

# Observability:

Ein Leitfaden für Einsteiger

Komplexität durchdringen und wissen,  
was Systeme, Dienste und Apps  
wirklich tun



**splunk**>  
turn data into doing™



Observability wurde schon vieles genannt, vom trendigen Buzzword bis hin zu „Monitoring auf Anabolika“, das man unbedingt haben muss. Die Wahrheit ist vielschichtiger – vor allem angesichts der gestiegenen Komplexität moderner Infrastrukturen und der unbestrittenen Notwendigkeit von besserem Monitoring über den gesamten Stack hinweg. Microservices, Containerisierung, Serverless Computing – all das treibt das Entwicklungstempo an und bietet wichtige geschäftliche Vorteile, erhöht aber auch die Komplexität und verringert die Transparenz.

Ein einfacher Service mit drei Ebenen von früher kann heute von bis zu 50 Microservices ausgeführt werden, die bei mehreren Cloud-Anbietern bereitgestellt sind. Hinter einigen „Microservices“ verbergen sich tatsächlich Aufrufe von serverlosen Funktionen. Dies erschwert die Beobachtung Ihrer gesamten Anwendung erheblich.

Außerdem haben sich die Teams, die operative Transparenz benötigen, über Sysadmins und ITOps-Analysten hinaus erweitert. Bei modernen DevOps-Modellen übernehmen die Entwickler mehr Verantwortung für die operativen Vorgänge, um ein besseres Kundenerlebnis zu schaffen. Um dies effektiv umzusetzen, benötigen alle Rollen Einblick in ihre gesamte Architektur – von der Infrastruktur über Anwendungen bis hin zu externen Drittanbieter-APIs – um Probleme zu beheben (und im Idealfall zu vermeiden).

Observability geht über bloßes Monitoring (selbst sehr komplizierter Infrastrukturen) hinaus und zielt stattdessen auf die Schaffung von Transparenz in jeder Ebene Ihres Unternehmens ab. Die gesteigerte Transparenz ermöglicht allen Beteiligten einen besseren Einblick in die Probleme und das Benutzererlebnis und schafft mehr Zeit für strategische Initiativen statt für die Bekämpfung von Problemen. Sie ist auch ein wesentlicher Baustein für den Erfolg von Site Reliability Engineering (SRE) oder DevOps-Organisationsmodellen. In modernen DevOps-Entwicklungsprozessen benötigen Entwickler ebenso Einblicke in die operative Performance wie herkömmliche Ops-Teams oder SREs.

In diesem Leitfaden wollen wir definieren, was Observability ist und was erforderlich ist, um sie zu erreichen. Außerdem finden Sie hier Beispiele zu Observability in der Praxis und Hinweise dazu, wie eine Lösung aussieht, die das Erreichen von Observability in Ihrem Unternehmen ermöglicht.





## Inhalt

KAPITEL 1	
Observability: Was sie ist und was nicht.....	5
KAPITEL 2	
Die Roadmap zu Observability.....	8
KAPITEL 3	
Observability in der Praxis .....	15
KAPITEL 4	
Optionen für Observability.....	23



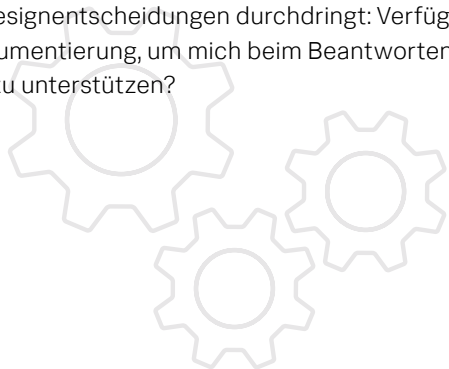
# Observability: Was sie ist und was nicht

## EINLEITUNG

### Integrieren von Feedback

Einfach ausgedrückt, ist Observability die Fähigkeit, jederzeit jede Frage zu Ihrem Unternehmen oder Ihrer Anwendung zu beantworten, unabhängig von der Komplexität Ihrer Infrastruktur. Die Umsetzung im Kontext der Anwendungsentwicklung und des Anwendungsbetriebs ist einfach – Sie instrumentieren Systeme und Anwendungen, um Metriken, Traces und Logs zu erfassen, und senden alle diese Daten an ein System, das sie speichern und analysieren und Ihnen so helfen kann, Erkenntnisse zu gewinnen.

Wesentliche Voraussetzung für Observability ist es, beim Erstellen von Apps den Gedanken zugrunde zu legen, dass sie von jemandem beobachtet werden. Die klassische Definition von Observability kommt aus der Systemsteuerungstheorie, in der Observability ein Maß dafür darstellt, wie gut sich die internen Zustände eines Systems aus der Kenntnis seiner externen Ausgaben erschließen lassen – eine Art digitaler Abluft. Stellen Sie es sich als eine Eigenschaft eines Systems vor – ein weiteres Attribut, wie Funktionalität, Leistung oder Testbarkeit. Sie können sich das auch als eine Denkweise vorstellen, die Designentscheidungen durchdringt: Verfügt mein System über die richtige Instrumentierung, um mich beim Beantworten von Fragen zu seiner Leistung zu unterstützen?



„Bei Observability geht es darum, Antworten auf Fragen zu erhalten, von denen wir nicht wussten, dass wir sie stellen müssen. Wenn ich über Observability nachdenke, denke ich Top-Down und Bottom-Up. Es sind die verwertbaren Erkenntnisse, die Sie aus dem gesamten System erfassen, nicht nur aus einem Teil, die Ihnen Aufschluss über den Zustand Ihrer Umgebung geben.“

– Brent Miller, Senior Director Cloud Operations, Quantum Metric



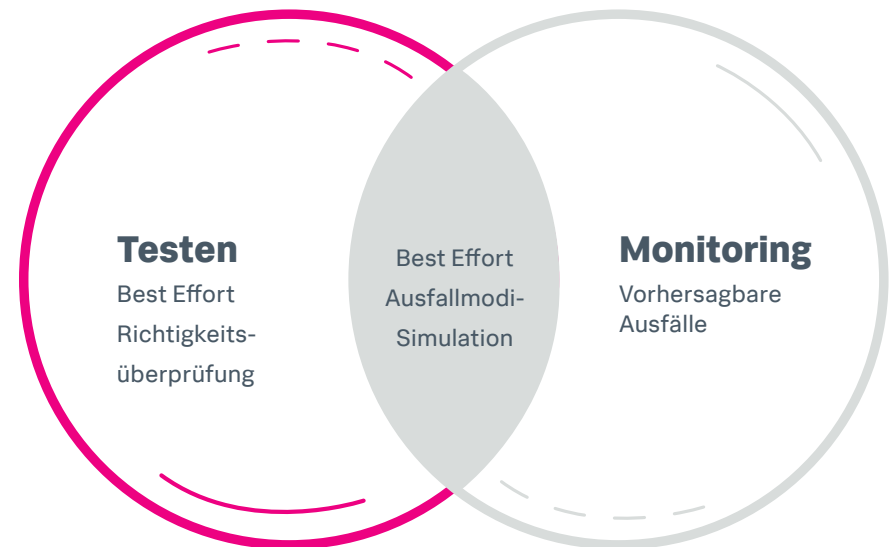
## Monitoring vs. Observability

Monitoring	Observability
Zeigt Ihnen, <i>ob</i> das System funktioniert	Lässt Sie die Frage stellen, <i>warum</i> es nicht funktioniert.
Die Erfassung von Metriken und Logs aus einem System	Die nützlichen Erkenntnisse, die aus diesen Daten gewonnen werden
Fehlerzentriert	Interessiert sich für das Gesamtverhalten des Systems
Ist „das Wie“ / etwas, das Sie tun	Ist „der Prozess“ / etwas, das Sie besitzen
Ich <i>überwache</i> Sie	Sie <i>machen sich selbst</i> beobachtbar



## Observability

Alle möglichen Permutationen von Voll- und Teilausfall





## Observability als Mindset

Monitoring ist etwas Notwendiges, aber nicht ausreichend zur Schaffung von Observability, durch die erst die „new Unknowns“ aus neuen Technologien wie Microservices oder Containern identifiziert werden können. Während Sie neue (System-)Monitore zu entwickeln, haben Sie vermutlich bereits auch eine Art Observability-Mindset entwickelt. Es ist wichtig, zu begreifen, dass es kein bestimmtes Tool gibt, das Ihnen auf magische Weise Observability verleiht – Observability ist eine Denkweise, kein Ergebnis.

Observability als Denkweise oder Mindset stellt den Grad dar, in dem ein Team oder ein Unternehmen Wert auf die Fähigkeit legt, Systeme, ihre Arbeitslast und ihr Verhalten zu untersuchen und zu verstehen. Observability geht über die Betrachtung einzelner Komponenten des Systems hinaus und betrachtet die Ergebnisse des Systems als Ganzes.

### Vorteile von Observability

- **Umfassendes Verständnis** von komplexen Systemen
- **Intelligentere** Planung von Codereleases und der Anwendungskapazität
- **Schnellere** Problemlösung und kürzere MTTR
- **Aufschlussreichere** Vorfallsberichte
- **Bessere** Betriebszeit und Leistung



- **Zufriedenere** Kunden und mehr Umsatz

Die Moderne Infrastruktur hat sich von einer Monitoringmentalität hin zu einer auf Observability basierenden Denkweise entwickelt. Früher war es wichtig, den Zustand der einzelnen Dienste zu überwachen, da ein Dienst für den größten Teil der Benutzererfahrung verantwortlich war. In modernen Anwendungen werden viele Dienste verwendet, um das Benutzererlebnis zu gewährleisten. Wenn eine Instanz eines Dienstes ein Problem hat, ist das keine große Sache, solange der Benutzer immer noch tun kann, was er möchte. Wenn Sie ein Observability-Mindset besitzen, achten Sie auf das Gesamtsystem und die User Experience, nicht auf jede einzelne Komponente davon. Observability hilft Ihnen, sich auf das zu konzentrieren, was wirklich wichtig ist.

„Observability ist nicht das Mikroskop. Sie ist die Transparenz des Objektträgers unter dem Mikroskop.“

– Baron Schwartz



# Die Roadmap zu Observability

## Säulen der Observability

Es gibt drei Säulen, auf die sich Observability stützt. Mehr Daten sind immer besser, aber ohne diese Säulen wird es schwierig, die Vorteile von Observability zu nutzen:



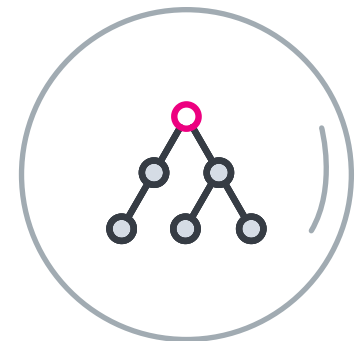
### Logs/Events

Unveränderliche Aufzeichnungen diskreter Events, die sich über einen gewissen Zeitraum ereignen



### Metriken

Zahlen, die einen bestimmten Prozess oder eine bestimmte Aktivität beschreiben, der/die über Zeitintervalle gemessen wird



### Traces

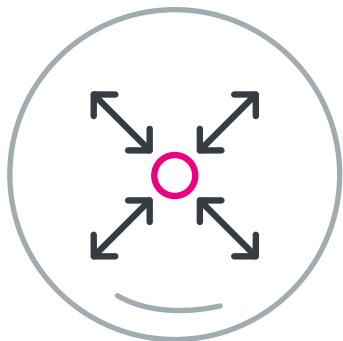
Daten, die für jeden Aufruf jedes nachgelagerten Services zeigen, welche Instanz und welche Methode innerhalb dieser Instanz aufgerufen wurde, mit welcher Leistung die Anfrage ausgeführt wurde und welche Ergebnisse sie erbrachte





# Moderne Event-Handling-Techniken

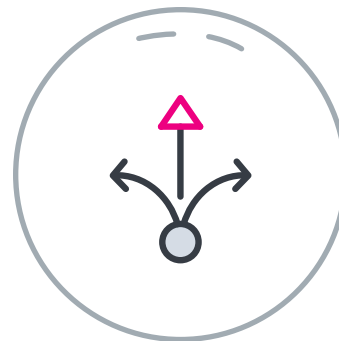
Die Verarbeitung der gesammelten Daten zu Informationen und Erkenntnissen, die Observability ermöglichen, erleichtert eine Reihe von Dingen, insbesondere die gemeinsame Nutzung von Erkenntnissen, eine kollaborative Reaktion auf Vorfälle, eine datengestützte Entwicklung und intelligente Betriebsabläufe. Damit Sie diese Vorzüge nutzen können, benötigen Sie ein System, das eben diese Dinge erledigen kann:



## Sammeln aller Daten

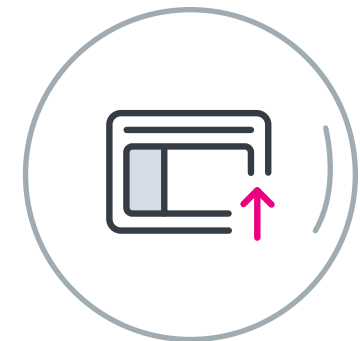
Sie müssen in der Lage sein, über Stacks, Technologien und alle Umgebungen hinweg zu sehen:

- Cloud-nativ (Container, Cloud, serverless)
- Herkömmlich (selbstgehostet, lokal gehostet, monolithisch)
- Unterstützung für alle von Ihnen verwendeten Sprachen und Frameworks



## Analysieren und Deduplizieren

- Trennen aussagekräftiger Signale vom Rauschen
- Speichern von Statistiken über Ihre Daten zum Zeitpunkt der Erfassung, um schneller zu Benachrichtigungen und Erkenntnissen zu gelangen
- Automatische Erkennung von Ausreißern oder anderen Anomalien



## Hinzufügen von Kontext

- Zeigen Sie dem antwortenden Techniker, was er benötigt, um das Problem schnell zu beheben
- Minimieren Sie Ausfallzeiten, indem Sie zugehörige Daten zu Incidents mit einem Klick anzeigen
- Bestimmen Sie die Auswirkungen von Codebereitstellungen auf wichtige Metriken



## Die Rolle von KI und ML

Der Umfang, die Geschwindigkeit und die Vielfalt der Daten, die benötigt werden, um jede Frage über Ihr Unternehmen zu beantworten, sind riesig – und im Grunde von Menschen nicht zu bewältigen. So schlagwortartig es auch anmuten mag, um wirklich Observability zu erreichen, sind ausgefeilte Analysetechniken mit künstlicher Intelligenz (KI) und Machine Learning (ML) unerlässlich.

Hochwertige Observability-Systeme verfügen über Lernalgorithmen, die den Zustand Ihrer Services und Anwendungen in der Vergangenheit verstehen können, um die Vorhersage der kommenden Ereignisse zu unterstützen. Die vollständige Einbeziehung aller Daten über Ihr Unternehmen hilft Machine-Learning-Modellen dabei, genaue Perspektiven von historischen und Echtzeitdaten zu erhalten – ML hilft bei der Vorhersage von hoch wahrscheinlichen, potenziellen zukünftigen Ereignissen und nutzt die Leistung von KI, um Predictive Intelligence zu erreichen.



## KI-gestützte Analysen

**Fortschritte in der KI können Ihnen folgende Vorteile bringen:**

- Reduzieren der unwesentlichen Events und False Positive-Werte durch eine multivariate Anomalieerkennung
- Automatisches Ausblenden doppelter Events, um die Konzentration auf relevante Events zu erhöhen und Over-Alerting zu vermeiden
- Einfaches Durchsuchen riesiger Mengen von Events durch Filtern, Markieren und Sortieren
- Anreichern und Hinzufügen von Kontext zu Events, um sie informativ und praktisch umsetzbar zu machen

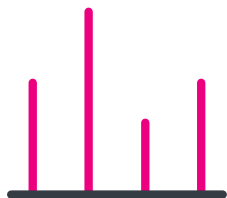
„Eine lernende Maschine ist jedes Gerät, dessen Handlungen von vergangenen Erfahrungen beeinflusst werden.“

– Nils John Nilsson



## Die wichtigsten Metriken

Analysten wie Gartner, Forrester, IDC und Computing UK haben alle eigene Sammlungen von „relevanten Metriken“ entwickelt. Aufbauend auf dieser Arbeit finden Sie nachfolgend eine Liste von Metriken und Events, die wir als entscheidend für die Erreichung von umfassender Observability erachten:



### Metriken

Zu den gängigen Metrikquellen gehören:

- Systemmetriken (CPU, Arbeitsspeicher, Festplatte)
- Infrastrukturmetriken (AWS CloudWatch)
- Skripts zur Webverfolgung (Google Analytics, Digital Experience Management)
- Anwendungs-Agents/-Kollektoren (APM, Fehlerverfolgung)
- Geschäftsmetriken (Umsatz, Kundengewinnung, Absprungrate, Aufgabe des Einkaufswagens)

1481050800



Zeitstempel

os.cpu.user



Metrikname

42.12345

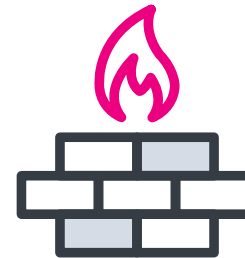


Wert

hq:us-west-1



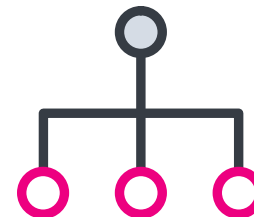
Dimensionen



### Events (Logs)

Events kommen in drei Formen vor – unformatierter Text, strukturiert und binär. Zu den gängigen Event-Quellen gehören:

- System- und Serverlogs (syslog, journald)
- Logs von Firewall und Intrusion Detection System
- Feeds aus sozialen Medien (Twitter usw.)
- Anwendungs-, Plattform- und Serverlogs (log4j, log4net, Apache, MySQL, AWS)



### Traces

Bestimmte Teile der Reise eines Benutzers werden in Traces gesammelt, die zeigen, welche Services aufgerufen wurden, auf welchen Containern/Hosts/Instanzen sie ausgeführt wurden und was die Ergebnisse der einzelnen Aufrufe waren.



## Sammeln von Observability- und Monitoring-Daten

Die gute Nachricht ist, dass es jede Menge Daten gibt – die Herausforderung besteht darin, sie zu aggregieren und aus den vielen Daten Erkenntnisse zu gewinnen. Folgend finden Sie die Typen von Datenquellen, die sich im Lauf der Jahre herausgebildet haben – sie sind alle wichtig beim Erreichen von Observability.



## Vorhandene Quellen

- Netzwerkverkehrsdaten: Router-/Switch-Leistungsindikatoren, Firewall-Logs usw.
- Virtuelle Server: VM-Logs, ESXi-Logs usw.
- Cloud-Services: AWS-Datenquellen wie etwa EC2, EMR, S3 usw.
- Docker: Loggingtreiber, syslog, Anwendungsprotokolle usw.
- Container und Microservice-Architekturen: Logs von Containern und Microservices, Containermetriken und -Events usw.
- Services von Drittanbietern: SaaS, FaaS, serverless usw.
- Steuerungssysteme: vCenter, Swarm, Kubernetes usw.
- Entwicklungsautomation: Jenkins, Sonarcube usw.
- Infra-Orchestrierung: Chef, Puppet, Ansible usw.
- Signale von mobilen Geräten: Produkteinführung, Benutzer und Clients, Annahme von Features usw.
- Metriken für die Geschäftsanalyse: App-Daten, HTTP-Events, SFA/CRM
- Signale aus der sozialen Empfindungsanalyse: Analyse von Tweets im zeitlichen Verlauf
- Analyse des Kundenerlebnisses: App-Logs, Logs von Geschäftsprozessen, Anrufdetailerfassungen usw.
- Nachrichtenbusse und Middleware



## Cloud-native Quellen

### Auf dem neuesten Stand der Technik

- OpenTelemetry: ein Framework, das sich in die meisten OSS- und kommerziellen Produkte integrieren lässt, um Metriken und Traces von in vielen Sprachen geschriebenen Anwendungen zu sammeln

### Von Cloud-Anwendern der ersten Stunde genutzt

- collectd: ein Daemon, der Metriken erfasst
- statsd: ein Daemon, der nach Statistiken sucht
- fluentd: ein Daemon, der die Erfassung von Logdaten vereinheitlicht
- Zipkin, Jaeger: Verteilte Open Source Back-End-Tracing-Systeme



Diese Deemons senden Metriken an einen definierten Speicherort, im Gegensatz zu Observability-Ansätzen, bei denen die wichtigen Metriken erstellt und definiert werden und Aktionen ausgelöst werden, wenn die Metriken ihre Grenzwerte über- oder unterschreiten.

Es ist wichtig zu beachten, dass kein Code „fertig“ ist, bevor Sie nicht die Analyse und Instrumentierung zur Unterstützung aufgebaut haben. Dies müssen Sie insbesondere deshalb im Blick behalten, da Sie einem Observability-Mindset folgen.

Ohne diese Art von Transparenz können Sie nicht bestimmen, *warum* ein System ausgefallen ist, was die Reaktion auf geschäftskritische Probleme und ihre Behebung verlangsamt.

Die richtige Instrumentierung ist entscheidend, um die aussagekräftigen Ergebnisse, die Sie sich für ein Observability-System wünschen, überhaupt erst zu erhalten. Die Einführung von OpenTelemetry kann der schnellste Weg sein, die Instrumentierung zu realisieren und die Vorteile von Observability schneller zu nutzen.



## Erforderliche Tools für Observability

Es gibt viele Lösungen, die Ihnen dabei helfen können, Erkenntnisse aus der überwältigenden Menge an disparaten Daten aus allen oben genannten Quellen zu gewinnen. Aber Sie werden wahrscheinlich feststellen, dass Sie die folgenden Tools benötigen, um alle Fragen zu Ihrer Anwendung zu beantworten und ein vollständiges End-to-End-Bild von ihr zu erhalten. Es ist wichtig, bei all diesen Tools Wert auf die größtmögliche Genauigkeit zu legen:

Tool	Zweck
Infrastructure Monitoring	Ermitteln Sie Zustand und Leistung der Container und der Umgebung, in denen Ihre Anwendungen ausgeführt werden.
Application Performance Monitoring	Untersuchen Sie das Verhalten Ihrer Anwendung auf Service-Ebene. Bestimmen Sie, wohin Aufrufe gehen und welche Leistung sie bringen.
Real User Monitoring	Verstehen Sie das Erlebnis realer Benutzer, indem Sie Daten über die Leistung und das Aussehen Ihrer Seite aus Browsern erfassen. Isolieren Sie Probleme auf das Front-End oder Back-End.
Synthetic Monitoring	Messen Sie die Auswirkungen von Releases, Drittanbieter-APIs und Netzwerkproblemen auf die Leistung und Zuverlässigkeit Ihrer App.
Log Viewing	Gehen Sie dem „Warum hinter dem Was“ auf den Grund, wenn Probleme auftreten. Finden Sie heraus, wie Sie die Probleme schnell beheben können.
Incident Response	Alarmieren Sie gleich beim ersten Mal das richtige Team, um das Problem zu beheben, und stellen Sie ihm die Daten zur Verfügung, die es dazu benötigt – alles an einem Ort.



# Observability in der Praxis

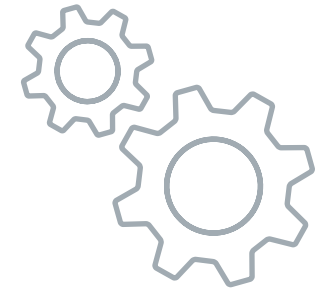
## EINLEITUNG

Jetzt, da wir über Observability und ihre Relevanz gesprochen und die Metriken und Events kennengelernt haben, auf denen sie basiert, lassen Sie uns Observability in der Praxis betrachten und herausfinden, welche Vorteile sie bringt.

Die folgenden Fallstudien präsentieren reale Kundendaten und Ergebnisse von Unternehmen, die Splunks Observability Cloud-Produkte einsetzen.



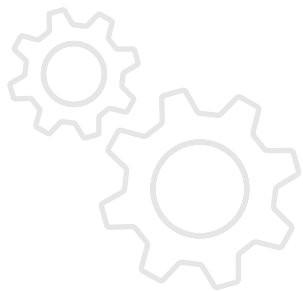




# Application Performance Monitoring

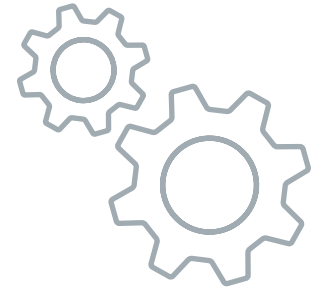
**Quantum Metric:** Das schnell wachsende Unternehmen mit Unicorn-Status, Quantum Metric, benötigte eine flexible Observability-Lösung, die alle Daten zu seiner Umgebung an einem Ort sammelt. Auf der ganzen Welt bauen Unternehmen auf Quantum Metric, um Kundeneinblicke in Echtzeit zu erhalten, z. B. wenn bei ihrer Anwendung Fehler auftreten oder die Conversion-Rates sinken. Durch die Einführung von Splunk Observability Cloud konnte Quantum Metric ein besseres Verständnis seiner komplexen Infrastruktur erlangen und darüber hinaus von folgenden Vorteilen profitieren:

- Eine bessere Downsizing-Analyse und Kapazitätsplanung führte zu Einsparungen von über 80.000 USD.
- Die Anwendungsentwicklung wurde um 96 % beschleunigt, wodurch sich die Produktivität der Entwickler erhöhte.
- Die Anzahl der ausstehenden CI-Aufgaben wurde um 95 % reduziert.
- Kundenspezifische SLOs (Service Level Objectives) mit integrierten Detektoren geben sofort Benachrichtigungen aus, wenn Probleme auftreten.



„Bei Observability geht es darum, Antworten auf Fragen zu erhalten, von denen wir nicht wussten, dass wir sie stellen müssen.“

– Eric Irwin, Director of Engineering



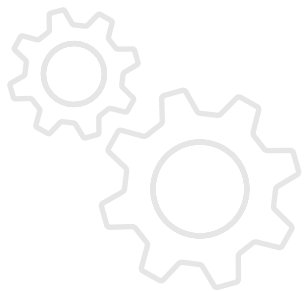
## Splunk Application Performance Monitoring

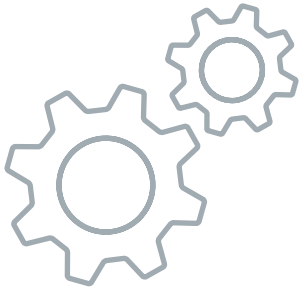
**Freecharge:** Indiens führende App für digitalen Zahlungsverkehr stieß bei der Umstellung auf eine Microservices-basierte Umgebung auf Schwierigkeiten. Zuvor waren mehrere Monitoring-Tools erforderlich, um Einblick in ihre komplexe Anwendung zu erhalten. Sie führten Splunk Application Performance Monitoring ein und konnten von den folgenden Vorteilen profitieren:

- KPI-Monitoring half dem Kundenerfolgsteam, Probleme bei Betriebszeit und Latenz 60 % schneller zu lösen.
- Mehr als tausend Compute-Instanzen wurden auf unter 700 reduziert, was zu erheblichen Kosteneinsparungen führte.
- Das Business-Team wird innerhalb von Minuten auf Probleme aufmerksam gemacht, mit den früheren Tools waren es Stunden.

„[Splunk Infrastructure Monitoring] überwacht den Herzschlag des gesamten Systems, mit dem unsere Kunden interagieren – nicht nur unsere interne Infrastruktur, sondern auch die externen Anbieter, die über APIs integriert sind. So können wir Probleme leicht lokalisieren und beheben, unabhängig davon, wo sie sich in unserem Ökosystem befinden.“

– Sachin Sharma, Senior Director, Infrastructure





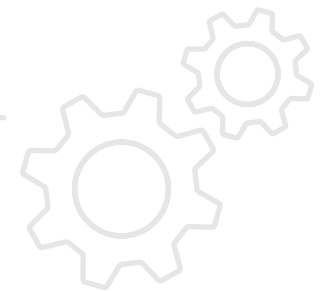
# Splunk Infrastructure Monitoring

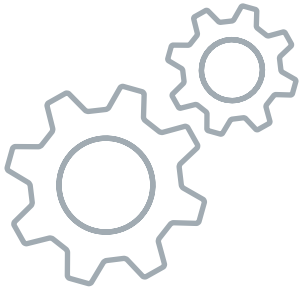
**Mark43:** Die bisherige Infrastruktur-Monitoringplattform von Mark43 war instabil und von Alarmrauschen behaftet, was die Arbeitsbelastung erhöhte und reale Probleme verdeckte. Nach der Einführung von Splunk Infrastructure Monitoring profitiert Mark43 von folgenden Vorteilen:

- Benachrichtigung über Probleme innerhalb von Sekunden, verglichen mit einer Latenz von 10 Minuten bei den bisherigen Tools.
- Verbesserungen (die bisher ein ganzes Team fast eine Stunde lang beschäftigten) können durch einen Techniker innerhalb von Minuten umgesetzt werden.
- Möglichkeit zur Behebung von Problemen, bevor sie die Arbeit der nachgelagerten Mitarbeiter beeinträchtigen, die die Plattform verwenden.

„Leistungsverbesserungen, für die früher ein ganzes Team fast eine Stunde brauchte, kann ein einzelner Techniker in wenigen Minuten erledigen.“

– Kevin Heins, DevOps Technical Lead





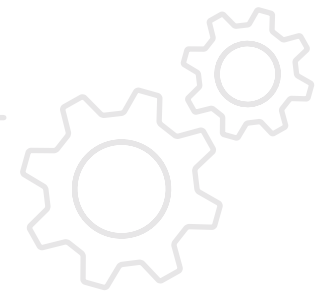
# Splunk Infrastructure Monitoring

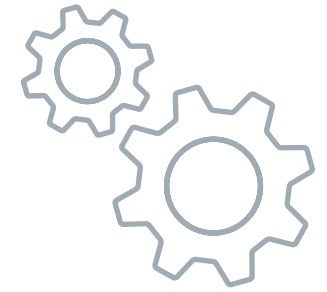
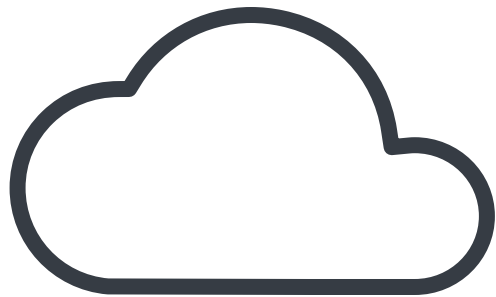
**Acquia:** Die Digital-Experience-Plattform Acquia erlebte ein explosives Wachstum und wuchs schnell über das selbst entwickelte Monitoring-System hinaus. Änderungen dauerten Wochen und überall im System fehlten Daten oder waren unvollständig. Acquia investierte erneut in seine Kernkompetenz und führte Splunk Infrastructure Monitoring ein, um diese Vorteile zu realisieren und zusätzlich umfassende Observability für mehr als 20.000 EC2-Instanzen zu erlangen:

- Die Fähigkeit, 300 Metriken mit 4-fach höherer Granularität als bisher zu senden und zu analysieren.
- Jährliche Produktivitätssteigerung in Höhe von 1 Million USD durch 26 % geringeren Zeitaufwand pro Incident.
- Jährliche Einsparungen bei der AWS-Infrastruktur in Höhe von über 600.000 USD.
- Zeitersparnis von einer Stunde pro Tag und technischem Mitarbeiter.

„Dank Splunk können wir unsere Produktentwicklung beschleunigen, die Effizienz des Supports steigern und unseren Kunden erfolgskritische Analysen zur Verfügung stellen.“

– Aaron Pacheco, Product Manager

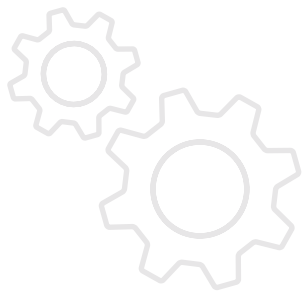


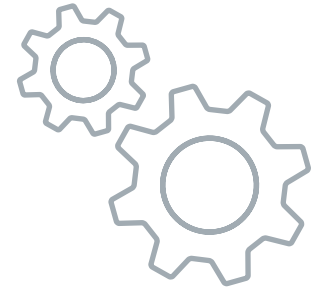


## Splunk Observability Cloud

**Atlassian:** Der branchenführende Cloud-Technologie-Anbieter Atlassian wechselte von einem Konkurrenzprodukt zu Splunk Observability Cloud, weil das Konkurrenzprodukt nicht in der von Atlassian benötigten Größenordnung betrieben werden konnte. Beanstandet wurde eine unbefriedigende Leistung, unklare Abrechnungen und ein Mangel an Transparenz bezüglich der Nutzung. Atlassian wechselte zu Splunk Observability Cloud und freut sich nun über:

- Die Bereitstellung von mehr als 1.000 hochgradig zuverlässigen Services für über 150.000 Kunden.
- Eine massive Monitoring-Infrastruktur, die über 1,5 Millionen Metriken/Sekunde und über 1.000 Dashboards und Detektoren verarbeitet.
- Ein riesiges Team von über 2.000 Entwicklern und SREs.
- Einen standardisierten Terraform-basierten Ansatz für „Observability as Code“.

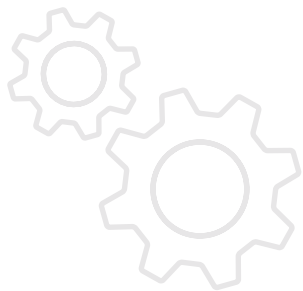


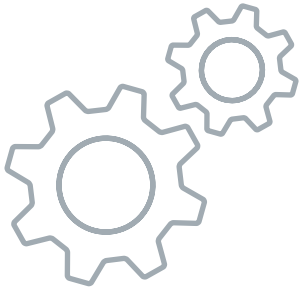


## Splunk Observability Cloud

**Rappi:** Das rasante Wachstum des größten lateinamerikanischen E-Commerce-Unternehmens Rappi in Kombination mit der Einführung von Containern und Microservices auf mehr als 6.000 Hosts überforderte die alte Monitoring-Plattform, der es an ausgefeilten und detaillierten Analysen mangelte, was zu langen Verzögerungen bei der Bereitstellung von Benachrichtigungen führte. So stellt sich die Lage für Rappi nach der Einführung von Splunk Observability Cloud dar:

- Es wurde Observability in Echtzeit für die gesamte Umgebung erreicht.
- Die MTTR in der Produktion wurde von fünf Minuten auf Sekunden reduziert.
- Der Zugriff auf komplexere Datenanalysen und die bessere Korrelation von Metriken führte zu einer kürzeren MTTR.
- Das Vertrauen in die weitere Migration zu einer Microservices- und Serverless-Architektur mit ECS, Kubernetes und AWS Lambda (mehr als 100 Services) ist gewachsen.





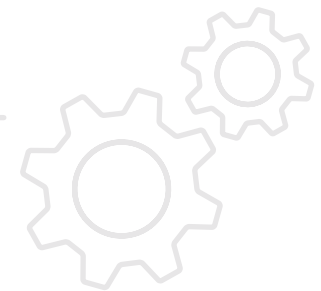
## Splunk Incident Response

**PSCU:** Das Finanztechnologieunternehmen PSCU weiß, dass Ausfallzeiten Geld kosten. Vor der Einführung von Splunk On-Call verzeichnete das Unternehmen MTTAs von etwa vier Stunden. Vor dem Einsatz von Splunk On-Call gab es einen einfachen Round-Robin-Eskalationsprozess. Nach einem Jahr der Verwendung von Splunk On-Call war ihre MTTA um erstaunliche 90 % auf 20 Minuten gesunken. Mit dem weiteren Einsatz von Splunk On-Call ließ sich die MTTA sogar noch weiter reduzieren. Ferner wurden die folgenden Wirkungen festgestellt:

- On-Call-Zeitpläne werden zugunsten maximaler Transparenz abteilungsübergreifend verwaltet.
- Erhöhte Verantwortlichkeit für Bereitschaftsteams mit Verfolgung von Incidents und deren Ergebnissen.
- Verbesserte Erfahrung mit dem Bereitschaftsdienst, da die Benachrichtigungen gleich beim ersten Mal an die richtige Person geleitet werden.

„Mit Splunk On-Call haben wir unsere MTTA von vier Stunden auf zwei Minuten reduziert und eine stärkere Verantwortlichkeit des Einsatzteams erreicht.“

– Earl Diem, IT Operations Manager





# Optionen für Observability

## EINLEITUNG

Da der Bedarf von und die Nachfrage nach Observability wachsen, springen naturgemäß einige Anbieter von Monitoring-Tools auf den Zug auf – genau wie vor einiger Zeit bei DevOps.



Es ist aber wichtig, zu beachten, dass kein Tool Ihnen Observability „schenken“ kann. Observability ist ein Mindset – keine Praktik. Daher sollte bei der Abwägung Ihrer Optionen jeder Anbieter, der Ihnen „schlüsselfertige Observability“ verspricht, Ihre Alarmsirenen schrillen lassen.

Erschwerend kommt hinzu, dass viele Anbieter zwar behaupten, über umfassende Funktionen zur Observability zu verfügen, Ihnen bei genauerer Betrachtung aber nur einen Teil des Notwendigen bieten. Wenn Sie sich die Mühe machen, ein Observability-Mindset anzunehmen, müssen Sie sicherstellen, dass Ihr Tool alle Daten verarbeiten kann und Ihnen echte Erkenntnisse liefert.

# Observability – Konzipiert für Komplexität

Wie wir bereits erörtert haben, bringen moderne Entwicklungs- und Bereitstellungspraktiken eine höhere Komplexität mit sich. Diese Komplexität macht es immer schwieriger, Anwendungen zuverlässig zu betreiben. Es sollte das finale Ziel eines Observability-Tools sein, Ihre Erkenntnisse besser nutzbar und Ihr Unternehmen effektiver zu machen. Unsere Empfehlung: Überlegen Sie, inwieweit jedes Tool, das Sie evaluieren, Ihnen hilft, diese drei wichtigen operativen Funktionen besser zu erfüllen:



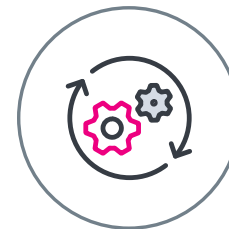
## Monitoring

für zentralisierte Transparenz in allen relevanten Infrastrukturen und Anwendungen, unabhängig davon, wo oder wie sie gehostet werden. Blicken Sie in Container hinein und über Cloud- und Hybrid-Umgebungen hinweg. Erkennen Sie die Kernursache von Problemen und stellen Sie Kontext bereit. Generieren Sie Erkenntnisse in automatisierter Weise, um Probleme frühzeitig zu erkennen.



## Zusammenarbeit

über Unternehmenssilos hinweg mit Freigabe der relevanten Daten für alle Beteiligten, um die Lösung von Incidents zu verwalten und wiederholbare Aktionspläne aufzubauen. Stellen Sie sicher, dass bei allen Benachrichtigungen auf Anhieb die richtige Person eingeschaltet wird. Teilen Sie den Einblick in Probleme oder Anomalien, für die keine Erläuterung zur Reproduktion erforderlich ist.



## Automatisieren

des Alltäglichen, Orchestrieren des Komplexen. Automatisieren Sie Prozesse, um Zeit zu sparen, in der Sie sich statt nur auf das Monitoring und das Troubleshooting auf das Wesentliche konzentrieren können – wie etwa strategische Geschäftsinitiativen. Orchestrieren Sie schließlich mehrere Prozesse, um menschliche Eingriffe beim Monitoring, bei der Ursachenanalyse und Problemlösung zu optimieren (und zu minimieren).

# Darum benötigen Sie die Splunk Observability Cloud

Ihre Infrastruktur und Ihre Anwendungen generieren jede Sekunde riesige Datenmengen. Die Erfassung all dieser Daten und die Verwendung fortschrittlicher Analyse- und Verarbeitungstechniken hilft Ihnen, die Komplexität zu bewältigen, Probleme schneller zu lösen, die Benutzerfreundlichkeit zu verbessern und all Ihre Daten so zu nutzen, wie Sie es wollen – mit OpenTelemetry. Splunk Observability Cloud bündelt alle notwendigen Komponenten, um Sie beim Aufbau Ihres Observability-Mindsets zu unterstützen: Infrastructure Monitoring, Application Performance Monitoring, Real User Monitoring, Synthetic Monitoring, Log-Exploration und Incident Response.

Der wichtigste Vorteil von Splunk Observability Cloud besteht darin, dass sie dafür sorgt, dass Sie die komplexe Architektur verstehen, die durch moderne Entwicklungspraktiken entsteht. Selbst wenn Ihr Unternehmen noch keine Cloud-First-Lösung eingeführt hat, werden neue Entwicklungen mit der Zeit langsam in diese Richtung drängen. Containerisierung, Public- oder Private-Cloud-Hosting, Serverless-Funktionen und dergleichen verkürzen die Entwicklungszeit und erleichtern Innovationen, aber sie erschweren es auch, den Überblick zu behalten. Splunk Observability Cloud konsolidiert Daten über jede Hosting-Umgebung hinweg, für jede Anwendung, und ist das einzige Tool, das *alle* Ihre Daten erfassen kann und sicherstellt, dass Sie nichts übersehen.

Probleme treten bei jedem System auf. Es wird immer etwas schiefgehen, und es ist wichtig, dass das Problem schnell gefunden und behoben werden kann, wenn

es auftritt. Viele Unternehmen führen derzeit nur eine reaktive Fehlersuche durch – sie stellen fest, dass etwas nicht in Ordnung ist, und beginnen dann, die Logdateien zu durchsuchen, um die Ursache zu finden. Mit Splunk Observability Cloud können Sie mit ein paar Klicks sehen, was und wo etwas für einen bestimmten Benutzer schief gelaufen ist, statt das Problem ohne eine Spur überall in Ihrer gesamten Infrastruktur zu suchen.

Letztlich werden alle Anwendungen entwickelt, um Benutzern einen Service zu bieten. Observability-Systeme, die das reale Benutzererleben nicht berücksichtigen, liefern kein vollständiges Bild des Geschehens. Splunk Observability Cloud bietet Ihnen die Möglichkeit, die tatsächliche, reale Benutzer-Erfahrung zu betrachten, indem Sie genau sehen, wie lange jeder Teil des Seitenaufrufs gedauert hat, sodass sogar Empfehlungen zur Verbesserung dieser Leistung möglich sind.

Schließlich ist die Instrumentierung all Ihrer Anwendungen und der gesamten Infrastruktur ein zeitaufwändiger Prozess. Es ist die Art von Aufgabe, die Sie tun müssen, aber die Sie idealerweise nur einmal erledigen. Splunk Observability Cloud wurde für OpenTelemetry entwickelt, ein als Branchenstandard etabliertes Instrumentierungssystem. OpenTelemetry ist das zweitaktivste Projekt der Cloud Native Computing Foundation und wird zunehmend von anderen Open Source- und kommerziellen Projekten übernommen. Die Instrumentierung Ihrer Anwendungen mit OpenTelemetry bedeutet, dass Sie nur einmal instrumentieren müssen und Ihre Daten dann in Zukunft zu jedem anderen Anbieter bringen können. Da immer mehr Projekte OpenTelemetry einführen, werden Sie vielleicht sogar feststellen, dass neue Anwendungen bereits vorinstrumentiert und ohne weitere Maßnahmen bereit sind, Daten an Splunk Observability Cloud zu senden.





## Observability auf einen Blick

- Sie ermöglicht Ihnen, die Komplexität moderner Architekturen und Anwendungen zu bewältigen und jede Frage zu Ihrer Anwendung und Ihrem Business zu beantworten.
- Ist ein Mindset, keine Praktik.
- „Absorbiert“ klassische Monitoringsysteme und erweitert sie, damit Sie Fragen beantworten können und nicht nur erfahren, dass etwas nicht stimmt.
- Nutzt alle Ihre Daten, um automatisch Erkenntnisse zu liefern, Fehler vorherzusagen und Apps besser und Benutzer zufriedener zu machen.
- Hilft Ihnen, Probleme in Sekunden zu lösen statt in Stunden. Sagt voraus, was schiefgehen könnte und hilft, die Kernursache von Problemen zu identifizieren.
- Gibt Ihnen die Möglichkeit, das Benutzererlebnis kontinuierlich zu verbessern, indem Sie Momentaufnahmen dessen sehen, was Ihre Benutzer erleben.
- Gibt Ihnen volle Kontrolle über Ihre Daten und die Nutzung der Open Source-Community, um Ihre Observability-Reise zu beschleunigen.

# Fazit

Der Wirbel um Observability ist wohlverdient. Sie ermöglicht es Engineering-Teams, mehr Verantwortung für die Uptime und Leistung zu übernehmen. Ihr Erfolg setzt einen Wandel der Unternehmenskultur voraus. Observability durchbricht die Komplexität moderner Architekturen und sorgt für eine End-to-End-Transparenz in Ihrem gesamten System, sodass Sie zu quantifizierbaren Ergebnissen gelangen.

Sie können Probleme schnell beheben und eventuell verhindern, sodass mehr Zeit für strategische Initiativen und die Verbesserung des Benutzererlebnisses bleibt. Der beste Weg, Observability zu erreichen, besteht darin, sich auf diese Denkweise festzulegen und dann einen Ansatz zu wählen, der es Ihnen ermöglicht, jede Benutzeranfrage oder jeden Vorfall den ganzen Weg durch Ihren Stack und darüber hinaus zu verfolgen – vom Browser des Benutzers bis hin zu APIs von Drittanbietern. Wenn Probleme auftreten, wählen Sie ein Tool, das das Monitoring, die Zusammenarbeit und die Automatisierung erleichtert, idealerweise unterstützt durch KI und ML. Kunden, die Observability mit Splunk erreicht haben, haben eine große Bandbreite an messbaren Geschäftsergebnissen erzielt, konnten die Entwicklerzufriedenheit steigern und profitieren von einer schnelleren Behebung komplizierter Probleme.

Splunk Observability Cloud ist die einzige Lösung, um Observability in jedem Unternehmen und jedem Einsatzszenario in jeder Größenordnung zu erreichen – von Megabytes bis Petabytes an Daten pro Tag. [Sehen Sie sich hier eine Demo an.](#)

**Starten Sie jetzt  
kostenfrei**

Splunk, Splunk>, Data-to-Everything, D2E und Turn Data Into Doing sind Marken und eingetragene Marken von Splunk Inc. in den Vereinigten Staaten und anderen Ländern. Alle anderen Markennamen, Produktnamen oder Marken gehören den entsprechenden Inhabern. © 2021 Splunk Inc. Alle Rechte vorbehalten.

21-15581-Splunk-Beginners-Guide-to-Observability-EB-110\_DE

**splunk**>  
turn data into doing™