehmen anhäufen, besteht darin, dass sie in einer schwindelerregenden Vielfalt von Formaten vorliegen, mit denen herkömmliche Tools für Monitoring und Datenanalyse nicht umgehen können. Viele Tools sind von den unterschiedlichen Datenstrukturen, Quellen oder Zeitspannen überfordert. Und das geht weit über reine Maschinendaten hinaus. Doch die Vorteile, die sich aus dem Erschließen Ihrer Daten ergeben, sind enorm. Und genau hier kommt Splunk ins Spiel.

Mit Splunk können Sie Daten für jede Frage, Entscheidung und Maßnahme in Ihrem Unternehmen heranziehen, um aussagekräftige Ergebnisse zu erzielen. Im Gegensatz zu allen anderen Plattformen ist Splunk tatsächlich in der Lage, beliebige Daten aus beliebigen Quellen zu verarbeiten, um damit konkrete Maßnahmen anzustoßen, von denen Ihr Unternehmen profitiert. Der Nutzen reicht vom Monitoring der IT-Infrastruktur und Security bis zur Überwachung und Verwaltung der DevOps- und Anwendungsleistung.

Data-to-Everything in der Praxis

Nutzen Sie Daten für diese Zwecke:



Untersuchen **Überwachen** **Analysieren** **Handeln**

Die Organisationen, die am meisten von ihren Daten profitieren, sind diejenigen, die in der Lage sind, unterschiedliche Datentypen heranzuziehen, sie anzureichern und Antworten herauszufiltern. Doch nicht zu wissen, welche Daten verarbeitet werden sollten, kann Unternehmen ausbremsen, ehe sie überhaupt loslegen.

Indem Sie sich mit allgemeinen Use Cases in den Bereichen Sicherheit, IT Operations, Business Analytics, DevOps, Internet of Things (IoT) und mehr – einschließlich der zugehörigen Datentypen und -quellen – vertraut machen, können Sie sofort den richtigen Lösungsweg einschlagen.

Hier ein Beispiel:

1. Die Bestellung eines Kunden wird nicht bearbeitet.
2. Der Kunde ruft den Support an, um das Problem zu lösen.
3. Nachdem der Kunde zu viel Zeit in der Warteschleife verbracht hat, gibt er auf und veröffentlicht einen Tweet mit einer Beschwerde über das Unternehmen.

Wie sehen Maschinendaten aus?

Abbildung 1: Daten können aus einer beliebigen Anzahl von Quellen stammen und auf den ersten Blick wie beliebiger Text aussehen.

Maschinendaten liefern wesentliche Erkenntnisse

Abbildung 2: Der Mehrwert der Daten ist in diesem scheinbar beliebigen Text verborgen.

Maschinendaten liefern wesentliche Erkenntnisse

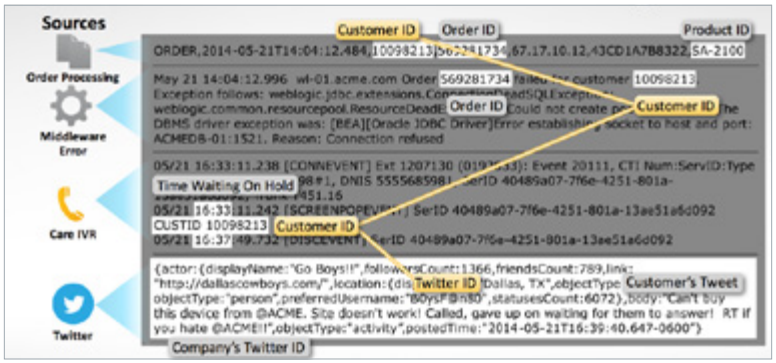


Abbildung 3: Indem verschiedene Datentypen miteinander korreliert werden, können Sie einen echten Einblick in die Vorgänge innerhalb Ihrer Infrastruktur erhalten, Sicherheitsbedrohungen erkennen oder die Erkenntnisse sogar für bessere Geschäftsentscheidungen nutzen.

Durch das Erfassen aller am Prozess beteiligten Daten – dies geschicht, indem Informationen aus Auftragsabwicklungen, der Middleware, interaktiven Sprachdialogsystemen und Twitter abgerufen werden – kann sich ein Unternehmen einen vollständigen Überblick über Probleme innerhalb der Kundenerfahrung verschaffen.

Infrastrukturdaten

Dieses E-Book verschafft Ihnen eine allgemeine Übersicht über den Nutzen, den Sie aus den Daten ziehen können, die von Ihrer virtuellen und physischen Infrastruktur im normalen Betrieb erzeugt werden. Diese Daten können eine Vielzahl von Anwendungsfällen unterstützen, die vom Monitoring Ihrer Cloud-Bereitstellungen über die Identifizierung von Angriffsversuchen bis zur Behebung von Schwachstellen reichen.

Die Bedürfnisse und Datenquellen jedes Unternehmens variieren je nach Anbieter, Produkt und Infrastruktur. Dennoch wird in diesem E-Book detailliert beschrieben, wo Sie nach der Art der Maschinendaten und dem potenziellen Nutzen für Anwendungsfälle in den Bereichen IT, Security, IoT und Business Analytics suchen sollten.

Viele der in diesem E-Book aufgeführten Datenquellen können mehrere Use Cases unterstützen, was den enormen Stellenwert von Maschinendaten wesentlich mitbestimmt.

Sicherheit und Compliance

IT Operations, Anwendungsbereitstellung und DevOps

Internet of Things (IoT)

Business Analytics

Inhalt

Daten zur virtuellen Infrastruktur

AWS Services

Anwendungsfälle: Sicherheit und Compliance, IT Operations

Beispiele: CloudTrail, CloudWatch, Config, S3

AWS ist die größte und meistgenutzte öffentliche Cloud-Infrastruktur, die on demand Compute-, Speicher-, Datenbank-, Big Data- und Anwendungsservices mit verbrauchsabhängiger Preisgestaltung anbietet. AWS kann dazu genutzt werden, die herkömmliche virtuelle Serverinfrastruktur eines Unternehmens zu ersetzen – in der Software auf einzelnen virtuellen Maschinen (VM) läuft – oder um Cloud-native Anwendungen zu hosten, die aus einer Zusammenstellung von AWS-Services bestehen. AWS bietet eine Vielzahl von Services in den Bereichen Serviceverwaltung, Automatisierung, Security, Netzwerk und Monitoring. Diese Services werden für die Bereitstellung, Skalierung, Außerbetriebnahme, Überprüfung und Verwaltung der eigenen AWS-Umgebung, der Abonnements und der gehosteten Anwendungen genutzt.

Anwendungsfälle

Sicherheit und Compliance: Zu den Sicherheitsdaten der AWS-Services gehören Login und Logout-Events und -Versuche, API-Aufrufe und Logs von Netzwerk- und Webanwendungs-Firewalls.

IT Operations: AWS-Services bieten ähnliche Arten von System- und Servicedaten wie herkömmliche IT-Infrastrukturen, von denen ein Großteil vom CloudWatch-Service konsolidiert wird. Dazu gehören das Monitoring von Services, Alarme und Dashboards für Metriken, Logs und Events, die von anderen AWS-Ressourcen und -Anwendungen generiert werden. Zu den typischen Events und Messgrößen gehört die Instanziierung und Außerbetriebnahme von Instanzen, die CPU-Auslastung, der Netzwerkverkehr und die Speicherbelegung.

Google Cloud Platform (GCP)

Anwendungsfälle: Sicherheit und Compliance, IT Operations

Beispiele: Stackdriver

GCP ist eine beliebte und umfassend genutzte öffentliche Cloud-Infrastruktur, die auf Abruf Compute-, Speicher-, Datenbank-, Big Data- und Anwendungsservices mit verbrauchsabhängiger Preisgestaltung anbietet. GCP kann genutzt werden, um herkömmliche virtuelle Serverinfrastrukturen in Unternehmen zu ersetzen – in denen Software auf einzelnen VMs läuft – oder um Cloud-native Anwendungen zu hosten, die aus einer Zusammenstellung von GCP-Services bestehen. GCP bietet eine Vielzahl von Services in den Bereichen Serviceverwaltung, Automatisierung, Security, Netzwerk und Monitoring. Diese Services werden für die Bereitstellung, Skalierung, Außerbetriebnahme, Überprüfung und Verwaltung der eigenen GCP-Umgebung, der Abonnements und der gehosteten Anwendungen genutzt.

Anwendungsfälle

Sicherheit und Compliance: Zu den Sicherheitsdaten von GCP-Services gehören Login und Logout-Events und -Versuche, API-Aufrufe und Logs von Netzwerk- und Webanwendungs-Firewalls.

IT Operations: GCP-Services bieten ähnliche Arten von System- und Servicedaten wie herkömmliche IT-Infrastrukturen, von denen ein Großteil von Stackdriver konsolidiert wird. Dazu gehören das Monitoring von Services, Alarme und Dashboards für Metriken, Logs und Events, die von anderen GCP-Ressourcen und -Anwendungen generiert werden. Zu den typischen Events und Messgrößen gehören die Instanziierung und Außerbetriebnahme von Instanzen, die CPU-Auslastung, der Netzwerkverkehr und die Speicherbelegung.

Microsoft Azure

Anwendungsfälle: Sicherheit und Compliance, IT Operations

Beispiele: WADLogs, WADEventLogs, WADPerformanceCounter, WADDiagnostInfrastructure

Azure ist eine beliebte und weit verbreitete öffentliche Cloud-Infrastruktur, die auf Abruf Compute-, Speicher-, Datenbank-, Big Data- und Anwendungsservices mit verbrauchsabhängiger Preisgestaltung anbietet. Azure kann genutzt werden, um herkömmliche virtuelle Serverinfrastrukturen in Unternehmen zu ersetzen – in denen Software auf einzelnen VMs läuft – oder um Cloud-native Anwendungen zu hosten, die aus einer Zusammenstellung von Azure-Services bestehen. Azure bietet eine Vielzahl von Services in den Bereichen Serviceverwaltung, Automatisierung, Security, Netzwerk und Monitoring. Diese Services werden für die Bereitstellung, Skalierung, Außerbetriebnahme, Überprüfung und Verwaltung der eigenen Azure-Umgebung, der Abonnements und der gehosteten Anwendungen genutzt.

Anwendungsfälle

Sicherheit und Compliance: IT-Sicherheitsteams können Logs von Azure-Services verwenden, um die Einhaltung festgelegter Richtlinien zu überprüfen und zu bestätigen. Logdaten sind auch für die forensische Analyse von Störungen von unschätzbarem Wert, z. B. zur Identifizierung unbefugter Zugriffsversuche in Zugriffs-Logs, zur Verfolgung von Ressourcen und Konfigurationsänderungs-Events und zur Ermittlung von Schwachstellen in Hosts oder Firewalls.

IT Operations: Azure-Services bieten detaillierte Metriken und Logs für das Monitoring der eigenen Infrastruktur im gesamten IT-Stack – von VMs über Container und Datenspeicher bis zu Anwendungs-Services. Die Daten sind hilfreich bei der Qualitätssicherung bezüglich der Anwendungsbereitstellung und der Service-Levels, bei der Messung des Benutzerverhaltens und der Ressourcenauslastung sowie für die Kapazitätsplanung und das Kostenmanagement.

DATEN ZUR VIRTUELLEN INFRASTRUKTUR

Pivotal Cloud Foundry (PCF)

Anwendungsfälle: IT Operations und DevOps

Beispiele: Loggregator, PCF Healthwatch

Pivotal Cloud Foundry ist eine Platform-as-a-Service-Lösung (PaaS), die auf Cloud Foundry, einer Open-Source-Plattform für Cloud Computing, aufbaut und Entwicklern das einfache Bereitstellen, Betreiben und Skalieren Cloud-nativer Anwendungen ermöglicht. Unternehmen können den gesamten Anwendungslebenszyklus – vom Packaging über die Bereitstellung bis hin zur Ausführung – verwalten, da Cloud Foundry viele Cloud-Frameworks und -Anwendungssprachen unterstützt. Mit Funktionen wie Infrastrukturverwaltung und -bereitstellung, Betriebssystem-Patches, Containerorchestrierung, Sicherheit und mehr vereinfacht PCF die Installation und Verwaltung Cloud-nativer Anwendungen.

Anwendungsfälle

IT Operations und DevOps: Operations-Teams können PCF-Metriken nutzen, von denen ein Großteil von Loggregator Firehose konsolidiert wird, um Einblicke in Bereitstellungszustand, Kapazitätsbedarf und Anwendungszustand zu gewinnen, ehe Endbenutzer durch Leistungseinbußen beeinträchtigt werden. Da PCF es DevOps ermöglicht, Anwendungen in jeder beliebigen Cloud schnell auszuführen und bei Bedarf zu skalieren, sind PCF-Daten für die Teams von entscheidender Bedeutung, um einen umfassenden Einblick in den gesamten Lebenszyklus zu erhalten und Transparenz zwischen den einzelnen Komponenten herzustellen. Wenn es darum geht, maßstabsgerechte PCF-Bereitstellungen zu betreiben, hängt das Verstehen der Performance von den Abhängigkeiten zwischen den verschiedenen Schichten innerhalb der App, des Containers und der übergeordneten Architektur ab.

VMware-Server-Logs, -Konfigurationsdaten und -Leistungsmetriken

Anwendungsfälle: Sicherheit und Compliance, IT Operations

Beispiele: vCenter, ESXi

VMware vSphere ESXi ist die am häufigsten eingesetzte Server-Virtualisierungsplattform für Unternehmen. Die VMware-Management-Plattform – sei es eines der vSphere-Produkte oder der eigenständige Hypervisor – produziert eine Vielzahl von Daten in vier Hauptkategorien:

- **vCenter-Logs:** vCenter ist das „Kontrollzentrum" einer vSphere-Umgebung. Die vCenter-Logs enthalten z. B. Informationen darüber, wer sich anmeldet, um Änderungen vorzunehmen, welche Personen Änderungen vorgenommen haben und welche Authentifizierungsfehler aufgetreten sind.
- **ESXi-Logs:** Zu jeder vSphere-Umgebung gehören einzelne oder mehrere ESXi-Hypervisoren. Das sind die Systeme, auf denen die virtuellen Maschinen gehostet werden. ESXi-Logs enthalten Informationen, die bei der Behebung von Hardware- und Konfigurationsproblemen hilfreich sind.
- **Bestandsinformationen:** Die vCenter-Umgebung verfolgt die Konfiguration einer Reihe von Konfigurationselementen nach – einschließlich Hypervisoren, VMs, Datenspeicher, Cluster und mehr. Dazu gehört die Konfiguration jedes Elements und die Beziehung eines bestimmten Elements zu allen anderen. Diese Informationen werden nicht in den Logdateien der vCenter- oder ESXi-Server abgebildet. Sie können mithilfe des vSphere-Clients oder von vSphere-APIs eingesehen werden. In beiden Fällen werden diese Informationen von den vCenter-Servern abgerufen.
- **Informationen zur Performance:** Für jedes konfigurierte Element verfolgt der vCenter-Server eine Reihe von Leistungsmetriken nach. Dazu zählen die Latenz von Datenspeichern, die Auslastung virtueller oder physischer CPUs und über 100 andere Metriken. Wie bei den Bestandsinformationen sind diese Informationen nicht in den Logdateien enthalten und müssen über den vSphere-Client eingesehen oder über die vSphere-API abgefragt werden.

Anwendungsfälle

Sicherheit und Compliance: Die Entkopplung der virtuellen Ressourcen und der zugrunde liegenden physischen Hardware kann bei der Untersuchung von Störfällen, bei Kapazitätsanalysen, bei der Nachverfolgung von Änderungen und der Erstellung von Sicherheitsberichten zu komplexen Herausforderungen führen. Ein gängiger sicherheitsrelevanter Anwendungsfall für VMware-Daten betrifft die vCenter-Logs. Diese dienen zum Überprüfen der Aktivitäten von Personen, die über die vSphere-Benutzeroberfläche Benutzerberechtigungen innerhalb der VMware-Umgebung neu zuweisen.

IT Operations: Operations-Teams können VMware-Daten nutzen, um die Integrität der gesamten Hypervisor-Umgebung und der zugrunde liegenden Gastbetriebssysteme zu messen. Administratoren können diese Daten zur Kapazitätsplanung und Behebung laufender Performance-Probleme einsetzen, z. B. bei Latenzproblemen mit dem Datenspeicher.

In diesen Daten wird auch die Nutzung von Hardwareressourcen aufgezeichnet, die zur Optimierung von VM-Bereitstellungen in einem Serverpool verwendet werden können. So kann der Ressourceneinsatz maximiert werden, ohne dass Workloads einen bestimmten Server überlasten.

Daten zur physischen Infrastruktur

Backup

Anwendungsfall: IT Operations

Trotz des Einsatzes der Datenreplikation zur Spiegelung von Systemen, Datenbanken und Dateispeichern bleibt die Datensicherung eine wesentliche IT-Aufgabe. Sie sorgt für die langfristige, archivierte Speicherung wertvoller Informationen, von denen ein großer Teil gesetzliche und regulatorische Anforderungen bezüglich der Aufbewahrung erfüllen muss. Backups können auch dazu dienen, mehrere Versionen von System-Images und Daten zu speichern. Dadurch können Unternehmen Änderungen, ungewollte Löschvorgänge oder beschädigte Daten schnell wiederherstellen und das System oder die Datenbank in einen früheren und funktionierenden Zustand zurückversetzen. Die Sicherungssoftware kann je nach Wahrscheinlichkeit des Bedarfs an den Daten verschiedene Arten von Speichermedien nutzen: externe Datenträger oder virtuelle Tape-Bibliotheken für aktive Daten und Tape, optische Datenträger oder einen Cloud-Service zur langfristigen Speicherung.

Anwendungsfälle

IT Operations: Sicherungssysteme protokollieren regelmäßig Aktivitäten und Systemstatus und zeichnen Informationen wie die Job History, den Fehlerstatus, das Sicherungsziel und ein detailliertes Verzeichnis der kopierten Dateien oder Datenträger auf. Diese Daten ermöglichen es Operations-Teams, die Integrität von Backup-Systemen, Software und Aufträgen zu überwachen. Sie lösen im Falle von Fehlern Warnmeldungen aus und helfen bei der Behebung von Fehlern beim Backup. Mit ihnen können Teams außerdem lokalisieren, wo bestimmte Daten gespeichert sind, sobald eine Wiederherstellung erforderlich ist.

Umgebungssensoren

Anwendungsfälle: Internet of Things, Business Analytics

Beispiele: Bosch Sensortec, Mouser Electronics, Raritan, Schneider Electric, TSI, Vaisala

Umgebungssensoren liefern Daten zum barometrischen Luftdruck, zur Luftfeuchtigkeit, Umgebungslufttemperatur und Luftqualität. Sie werden vielfältig eingesetzt – von der Bekämpfung von Umweltverschmutzung über die Erkennung von Gasen bis hin zum Schutz von Rechenzentren vor Überhitzung.

Anwendungsfälle

Internet of Things: Umgebungssensoren sind eine Form intelligenter Zähler, die für das Monitoring von Umgebungsbedingungen optimiert wurden. In einigen Fällen, wie z. B. in einem Rechenzentrum, werden die von diesen Sensoren übermittelten Informationen zur automatischen Änderung der Temperatureinstellung und des Wärmeflusses verwendet.

Business Analytics: Die Erfassung von Umgebungssensordaten kann in Anwendungen für den Einzelhandel genutzt werden. Dieser ist dann in der Lage, vorausschauende Fragen zu beantworten. Zum Beispiel: Welche Auswirkungen schlechtes Wetter auf den Publikumsverkehr in einem Einkaufszentrum haben könnte.

Industrielle Steuerungssysteme (ICS)

Anwendungsfälle: Sicherheit und Compliance, Internet of Things, Business Analytics

Beispiele: ABB, Emerson Electric, GE, Hitachi, Honeywell, Rockwell Automation, Siemens, Toshiba

In einer Fertigungsumgebung arbeiten industrielle Steuerungssysteme mit speicherprogrammierbaren Steuerungen, die sowohl Daten erfassen als auch Monitoring-Aufgaben übernehmen. Ein Großteil der Prozessautomatisierung in einer Fertigungsanlage wird durch die industriellen Steuerungssysteme ermöglicht.

Anwendungsfälle

Sicherheit und Compliance: Industrielle Steuerungssysteme spielen eine entscheidende Rolle bei der Erbringung von Dienstleistungen für die Industrie und Gemeinden auf der ganzen Welt. Diese Systeme bauen auf herkömmlicher IT-Infrastruktur auf und – obwohl oft separiert von der Unternehmens – drängt die digitale Transformation Unternehmen dazu, Verbindungen mit diesen Systemen einzurichten, was die Anfälligkeit für Angriffe erhöht. Diese Systeme sind aus sicherheitstechnischer Sicht meist unbemannt. Unabhängig davon, wie industrielle Steuerungssysteme angegriffen oder infiziert werden können, sorgen Daten von den zugehörigen Geräten für Transparenz und können zur Analyse und Identifizierung bösartiger Aktivitäten und potenzieller Bedrohungen dienen. Diese Transparenz ermöglicht es Unternehmen, Auswirkungen und Risiken zu messen und mit Geschäftsprozessen in Einklang zu bringen.

Internet of Things: Maschinendaten von industriellen Steuerungssystemen können eingesetzt werden, um in Echtzeit einen Überblick über die Betriebszeit und Verfügbarkeit kritischer Assets zu erhalten. Dadurch können Unternehmen ein Problem erkennen, eine Ursachenanalyse durchführen und vorbeugende Maßnahmen ergreifen, um bestimmte Ereignisse in Zukunft zu verhindern. Unternehmen nutzen Maschinendaten von industriellen Steuerungssystemen auch, um diese unternehmenskritischen Assets abzusichern.

Business Analytics: Unternehmen können Machine Learning-Algorithmen auf die von industriellen Steuerungssystemen erzeugten Maschinendaten anwenden, um die Produktivität, Betriebszeit und Verfügbarkeit zu verbessern. Diese Daten können auch die Transparenz komplexer Fertigungsprozesse erhöhen und dabei helfen, Engpässe zu erkennen und Effizienzmängel zu beseitigen.

Mainframes

Anwendungsfälle: IT Operations

Mainframes sind die ursprünglichen Unternehmenscomputer: große, zentralisierte Systeme mit Systemspeicher, mehreren Prozessoren und E/A-Controllern. Trotz ihrer 60-jährigen Geschichte sind Mainframes immer noch weit verbreitet und werden für unternehmenskritische Anwendungen, insbesondere für die Transaktionsverarbeitung verwendet. Obwohl sie in der Regel mit einem proprietären Betriebssystem arbeiten, können Mainframes auch so virtualisiert werden, dass auf ihnen UNIX und Linux oder, mit zusätzlichen Prozessorkarten, ein Windows Server laufen kann. Mainframes werden für ihre unangreifbare Zuverlässigkeit und Sicherheit geschätzt, wobei hochredundante Hardware und ausfallsichere, streng geprüfte Software zum Einsatz kommen. Daher sind sie für Unternehmen interessant, die Workloads auf einer kleinen Anzahl von Systemen konsolidieren möchten und die zusätzliche Zuverlässigkeit und Vielseitigkeit benötigen.

Anwendungsfälle

IT Operations: Wie andere Server messen und protokollieren Mainframes zahlreiche Systemparameter, die ihren aktuellen Status, ihre Konfiguration und den allgemeinen Zustand widerspiegeln. Da die meisten Mainframe-Subsysteme redundant sind, zeigen die System-Logs auch nicht unterbrechende Hardwareausfälle oder anomales Verhalten an, das auf einen bevorstehenden Ausfall hinweist. Aufgrund ihres Einsatzes für wichtige Anwendungen zeichnen Mainframes häufig Daten zur Anwendungsleistung auf wie z. B. Arbeitsspeicherauslastung, E/A- und Transaktionsdurchsatz, Prozessorauslastung und Netzwerkaktivität.

Medizinische Geräte

Anwendungsfälle: Internet of Things, Business Analytics

Beispiele: Abbott Laboratories, Apple, Baxter, Boston Scientific, GE, Siemens, St. Jude Medical

Sämtliche Geräte, z. B. auf Intensivstationen oder auch tragbare Geräte, generieren verschiedene Arten von Maschinendaten. Tatsächlich kann nahezu jeder Aspekt der Patientenversorgung innerhalb und außerhalb eines Krankenhauses instrumentiert werden. Während das primäre Ziel darin besteht, Leben zu retten, ist ein wesentliches sekundäres Ziel die Senkung der Gesundheitskosten, indem sowohl die Zahl der potenziellen Krankenhausbesuche als auch die Aufenthaltsdauer reduziert wird.

Anwendungsfälle

Internet of Things: Die meisten Geräte in einem Krankenhaus sind an lokale Monitoring-Anwendungen angeschlossen. Es ist allerdings auch möglich, die Patientenversorgung aus der Ferne zu überwachen, indem Sensoren verwendet werden, die entweder mit einem tragbaren Gerät oder einem anderen System zur häuslichen Patientenüberwachung kommunizieren.

Business Analytics: Maschinendaten erleichtern es medizinischem Fachpersonal auch, sowohl Patienten- als auch anonyme Daten über ein breiteres Spektrum geografisch verteilter Regionen hinweg zu analysieren. Damit lässt sich beispielsweise überprüfen, wie bestimmte Krankheiten eine Patientengruppe stärker beeinträchtigen als eine andere.

Metrikerfassungs-protokolle

Anwendungsfälle: IT Operations, Anwendungsbereitstellung, Internet of Things

Beispiele: collectd, statsd

Metriken sind Messungen, die von einem Prozess erzeugt werden, der auf einem System läuft und einen regelmäßigen Datenpunkt zu einer bestimmten Metrik liefert, wie z. B. die CPU-Auslastung. Metrikdatenquellen erzeugen Messungen in regelmäßigen Abständen und bestehen in der Regel aus folgenden Elementen:

- Zeitstempel
- Metrikname
- Messung (ein Datenpunkt)
- Dimensionen (die oft den Host, die Art der Instanz oder andere Attribute beschreiben, anhand derer Sie Metriken filtern oder sortieren möchten)

Metriken werden üblicherweise von einem Daemon (oder Prozess) generiert, der auf einem Server (Betriebssystem), in einem Container oder einer Anwendung läuft. Jede Datenmessung wird über ein Netzwerkprotokoll, wie z. B. UDP oder HTTP, an einen Server übertragen, der diese Informationen indiziert und analysiert.

Metriken eignen sich besonders gut für das Monitoring. Ein Beispiel hierfür wäre ein Herzmonitor, der regelmäßig den Puls eines Patienten überprüft. Metriken liefern Einblicke in Entwicklungen oder Probleme, die sich auf die Leistung und Verfügbarkeit von Infrastruktur und Anwendungen auswirken. Ein Herzmonitor wird Ihnen jedoch nicht verraten, warum ein Patient ein plötzliches Problem mit seiner Herzfrequenz hat. Sie benötigen andere Mittel, um die Ursache schnell zu erkennen und den Patienten zu stabilisieren. Das Gleiche gilt für Maschinendaten. In Kombination mit anderen Datenquellen, in der Regel Logs, erhalten Sie einen Einblick in das Geschehen und die ursächlichen Hintergründe.

Beispiele für Metrikerfassungsprotokolle

collectd: collectd ist ein Protokoll, bei dem ein Agent auf einem Server läuft, der so konfiguriert ist, dass er bestimmte Attribute misst und diese Informationen an ein angegebenes Ziel überträgt. collectd ist eine erweiterbare Mess-Engine, sodass Sie ein breites Spektrum von Daten erfassen können. Gegenwärtig dient **collectd** vor allem dazu, Einblicke in das Monitoring der Kerninfrastruktur zu gewinnen – z. B. zu Workload, Arbeitsspeicherauslastung, E/A und zur Speicherung von Servern und anderen Infrastrukturkomponenten. collectd ist Teil der Open-Source-Community. Wenn Sie mehr über collectd erfahren möchten, besuchen Sie **http://collectd.org**.

statsd: statsd ist ein Netzwerk-Daemon, der in node.js läuft. Das Programm hat bei Windows-Administratoren, Experten für Anwendungsleistung und anderen Nutzern an Popularität gewonnen. statsd bietet verschiedene Funktionen, mit denen Metriken im Batch-Modus bereitgestellt werden können. Obwohl es die weniger zuverlässige Netzwerkmethode UDP verwendet, schätzen viele Administratoren die einfache Bereitstellung. Ähnlich wie collectd konzentriert sich statsd auf das Sammeln von Metriken, die hauptsächlich die Nutzung und Leistung von Anwendungen und Anwendungskomponenten betreffen. Diese werden über das Netzwerk an ein Tool gesendet, das diese Informationen sammeln und analysieren kann.

Anwendungsfälle

Anwendungsbereitstellung und IT Operations: Metriker-fassungsprotokolle liefern Nutzungs-, Leistungs- und Verfügbarkeits-daten für verschiedene Betriebssysteme, Speichergeräte, Anwendungen und andere IT-Infrastrukturkomponenten. Metriken sind besonders nützlich für den Monitoring-Teil von IT Operations und Anwendungsbereitstellung, bei dem Trends bei der Problemerkennung helfen können. Sobald Trends und Schwellenwerte Performance-Probleme aufzeigen, erfolgt häufig eine Korrelation mit anderen Datenquellen, um die Grundursache des Problems zu ermitteln.

Internet of Things: Je intelligenter die Geräte werden, desto mehr metrikbasierte Telemetrie wird eingeführt. Metrikerfassungsprotokolle stellen eine effiziente Möglichkeit für diese Geräte dar, über ihren Status und ihre Leistung zu berichten.

DATEN ZUR PHYSISCHEN INFRASTRUKTUR

Patch-Logs

Anwendungsfälle: Sicherheit und Compliance, IT Operations

Betriebssysteme und Anwendungen mit den neuesten Bug-Fixes und Sicherheits-Patches auf dem neuesten Stand zu halten, ist eine wichtige Aufgabe, um ungeplante Ausfallzeiten, unvorhergesehene Anwendungsabstürze und Sicherheitsverletzungen zu verhindern. Handelsübliche Anwendungen und Betriebssysteme verfügen häufig über integrierte Patch-Software. Dennoch setzen Unternehmen mitunter unabhängige Patch-Management-Software ein, um die Patch-Verwaltung zu konsolidieren, die durchgängige Anwendung von Patches in ihrem gesamten Softwarebestand zu gewährleisten und um Patch-Aufträge für benutzerdefinierte, interne Anwendungen einzurichten.

Eine Patch-Verwaltungssoftware führt einen Patch-Bestand mithilfe einer Datenbank verfügbarer Updates und kann diese mit der in einem Unternehmen installierten Software abgleichen. Zu den weiteren Merkmalen gehören die zeitliche Planung von Patches, Tests und die Überprüfung nach der Installation sowie die Dokumentation der erforderlichen Systemkonfigurationen und Patch-Verfahren.

Anwendungsfälle

Sicherheit und Compliance: Sicherheitsteams können Patch-Logs verwenden, um System-Updates zu überwachen und festzustellen, welche Assets aufgrund fehlgeschlagener oder veralteter Patches gefährdet sein könnten.

IT Operations: Operations-Teams nutzen Patch-Logs, um die rechtzeitige und ordnungsgemäße Anwendung geplanter Patches zu überprüfen, nicht gepatchte Systeme und Anwendungen zu ermitteln und vor Fehlern im Patch-Prozess zu warnen. Durch die Korrelation von Fehlern mit Patch-Logs kann festgestellt werden, wann ein Fehler auf einen Patch zurückzuführen ist.

Physische Kartenleser

Anwendungsfall: Sicherheit und Compliance

Die meisten Organisationen setzen automatisierte Systeme ein, um den physischen Zugang zu Gebäuden zu gewährleisten. In der Vergangenheit handelte es sich dabei um einfache Magnetstreifen, die auf Mitarbeiterausweisen angebracht waren. An Standorten mit strengen Sicherheitsanforderungen kann jedoch eine Form von biometrischem Lesegerät oder digitalem Schlüssel zum Einsatz kommen. Unabhängig von der Technologie vergleichen die Systeme die Identität einer Person mit einer Datenbank und öffnen Türen, sofern der Benutzer berechtigt ist, einen bestimmten Ort zu betreten. Als digitale Systeme zeichnen Sicherheitsausweisleser Informationen wie Benutzer-ID, Datum und Uhrzeit des Eintritts und eventuell ein Foto bei jedem Zugangsversuch auf.

Anwendungsfälle

Sicherheit und Compliance: IT-Sicherheitsteams erhalten durch die Daten von Kartenlesegeräten die gleiche Art von Zugangs-informationen für physische Standorte wie über das Log einer Netzwerk-Firewall. Mit den Daten können Eindringversuche aufgedeckt und mit System- und Netzwerk-Logs korreliert werden, um potenzielle Insider-Bedrohungen zu erkennen und ein Bewusstsein für die Gesamtsituation zu schaffen. Sie können ebenfalls zum Erkennen von Zugängen zu ungewöhnlichen Zeiten, mit ungewöhnlicher Dauer und an ungewöhnlichen Orten dienen.

Point-of-Sale-Systeme (POS)

Anwendungsfälle: Sicherheit und Compliance, Internet of Things, Business Analytics

Beispiele: IBM, LightSpeed, NCR, Revel Systems, Square, Toshiba, Vend

Point-of-Sale-Systeme sind meist mit Transaktionen verbunden, die in Einzelhandelsfilialen generiert werden. Dank des Aufkommens mobiler POS-Lösungen werden mehr und mehr dieser Systeme an temporären Orten bereitgestellt – wie z. B. auf Volksfesten oder bei schulischen Veranstaltungen.

Ein typisches POS-System umfasst eine Registrierkasse, die auf einem PC oder eingebetteten System aufsetzt, einen Monitor, einen Belegdrucker, ein Display, einen Strichcodescanner und ein Debit-/Kreditkartenlesegerät. Von POS-Systemen generierte Maschinendaten bieten Unternehmen einen umfassenden Echtzeit-Einblick in beispielsweise die Verkaufszahlen, den pro Transaktion generierten Betrag und die verwendeten Zahlungsmethoden.

Anwendungsfälle

Sicherheit und Compliance: POS-Systeme werden in der Regel für Finanztransaktionen verwendet und sind oft Ziel von Angriffen, da sie Konto-, Zahlungs- und Finanzdaten enthalten. Da die POS-Transaktionsdaten aufgrund ihres Wertes bei Angreifern sehr begehrt sind und das POS-System als Eintrittspunkt in das Netzwerk genutzt werden kann, müssen diese Systeme unbedingt geschützt werden. Darüber hinaus sind POS-Systeme in der Regel unbemannt, sie arbeiten mit einem zugrunde liegenden Betriebssystem und die Versionsverwaltung bzw. das Monitoring gehören in der Regel nicht in den Zuständigkeitsbereich der IT-Abteilung – das alles erschwert die Absicherung zusätzlich. Die Transparenz und Analyse von POS-Systemen und -Daten kann Erkenntnisse liefern, die für den Schutz von Finanzdaten, die Aufdeckung von Betrugsversuchen und die Beseitigung von Schwachstellen entscheidend sind.

Internet of Things: In der Vergangenheit waren POS-Systeme entweder nicht vernetzt oder wurden in einem dedizierten privaten Netzwerk verwaltet. Dank des Aufschwungs des IoT werden diese Systeme nun direkt mit Cloud-Plattformen verbunden, was die Remote-Verwaltung dieser Geräte an einem zentralen Standort erheblich vereinfacht. Es ist nicht mehr erforderlich, IT-Personal für die manuelle Aktualisierung der einzelnen Systeme zu entsenden. Dies ist insofern entscheidend, als ein POS-Ausfall längere Warteschlangen zur Folge hat, die das Kundenerlebnis beinträchtigen und möglicherweise zu Umsatzverlusten führen. Eine negative Kundenerfahrung in einer wettbewerbsintensiven Branche wie dem Einzelhandel kann leicht dazu führen, dass sich Kunden dafür entscheiden, woanders einzukaufen.

Business Analytics: POS-Systeme enthalten Informationen über verkaufte Artikel, Zahlungsmittel und das Verkaufstempo. Unternehmen können anhand dieser Daten den Umsatz in Echtzeit überwachen. Dies kann dazu beitragen, Kunden gezielter anzusprechen, die Produktplatzierung und den Absatz in einer Filiale zu verfolgen oder potenziell betrügerische Transaktionen sofort aufzudecken. Diese Art der Big Data-Echtzeitanalyse kann einen tiefgreifenden Einfluss auf die Cross- und Up-Selling-Möglichkeiten haben. POS-Daten liefern auch Einblicke in die Kundenerfahrung und geben z. B. Antworten auf die Fragen, welche Coupons am beliebtesten sind oder welche Kombinationen von Produkten zusammen verkauft werden. Werden diese Informationen mit Geolokalisierungsdaten angereichert, können zudem wertvolle Erkenntnisse anhand standortbezogener Analysen gewonnen werden.

RFID/NFC/BLE

Anwendungsfälle: Internet of Things, Business Analytics

Beispiele: Alien Technology, BluVision, CheckPoint Systems, Gimbal, MonsoonRF, Radius Networks, STMicroelectronics, TAGSYS RFID, ThingMagic

Die beiden primären drahtlosen Methoden, die Unternehmen heute zur Nachverfolgung von Objekten und zur Interaktion mit Kunden in Ladengeschäften einsetzen, sind zwei verschiedene Arten drahtloser Kommunikationstechnologien. Die bekanntere ist RFID (Radio Frequency Identification), bei der Tags verwendet werden, in denen Informationen – z. B. Produktinformationen oder welche Waren in einen Schiffscontainer verladen werden könnten – gespeichert sind.

Parallel dazu führen Unternehmen Funklösungen nach dem BLE-Standard (Bluetooth Low Energy) ein, die Signale an andere Geräte übertragen können. BLE wird am häufigsten in Beacons verwendet, die z. B. eingesetzt werden, um Käufer auf ihren Smartphones über neue Angebote in Filialen oder Fans über etwaige Events während einer Sportveranstaltung zu informieren.

Anwendungsfälle

Internet of Things: RFID ist wohl eines der ersten Beispiele einer IoT-Anwendung. RFID-Tags werden anstelle herkömmlicher Strichcode-Lesegeräte bereitgestellt und in allen Bereichen vom Warenversand bis zur Verfolgung von Nutztieren eingesetzt. IoT-Bereitstellungen erleichtern die Erfassung von RFID-Daten und das Verfolgen von Events bei allem, an das ein RFID-Tag angefügt ist. Die durch RFID gewonnenen Daten können dazu beitragen, die gesamte Lieferkette, die Auftragsabwicklung und die Bestandsführung zu verbessern.

BLE dient derweil dazu, Kunden direkter anzusprechen, wenn sie sich an einem bestimmten Ort bewegen. Dadurch werden Daten erzeugt, die zur Optimierung der Kundenerfahrung genutzt werden können.

Business Analytics: Ganz gleich, ob es sich um Bestände handelt, die mit RFID-Tags verfolgt werden, oder um Kunden und Mitarbeiter, die sich an bestimmten Orten bewegen – neue Arten von Analyse-anwendungen nutzen die von diesen Geräten generierten Daten, um nahezu in Echtzeit konkrete Geschäftserkenntnisse zu liefern. Einzelhändler können diese Daten für verschiedene Zwecke nutzen, z. B. um sicherzustellen, dass sich der Lagerbestand so nahe wie möglich an den Standorten befindet, an denen Kunden am ehesten kaufen würden.

Sensordaten

Anwendungsfälle: Sicherheit und Compliance, IT Operations, Internet of Things, Business Analytics

Beispiele: Binäre und numerische Werte einschließlich Schalterzustand, Temperatur, Druck, Frequenz, Durchfluss, von MQTT-, AMQP- und CoAP-Brokern, HTTP-Ereignissammlung

Industrieanlagen, Sensoren und andere Geräte haben oft eingebaute Prozessoren und Netzwerktechnik, mit deren Hilfe sie eine Vielzahl von Informationen über Betriebsbedingungen aufzeichnen und übertragen können. Unabhängig vom Gerät liefern ihre Daten ungeahnte Details zu Leistungsparametern und Anomalien, die auf größere Probleme hinweisen können – zum Beispiel bei einem Gerät, das ausfallgefährdet ist oder Probleme mit einem anderen System aufweist. Das Aggregieren und Korrelieren von Daten von mehreren Geräten und Subsystemen liefert ein vollständiges Bild der Leistung von Anlagen, Systemen, Fabriken oder Gebäuden.

Anwendungsfälle

Sicherheit und Compliance: Sensordaten können dazu beitragen, unternehmenskritische Anlagen und Industriesysteme vor Cyberangriffen und Sicherheitsbedrohungen zu schützen. Das gelingt, indem sie Einblick in die Systemleistung oder Sollwerte geben, die Maschinen oder Menschen gefährden könnten. Die Daten können auch verwendet werden, um Anforderungen an die Berichterstattung zur Compliance zu erfüllen.

IT Operations: Einige der wichtigsten zu überwachenden Parameter für Operations-Teams sind Umgebungsbedingungen wie Temperatur, Feuchtigkeit, Luftstrom und Spannungsregelung in einem Rechenzentrum. Ähnliche Messwerte sind von einzelnen Servern und Netzwerkgeräten verfügbar, die bei entsprechender Korrelation Probleme in der Anlage oder ausfallgefährdete Geräte anzeigen können.

Weitere Anwendungsfälle

Vorbeugende Wartungsmaßnahmen und Asset Lifecycle Management: Sensordaten können Einblicke in die Bereitstellung und Nutzung von Anlagen sowie in den Ressourcenverbrauch liefern. Betriebsdaten können außerdem genutzt werden, um die langfristige Verwaltung, Wartung und Leistung von Anlagen aktiv zu beeinflussen.

Monitoring und Diagnose: Monitoring-Sensoren können sicherstellen, dass Geräte am Einsatzort wie vorgesehen funktionieren, z. B. bei der Überwachung und Verfolgung ungeplanter Geräte- oder Systemausfälle. Die Daten können auch herangezogen werden, um die Fehlerursache bei einem Gerät zu verstehen, um die Effizienz und Verfügbarkeit zu verbessern und um Sonderfälle und Probleme bei der Herstellung oder Bereitstellung von Geräten zu identifizieren.

DATEN ZUR PHYSISCHEN INFRASTRUKTUR

Server-Logs

Anwendungsfälle: Sicherheit und Compliance, IT Operations, Anwendungsbereitstellung

Serverbetriebssysteme zeichnen routinemäßig eine Vielzahl von Betriebs-, Sicherheits-, Fehler- und Debugging-Daten auf. Dazu zählen z. B. beim Systemstart geladene Systembibliotheken, offene Anwendungsprozesse, Netzwerkverbindungen, eingebundene Dateisysteme und die Auslastung des Systemspeichers. Der Detailgrad kann vom Systemadministrator konfiguriert werden. Es gibt jedoch genügend Optionen, um sich ein vollständiges Bild der Systemaktivität während der gesamten Betriebsdauer zu verschaffen. Je nach Subsystem sind Server-Logs für System-, Netzwerk-, Speicher- und Sicherheitsteams nützlich.

Anwendungsfälle

Sicherheit und Compliance: Server-Logs enthalten Daten von Sicherheits-Subsystemen wie der lokalen Firewall sowie zu Anmeldeversuchen und Dateizugriffsfehlern. Diese Daten können die Sicherheitsteams zur Identifizierung von Angriffsversuchen, zur Nachverfolgung erfolgreicher Eindringversuche in das System und zum Aufspüren von Plug-In-Schwachstellen verwenden. Das Monitoring von Server-Logs in Bezug auf Dateizugriff, Authentifizierung und Anwendungsnutzung kann zur Absicherung von Infrastrukturkomponenten beitragen.

Anwendungsbereitstellung und IT Operations: Server-Logs liefern detaillierte Aufzeichnungen zur allgemeinen Integrität des Systems sowie forensische Informationen zum genauen Zeitpunkt von Fehlern und anomalen Bedingungen. Diese Daten sind bei der Suche nach der Ursache von Systemproblemen von unschätzbarem Wert.

Intelligente Zähler

Anwendungsfälle: Internet of Things, Business Analytics

Beispiele: ABB, GE, Google, eMeter, IBM, Itron, Schneider Electric, Siemens

Intelligente Zähler (Smart Meters) zeichnen den Verbrauch von Energie, Wasser oder Erdgas so auf, dass die Informationen kontinuierlich verarbeitet und weitergegeben werden können. Üblicherweise ermöglichen intelligente Zähler eine bidirektionale Kommunikation in Echtzeit, sodass Messgeräte angepasst werden können.

Anwendungsfälle

Internet of Things: Intelligente Zähler sind in wichtigen Systemen großer Versorgungsunternehmen verteilt, z. B. bei Strom-, Gas- und Wasserversorgern. Diese Systeme sind das Lebenselixier der Infrastruktur, ihr Ausfall kann katastrophale Folgen nach sich ziehen. Das Echtzeit-Monitoring intelligenter Zähler kann Unternehmen dabei helfen, Störungen aus der Ferne besser zu analysieren, nachdem Ausfälle in Leitungen erkannt wurden. Ebenso wichtig ist es, die Geräte vor Manipulationen zu schützen, die zu böswilligen Angriffen und Sicherheitsverstößen führen könnten.

Energie- und Wasserversorger setzen in großem Umfang intelligente Sensoren ein, um alles von den Ölreserven bis zur Qualität der Wasserversorgung nachvollziehen zu können.

Business Analytics: In einer Vielzahl von Branchen werden die von intelligenten Zählern gesammelten Daten analysiert, um den Service zu optimieren. So muss z. B. ein Öl- oder Gasversorgungsunternehmen keinen Mitarbeiter mehr zum Kunden schicken, um einen Zähler abzulesen. Der Versorger weiß bereits, wie viel verbraucht wurde und wie viel noch übrig ist.

Intelligente Zähler werden in Zukunft in vielen Bereichen eingesetzt werden – von modernen Verkehrsleitsystemen bis zu Verteidigungssystemen zum Schutz wichtiger Infrastrukturen. Durch das Sammeln von Daten mit diesen intelligenten Zählern können Versorger entscheidende Einblicke in die Nachfrage gewinnen. Stark regulierte Versorger müssen bei Ereignissen zur Reaktion auf die Nachfrage festgelegte Leistungsvereinbarungen einhalten. Maschinendaten intelligenter Computer können Aufschluss über das Verhalten der Versorger geben.

Datenspeicher

Anwendungsfall: IT Operations

Beispiele: EMC, NetApp, IBM, Amazon EBS

Datenspeicher wird in Rechenzentren im Allgemeinen auf zwei Arten bereitgestellt: entweder in Server eingebaut und über verschiedene Netzwerkspeicherprotokolle gemeinsam genutzt oder über ein dediziertes Speicher-Array, das die Kapazität für die Nutzung durch mehrere Anwendungen bündelt. Diese greifen dann entweder über ein dediziertes Storage Area Network (SAN) oder ein Ethernet-LAN-basiertes File-Sharing-Protokoll darauf zu. Die Aktivität des internen, serverbasierten Speichers wird in der Regel in System-Logs aufgezeichnet. Speicher-Arrays verfügen jedoch über interne Controller/Speicherprozessoren, die ein speicheroptimiertes Betriebssystem ausführen und eine Fülle von Betriebs-, Fehler- und Nutzungsdaten protokollieren. Da viele Organisationen über mehrere solcher Arrays verfügen, werden die Logs oft von einem Speicherverwaltungssystem zusammengeführt, das über die gesamte Aktivität und Kapazität berichten kann.

Anwendungsfälle

IT Operations: Gemeinsam genutzte Speicher-Logs zeichnen die gesamte Integrität des Systems (sowohl Hardware als auch Software), Fehlerbedingungen (wie der Ausfall eines Controllers, einer Netzwerkschnittstelle oder von Datenträgern) und die Nutzung (sowohl die pro Datenträger genutzte Kapazität als auch Datei- oder Volume-Zugriffe) auf. Zusammengenommen können die Informationen Operations-Teams vor Problemen, bei Kapazitätsbedarf und bei Leistungsengpässen warnen.

Telefonie

Anwendungsfälle: IT Operations

Beispiele: Cisco Unified Communications Manager, Shoretel, Twilio

Geschäftliche Kommunikation in Echtzeit ist nicht mehr auf Sprachanrufe beschränkt, die über das analoge Festnetz getätigt werden. Stattdessen sind Sprach-, Video- und SMS-Nachrichten sowie Webkonferenzen nun IP-Anwendungen, die über bestehende Unternehmensnetze übertragen werden. Im Gegensatz zu konventionellen Client/Server- oder Webanwendungen stellen Telefonie- und andere Kommunikationsanwendungen strenge Anforderungen an Netzqualität, Latenz und Paketverluste, wodurch die Servicequalität und Zuverlässigkeit viel empfindlicher auf die Netzbedingungen und Reaktionsfähigkeit von Servern reagieren. Das traditionelle analoge Festnetz hat die Menschen daran gewöhnt, ein sofortiges klares Freizeichen zu erhalten, sobald sie den Hörer abnehmen, sodass sie sich vom Rauschen, Echo oder von anderen Problemen, die die IP-Telefonie mit sich bringen kann, gestört fühlen. Daher müssen die Systeme und die unterstützende Infrastruktur sorgfältig beaufsichtigt und verwaltet werden, um entsprechende Qualität und Zuverlässigkeit zu gewährleisten.

Anwendungsfälle

IT Operations: Wie bei VoIP bieten Telefonie-Logs ähnlich wie andere Netzwerkanwendungen einen Überblick über die Systemintegrität einschließlich Problembehandlungs- und Nutzungsdaten. Im Detail umfassen diese Daten Quelle, Ziel, Zeit und Dauer von Sprach-/Videoanrufen, Webkonferenzen und Textnachrichten, Metriken zur Anrufqualität (z. B. Paketverlust, Latenz, Klangtreue/Bitrate), Fehlerbedingungen und die Teilnehmerzahl bei Webkonferenzen. Durch die Integration von Telefonieaufzeichnungen der Quell-/Zieladresse mit einer Mitarbeiterdatenbank wie AD oder LDAP und einer DHCP-Datenbank können Unternehmen Anrufaufzeichnungen mit tatsächlichen Benutzer-IDs und IP-Adressen mit physischen Standorten verknüpfen. Diese Daten können bei der Problembehandlung und Abrechnung hilfreich sein. Anhand von Logs können auch Netzwerksegmente mit Engpässen oder anderen Leistungsproblemen ermittelt werden, die auf Geräteprobleme oder die Notwendigkeit eines Upgrades hinweisen.

Verkehr

Anwendungsfälle: Internet of Things, Business Analytics

Beispiele: Boeing, BMW, Ford, GE, General Motors, Daimler-Benz, John Deere, Volkswagen

Fahrzeuge aller Größen und Typen generieren täglich riesige Mengen an Maschinendaten. Diese können genutzt werden, um in Echtzeit einen Einblick in die Integrität und Leistung eines Verkehrsmittels zu erhalten und Anwendungen für die vorbeugende Wartung (Predictive Maintenance) voranzutreiben. Mit diesen Daten ausgestattet kann ein Flugzeug- oder Automobilhersteller ein Instandhaltungsprogramm verfolgen, das datengesteuert und nicht „nach Schema F" umgesetzt wird.

Dank dieser Informationen können dann beispielsweise Verfügbarkeit und Zuverlässigkeit verbessert und die Lebensdauer eines wenig genutzten Verkehrsmittels verlängert werden. Oder es lassen sich umgekehrt Komponenten, die bereits vorzeitig stark strapaziert wurden, ersetzen.

Anwendungsfälle

Internet of Things: Hersteller von Verkehrsmitteln versehen jede von ihnen verwendete mechanische und elektronische Komponente mit Sensoren. Auf diese Weise können Unternehmen sich einen einheitlichen Überblick über ihre Assets verschaffen, um Betriebsprobleme schnell zu erkennen und zu diagnostizieren und ungeplante Asset-Downtimes zu überwachen, zu verfolgen und zu vermeiden. Dadurch wird sichergestellt, dass alles wie vorgesehen funktionieren. Sie können auch Anomalien und Abweichungen vom normalen Verhalten erkennen, um frühzeitig Gegenmaßnahmen zu ergreifen und damit die Betriebszeit, Zuverlässigkeit und Langlebigkeit der Assets zu erhöhen.

Business Analytics: Dank des Zugriffs auf Maschinendaten können Hersteller von Verkehrsmitteln Analysen auf eine Art und Weise durchführen, die ihre Geschäftsmodelle grundlegend verändert. Statt ein Verkehrsmittel zu verkaufen, ziehen es die Hersteller zunehmend vor, dieses auf Grundlage der tatsächlichen Nutzung zu verleasen. Je länger das Verkehrsmittel zwischen Reparaturen genutzt werden kann, desto rentabler wird dieser Leasing-Service. Der Schlüssel zu einer wirtschaftlich sinnvollen Bereitstellung dieser Art von Service ist eine fortschrittliche Analysemethode, die auf alle gesammelten Daten angewendet wird.

Wearables

Anwendungsfälle: Internet of Things, Business Analytics

Beispiele: ARM, Intel, Lenovo, Microsoft, Samsung

Von Smartwatches, die gleichzeitig als Hilfsmittel im Bereich Fitness dienen, bis hin zu medizinischen Geräten, mit denen Ärzte lebenswichtige Werte aus der Ferne überwachen können, haben sich Wearables bewiesenermaßen etabliert. Wearables gehören zu den offensichtlichsten Bestandteilen des Internet of Things.

Anwendungsfälle

Internet of Things: Über die bloße Synchronisierung mit Smartphones hinaus nutzt die neueste Generation von Smartwatches die Vorteile von Systemen zur Geolokalisierung und APIs (Application Programming Interfaces), um Gerätebesitzern ein optimales Anwendungserlebnis zu bieten, das sowohl ihren Standort als auch häufig die Tageszeit berücksichtigt.

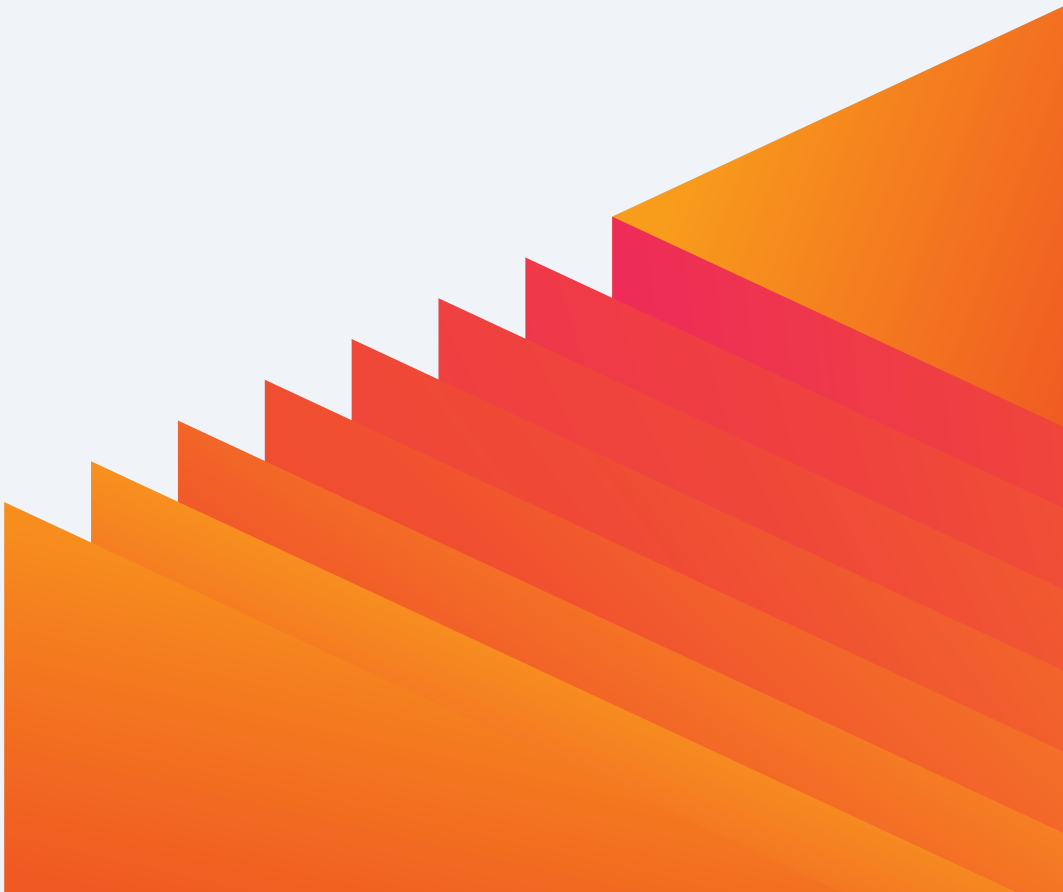
In Zukunft wird es bald ganz neue Arten von Wearables geben, die alles von Virtual-Reality-Anwendungen, welche über ein Headset übertragen werden, bis hin zu Sensoren, welche auf noch nie dagewesene Art und Weise eingebettet sind, nutzen und verarbeiten können.

Business Analytics: Da immer weniger Verbraucher ein Problem mit dem Teilen von Daten über Wearables haben, erleben viele die Leistungsfähigkeit von Analysen aus erster Hand. Entwickler von für Wearables optimierten Anwendungen geben Empfehlungen zu unterschiedlichsten Fragen, wie z. B. „Wie kann die Lebenserwartung verbessert werden?" oder „Wo ist das nächste Restaurant zu finden?". Analysedaten von Wearables können dazu beitragen, die Benutzererfahrung zu verbessern und Produktinnovationen voranzutreiben. Zum Beispiel können Produktmanager verstehen, wie Verbraucher mit Geräten interagieren, um so bessere Features zu entwickeln.

Über **Splunk**

Splunk verwandelt mit der Data-to-Everything™ Plattform Daten in Taten. Mit der Splunk-Technologie können Kunden Daten jeder Art und Größe untersuchen, überwachen, analysieren und als Basis für konkrete Handlungen nutzbar machen. Schließen Sie sich jetzt Millionen begeisterter Nutzer an und testen Sie Splunk gratis.

Kostenlose Testversion



splunk>

20-13476-SPLK-Essential-Guide-to-Data-Infrastructure-Data-104