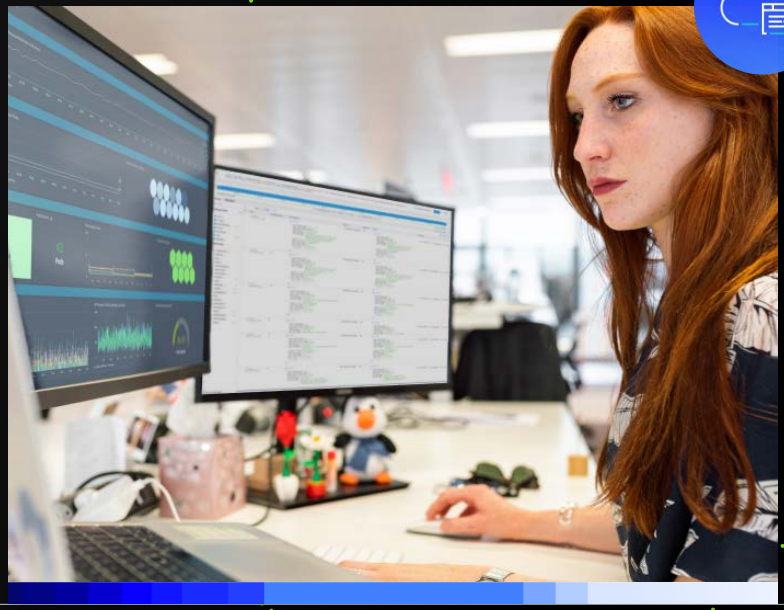
# Protokollanalysen im großen Maßstab

## Der beste Weg, um Ihre Anwendungen und Infrastruktur zuverlässig und sicher zu halten



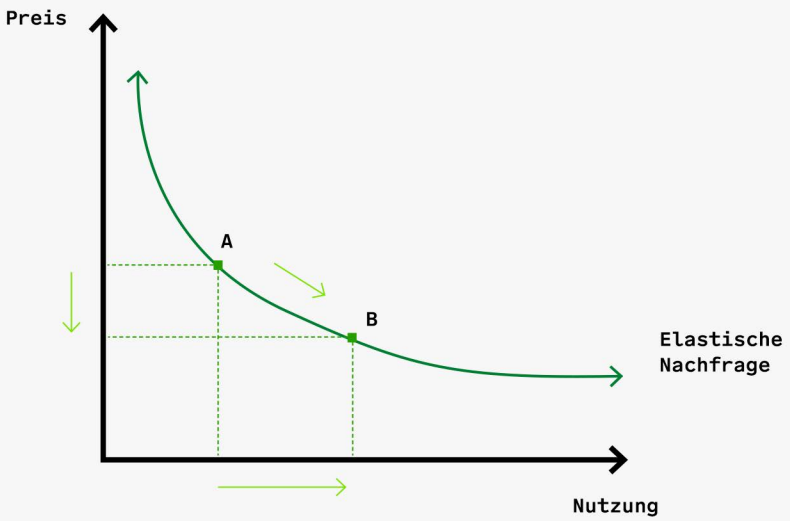
sumo logic

# Leitfaden zu Protokol-lanalysen

## Nur wenige Dinge sind so mächtig, so beängstigend, so übermächtig und so wichtig wie Daten.

Jeden Tag wechseln mehr Unternehmen für ihre wichtigen Geschäftsanwendungen zu Cloud-Lösungen. Dieser Wandel führt zu einer exponentiellen Zunahme der Daten aus verschiedenen Quellen in Cloud-Umgebungen. Während solide Protokollmanagementpraktiken helfen, diese Daten zu bändigen, sind Unternehmen auf Echtzeitanalysen und umsetzbare Erkenntnisse angewiesen, um die Zuverlässigkeit und Sicherheit digitaler Erlebnisse zu gewährleisten.

Laut einer Studie von Gartner wird sich über die Hälfte der IT-Ausgaben von Unternehmen in cloudbasierte Plattformen und Produkte verlagern. Wenn es um entscheidende Geschäftsabläufe geht, spielen Protokollmanagement und Protokollanalysen eine wesentliche Rolle. Gartner formuliert dies so: Technologie- und Dienstleistungsanbieter, die es nicht schaffen, sich an das Tempo der Cloud anzupassen, laufen Gefahr, zurückzubleiben, oder werden bestenfalls auf Märkte mit geringem Wachstum verwiesen.




Jevons Paradox

Eine visuelle Darstellung dessen, wie fallende Preise (mehr Effizienz) im Allgemeinen zu mehr bzw. weniger Verbrauch führen. Je geringer die Kosten, desto mehr Anwendungsmöglichkeiten entdecken Menschen für eine Ware. Da Cloud Computing immer billiger wird, finden Menschen immer mehr Möglichkeiten, dieses zu nutzen, weshalb es immer häufiger eingesetzt wird und die Nachfrage steigt. Diese „elastische Nachfrage“ ist Ausdruck einer effizienteren Preisgestaltung.

**In diesem Leitfaden geht es darum, wie Sie Protokollanalysen nutzen können, um vom Wachstum der Daten zu profitieren, statt darin unterzugehen. Wenn Sie Ihre Protokolle meistern, meistern Sie Ihr Unternehmen. Hier erfahren Sie, was Sie für den Einstieg wissen müssen.**

DEFINITION

# Protokolle, Protokoll-management und Analysen

Unternehmen generieren Daten in rasantem Tempo und aus unterschiedlichen Quellen.

In diesem Kontext handelt es sich bei einem Protokoll oder einer Protokolldatei um eine von einem Computer erzeugte Datendatei, die Informationen über Nutzungsmuster, Aktivitäten und Vorgänge innerhalb eines Betriebssystems, einer Anwendung, eines Servers oder eines anderen Geräts enthält. Diese mit einem Zeitstempel versehenen digitalen Aufzeichnungen dokumentieren Aktionen oder Ereignisse und stammen aus diversen Quellen.

Solides Protokollmanagement und Protokollanalysen liefern wertvolle Erkenntnisse für die effektive Überwachung dieser Komponenten.

**Maschinendaten stammen aus vielen Quellen**

**Anwendungen**

**Anwendungsinfrastruktur**

**Cloud-Infrastruktur**

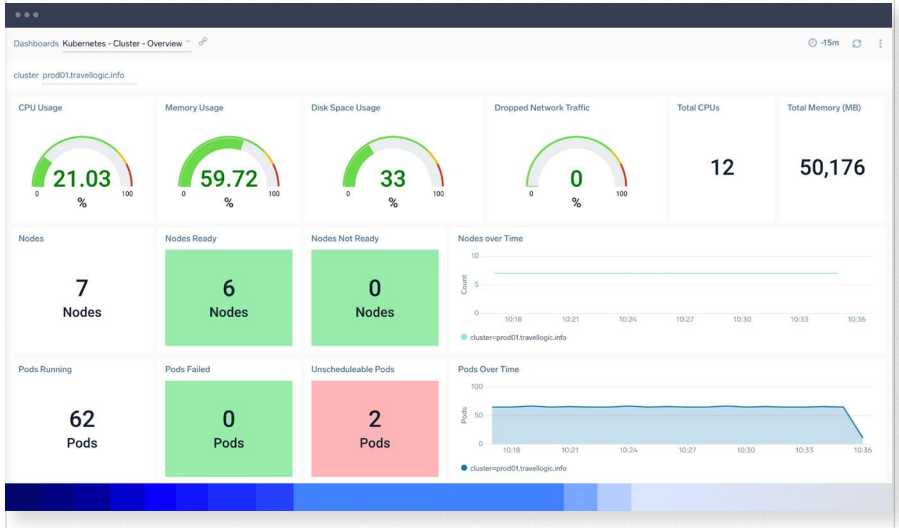
**Container**

**Load Balancer**

**Netzwerke**

**Server**

# Protokollmanagement und Protokollanalysen hängen eng zusammen, sind aber keine identischen Konzepte.




Fortlaufende Überwachung und proaktive Analysen kennzeichnen gut entwickeltes Protokollmanagement und Protokollanalysen.

**Protokollmanagement**
bezieht sich auf diverse Prozesse für das Sammeln, Verwalten, Speichern und Archivieren großer Mengen von Protokolldaten. Im Kontext der Standortzuverlässigkeit und eines größeren DevOps-Frameworks umfasst das Protokollmanagement das Sammeln und Analysieren von Protokolldaten aus relevanten Systemen, um die Leistung zu überwachen und zu verbessern, Probleme und Fehler zu erkennen und die Sicherheit zu verbessern.

**Protokollanalysen**
betreffen das Überprüfen, Interpretieren und Nachvollziehen von computergenerierten Aufzeichnungen (oder Protokollen). Protokolle sind für die Leistung und Sicherheit von Anwendungen unerlässlich. Sie bilden die Grundlage für proaktive DevSecOps-Praktiken.

## Was genau ist also eine Protokollanaly-selösung?

Eine Protokollanalyselösung kann ein bestimmtes Tool, eine bestimmte Plattform oder ein bestimmtes Framework sein, das bzw. die die Prioritäten eines Unternehmens für Protokollmanagement und -analysen festlegt. Ohne eine moderne Plattform für Protokollmanagement und -analysen stehen Unternehmen vor Herausforderungen, die Lösungen erfordern:

**Datensilos**
bei Entwicklungs-, SRE-, Ops- und Sicherheitsteams und Tools.

**Ein extrem hohes Volumen an Protokolldaten,**
mit dem sich nur schwer echte Transparenz oder umsetzbare Erkenntnisse erzielen lassen.

**Die mittlere Lösungszeit (MTTR)**
steigt durch die übermäßig langsame Rehydrierung der Protokolle, was die Teams bei der Problembehebung ausbremst. Eine umfassende Protokollmanagement- und Protokollanalyseplattform vereint diese Ziele und bietet eine Single Source of Truth, um Trends oder Störungen der Systemleistung und -ergebnisse nachzuvollziehen.

## Beispiele für Protokollanalyse-funktionen und -verfahren

Bei der Protokollanalyse geht es um die Behandlung komplexer, häufig separater Datenquellen und -typen, die sich bis auf die Extraktion spezifischer Informationen aus diesen Protokollen erstreckt. Es gibt mehrere gängige Methoden für die Organisation, Verarbeitung und Interpretation von Daten, darunter:

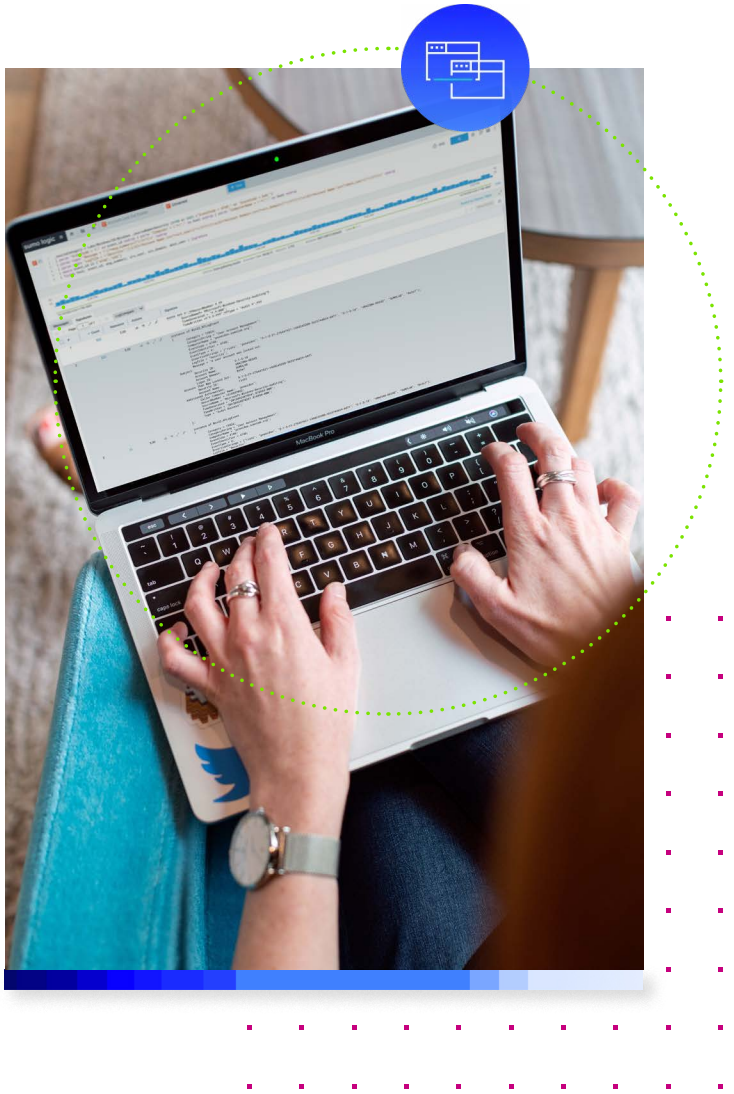
**Normalisierung**
indexiert, standardisiert und übersetzt Protokolldaten in ein gemeinsames Format, das den Vergleich und die Analyse erleichtert.

**Mustererkennung**
vergleicht Echtzeitdaten mit historischen Mustern, um Anomalien, Auffälligkeiten oder Fehler hervorzuheben. Dies ermöglicht eine schnellere Diagnose und Behebung.

**Klassifizierung und Kennzeichnung**
gruppieren ähnliche Protokolleinträge nach Typ, um bestimmte Fehlertypen oder -orte zu erkennen und zu beseitigen.

**Klassifizierung und Kennzeichnung**
führen Protokolle aus verschiedenen Quellen zusammen, um Verbindungen und potenzielle Korrelationen zwischen Systemen und Ereignissen zu erkennen.

# Protokollanalysen – Anwendungsfälle



Systemprotokolle bilden eine Fundgrube für Informationen und beantworten auch die Frage, ob Ressourcen ordnungsgemäß und optimal funktionieren. Protokollmanagement und -analysen bilden die Grundlage für Anwendungsfälle im Hinblick auf Beobachtbarkeit und Sicherheit (oder die Bewertung und Untersuchung des Verhaltens, der Aktionen, der Ausgaben und des Sicherheitsstatus eines Systems).

Auch in der jüngeren Vergangenheit erforderte das Sammeln und Auswerten von Protokollen mühsame manuelle Eingriffe, bei denen es leicht zu menschlichen Fehlern kam. DevOps und Sicherheitsteams sind im Nachteil, wenn sie nicht auf exakte, aktuelle Informationen zugreifen und diese verarbeiten können.

Vier allgemeine, primäre Anwendungsfälle der Protokollanalyse sind die proaktive Überwachung, die Problembehebung, die digitale forensische Untersuchung sowie Datenanalysen und Berichterstellung.

## VIER PRIMÄRE ANWENDUNGSFÄLLE FÜR PROTOKOLLANALYSEN

**Proaktive Überwachung**

Durch die Überwachung der Anwendungsleistung und -sicherheit können Unternehmen die Leistung und das Systemverhalten zeitnah und direkt verfolgen, um es nachzuvollziehen und zu verbessern. Hierzu gehören die Identifizierung ungewöhnlicher oder anomaler Aktivitäten sowie die Untersuchung von Sicherheitsvorfällen. Ziel ist es, Leistungsprobleme oder Sicherheitsbedrohungen schnell zu erkennen und zu beheben, bevor sie Chaos anrichten. Sumo Logic bietet eine Vielzahl von Tools für die proaktive Überwachung. Diese umfasst unter anderem die Infrastrukturüberwachung, Benutzerüberwachung in Echtzeit, Beobachtbarkeit von Anwendungen und Überwachung der Cloud-Sicherheit.

**Problembehebung**

Eine proaktive Überwachung verbessert die Möglichkeiten zur Problembehebung. Sobald eine Anomalie erkannt wird, sollte die Protokollanalyse einsehbare Einblicke dazu liefern, was vor, nach oder sogar gleichzeitig mit dem Problem oder verdächtigen Verhalten aufgetreten ist.

**Forensische Untersuchung**

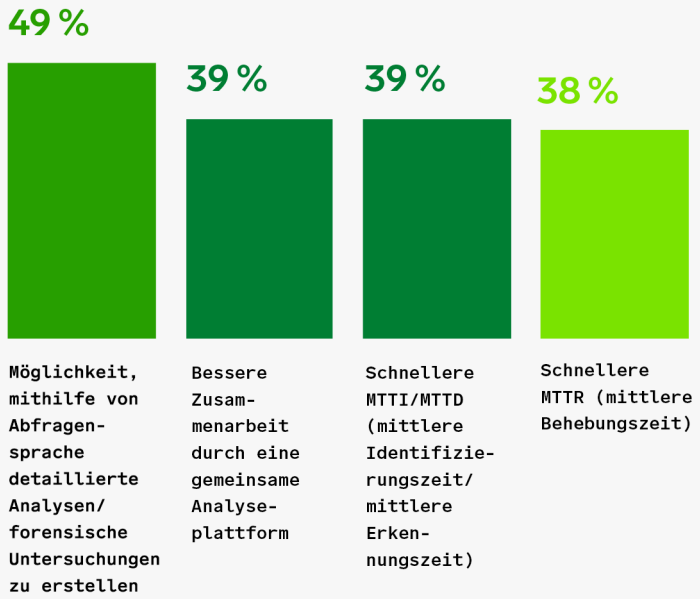
Die forensische Untersuchung bezieht sich auf den Prozess der Analyse der Protokolldaten, um zu erkennen, wann ein Sicherheitsvorfall aufgetreten ist, wer ihn initiiert hat, welche Aktionen in welcher Abfolge beteiligt waren und welche Auswirkungen diese auf das Unternehmen hatten. Sie hilft auch, die von einem Angriff betroffenen Daten zu identifizieren und die verwendeten Angriffstechniken zu lokalisieren.

**Datenanalysen und -berichte**

Das einfache Sammeln von Daten ist eine Sache – sie umsetzbar zu machen, ist ein weiterer Punkt. Jedes Protokollmanagement- oder Protokollanalyseprogramm ermöglicht unter anderem den einfachen Zugriff auf wichtige Informationen zur Systemleistung und weitere zugehörige Metriken, die nachvollzogen und auf die reagiert werden kann. Intuitive und anpassbare Dashboards stellen sicher, dass alle mit den gleichen Daten und abgestimmten Prioritäten arbeiten.

# Welche Vorteile bieten Protokoll-management und Protokollanalysen?

- Identifizieren von Möglichkeiten zur Rationalisierung von Geschäftsabläufen und Optimieren der Systemleistung für mehr Effizienz, einschließlich der potenziellen IT-Automatisierung.
- Implementieren eines Frameworks für eine bessere Ursachenanalyse, effektive Fehlerbehebung sowie schnellere Reaktionen und Lösungen bei Vorfällen.
- Verbesserung der Ressourcenzuteilung und -bereitstellung, um wichtige Elemente zu priorisieren und die Bandbreite entsprechend zu nutzen.
- Verbesserung der Cybersicherheitsmaßnahmen durch proaktive und kontinuierliche Überwachung.
- Sicherstellen der Einhaltung spezifischer Regulierungen wie HIPAA und DSGVO.
- Mehr Möglichkeiten für zeitnahe, sinnvolle Zusammenarbeit (z. B. zwischen Cloud-Architekten und -Betreibern).
- Stärkung der Effektivität von Vertriebs- und Marketingkampagnen durch die Auswertung von Metriken zu Website-Datenverkehr, Konversionsfehlern und mehr.




Wichtigste operative Vorteile der Verwendung von Sumo Logic

N=112

70 %

Weniger Verwaltungsaufwand bei der Verwaltung von Protokolldaten

Wichtigste Kostenvorteile der Verwendung von Sumo Logic

N=93

Quelle: UserEvidence-Umfrage unter Nutzern von Sumo Logic. Statistik geprüft 02.02.2023.

## Welche Rolle spielen Analysen im Protokollmanagementprozess?

Ein Protokollmanagementprozess verläuft in der Regel in vier Phasen, die jeweils von Protokollanalysen profitieren:

1 Die erste Phase ist die Protokollerfassung, bei der Protokolle von Betriebssystemen, Anwendungen, Cloud-Infrastruktur, Netzwerkgeräten usw. gesammelt werden. Das Erfassen und Aggregieren von Protokollen bildet die Grundlage einer kontinuierlichen Überwachung und einer zeitnahen Protokollanalyse. Die besten Aggregationstools bieten zuverlässige und konsistente Verfahren für die Optimierung des Protokollanalyseprozesses.

2 Die Zentralisierung und Indexierung von Protokollen in einem einzigen Repository bzw. an einem einzigen Speicherort, auf den die gesamte IT-Infrastruktur zugreifen kann, bildet eine notwendige Grundlage für die Protokollanalyse. In komplexen Umgebungen mit vielerlei Arten von datengenerierenden Systemen und Prozessen gewährleistet die Einhaltung von Best Practices für die zentrale Protokollierung eine zuverlässige, gemeinsame Source of Truth.

3 Das Suchen und Analysieren von Daten wäre mühsam, wenn es von manuellen Prozessen abhinge. Es würde so viel Zeit in Anspruch nehmen, diese Daten zusammenzustellen und dafür zu sorgen, dass sie fehlerfrei und vollständig sind, dass es schwierig würde, sie zeitnah zu bearbeiten. Lösungen wie Sumo Logic bieten die Protokollanalysen, die für die sinnvolle und effiziente Interpretation der Protokolldaten und das Gewinnen umsetzbarer Erkenntnisse benötigt werden.

4 Überwachung der Systemleistung und der Daten, um Anomalien oder andere Probleme effizient zu erkennen. Mit der Analyseplattform von Sumo Logic können Sie die kontinuierliche Überwachung um benutzerdefinierte Warnmeldungen erweitern, die Sie benachrichtigen, sobald bestimmte Ereignisse eintreten oder bestimmte Bedingungen erfüllt sind.

# Protokollanalysen – Best Practices

Die Einhaltung der folgenden Best Practices liefert ein effektives und wiederholbares Framework für Protokollanalysen, deren Interpretation und daraus resultierende Maßnahmen. Daten, die nicht ordnungsgemäß erfasst und standardisiert werden, können nicht effektiv analysiert werden.

**Entwickeln Sie Ihre Strategie**
Vermeiden Sie es, Zeit zu verschwenden oder sich durch ineffiziente Prozesse zu arbeiten. Entwickeln Sie Ihre Strategie, bevor Sie loslegen. Beginnen Sie mit dem Wichtigsten. Stellen Sie sich Fragen wie die folgenden:

- **Funktioniert unsere Infrastruktur optimal? Wo gibt es Möglichkeiten, Prozesse zu optimieren oder zu verbessern?**
- **Welche Faktoren verursachen Probleme bei der Berichterstellung oder bei Anwendungen? Berücksichtigen Sie Indikatoren wie Latenz und Fehlerquote.**
- Sind unsere Authentifizierungsverfahren sinnvoll und bieten ein angemessenes Maß an Sicherheit?
- **Auf welche Inhalte, Produkte oder Dienstleistungen verlassen sich unsere Nutzer am häufigsten? Erfüllen diese ihre Erwartungen?**
- **Verfolgen wir Kennwortänderungen, unbefugte Anmeldungen, Scans von Netzwerkports und neu erstellte Benutzerkonten in unseren On-Premises- und Cloud-Systemen?**

**Bringen Sie Ordnung in Ihre Daten**
Das bedeutet, dass Sie Ihre Daten für den Zugriff und die Analyse strukturieren und in einem Repository zentralisieren. Dies ermöglicht die effizientere Analyse und Interpretation sowie Kreuzanalysen.

**Identifizieren Sie Datenkorrelationen**
Wenn Sie unternehmensweit auf Daten zugreifen und diese analysieren können (das Gegenteil zur Speicherung in Silos), können Sie in diesen Daten einfacher sinnvolle Zusammenhänge erkennen und nachvollziehen. Dies ist essenziell für eine effiziente Ursachenanalyse und damit verbundene Verbesserungen der Frameworks für Protokollmanagement- und Analysefunktionen.

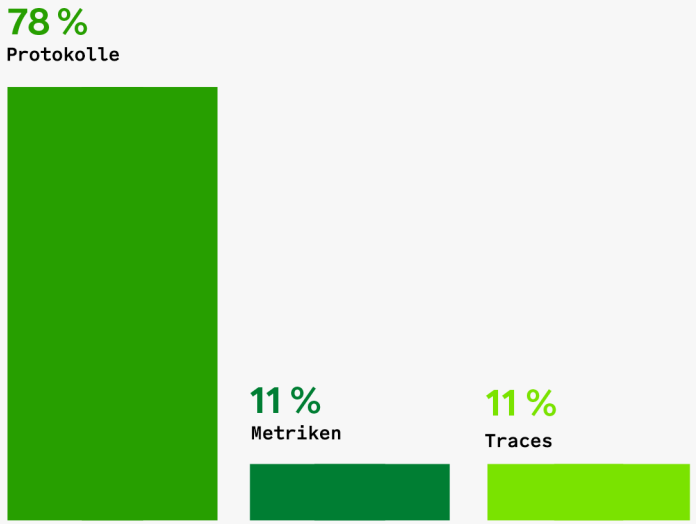
**Behalten Sie Ihre Echtzeitdaten im Auge**
Fortlaufende Überwachung und proaktive Analysen kennzeichnen gut entwickeltes Protokollmanagement und Protokollanalysen. Wenn diese Prozesse eingerichtet sind, können Unternehmen die Ursachenanalyse optimieren und Probleme schneller beheben.

**Richten Sie Warnungen ein**
Legen Sie Schwellenwerte für die Anwendungsleistung und Sicherheitsaktivitäten fest und richten Sie dann Warnmeldungen ein, die automatisch ausgelöst werden, sobald der Indikator den Schwellenwert über- oder unterschreitet. Anschließend können Sie das Problem mithilfe der detaillierten Datenanalyse beheben.

# Die richtige Protokollana-lyselösung

Eine SaaS-Analyseplattform wie Sumo Logic ermöglicht Unternehmen intelligentere und schnellere Entscheidungen. Sie versorgt DevOps und Sicherheitsteams mit zeitnahen Empfehlungen, die auf Echtzeitanalysen und -erkenntnissen basieren – auf einer einzigen Plattform.

Dies ist besonders wichtig, wenn die Komplexität und das Volumen der Daten mit der Zeit zunehmen. Eine proaktive und kontinuierliche Überwachung ist äußerst schwierig für Unternehmen, die bei ihrer digitalen Transformation ins Hintertreffen geraten sind. Moderne Lösungen erkennen, verstehen und beheben Informationslücken – auch solche, die mit isolierten Anwendungsarchitekturen oder Teams zusammenhängen.




Daten, die für Sumo Logic-Benutzer am hilfreichsten sind, wenn sie ein Leistungsproblem beheben müssen

N=139
Quelle: UserEvidence-Umfrage unter Nutzern von Sumo Logic. Statistik geprüft 02.02.2023.

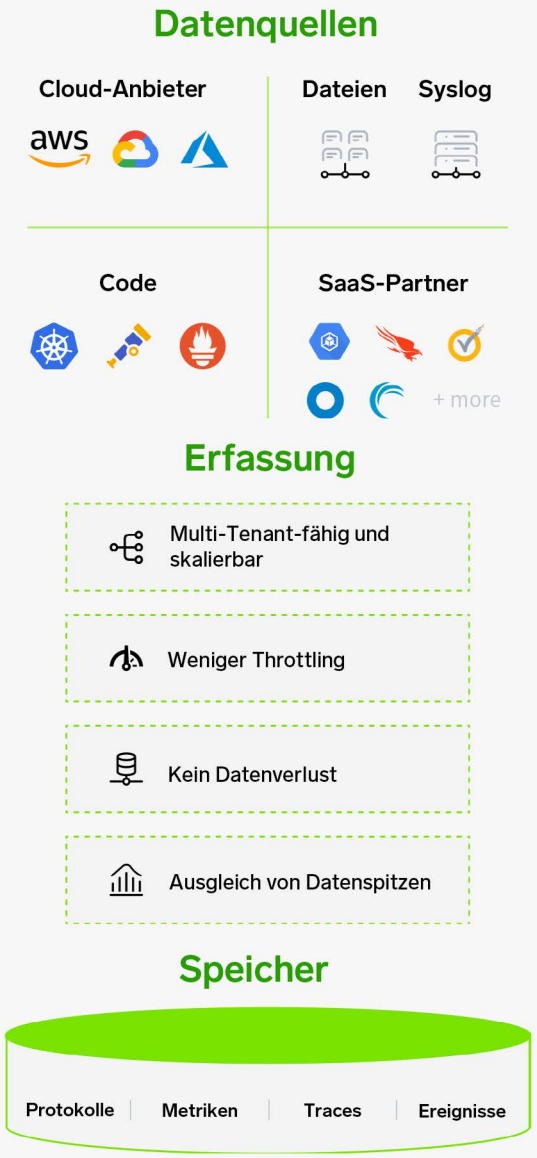
**„Seit dem Wechsel zu Sumo Logic kann unser Unternehmen extrem einfach selbst kleinste Störungen im Betrieb erkennen und innerhalb kürzester Zeit präzise beheben.“**

Manager einer großen Unternehmensbank

## Komplexe Anwendungsarchitektur und Multi-Cloud-Umgebung

Wenn Arbeitslasten in kleinere Komponenten unterteilt und innerhalb eines Unternehmens delegiert werden, entsteht eine komplexere Datenumgebung. Dies mindert den Nutzen der Daten, da sie weniger umfassend und für die Teams schlechter zugänglich sind. Sumo Logic bringt diese Systeme und die von ihnen erzeugten Daten in einem intuitiven Repository zusammen. Dies beschleunigt die Umsetzung von Qualitätsverbesserungen und liefert den kompletten Kontext.

Darüber hinaus wird es durch eine isolierte Architektur und Infrastruktur schwerer, ein vollständiges und skalierbares Datensystem zu erzielen. Die Multi-Cloud-Lösung von Sumo Logic aggregiert Daten aus dem gesamten Unternehmen und den Cloud-Umgebungen auf einer einzigen Oberfläche, was den Zugriff verbessert und eine kontinuierliche Überwachung in Echtzeit ermöglicht.




Sumo Logic – Datenerfassung und -speicherung

MODERNE LÖSUNGEN MÜSSEN FOLGENDES BEWÄLTIGEN:

## Sicherheitsbedrohungen

Je weniger kohärent die Protokollmanagement- und Protokollanalysesysteme eines Unternehmens sind, desto schwieriger wird ein proaktiver Schutz vor den neuesten Sicherheitsbedrohungen. Die Plattform von Sumo Logic trägt dazu bei, Schlüsselprozesse wie die Bedrohungserkennung und -reaktion zu beschleunigen. Damit lassen sich Bedrohungen schneller und einfacher erkennen, ihr Risiko bewerten und angemessen reagieren.

## Möglichkeiten zur Zusammenarbeit

„Wissen ist Macht“ ist aus gutem Grund ein Klischee – das in der Regel stimmt. Im Kontext der Protokollanalyse bedeutet dies die Einrichtung einer Single Source of Truth, die alle auf dem Laufenden und auf dem gleichen Stand hält. Unternehmen sollten möglichst von einem stark auf Silos basierenden Ansatz abrücken. Sumo Logic bietet einen zentralen Ort, an dem Techniker- und Business-Teams von überzeugenden Echtzeiteinblicken profitieren.

## Individuelle Integrationen

Sumo Logic ermöglicht Unternehmen die Optimierung von Workflows mit nativen Integrationen für beliebte Anwendungen wie Amazon Web Services, Google Cloud Platform, Microsoft Azure und andere. Sumo Logic ist für Skalierbarkeit und Flexibilität ausgelegt und ermöglicht Ihnen die Implementierung eigener benutzerdefinierter Abfragen.



# Machen Sie mehr aus Ihren Protokollen

Die Echtzeit-SaaS-Analysen von Sumo Logic ermöglichen DevOps und SecOps-Teams das Aggregieren und Zentralisieren der Ereignisprotokolle verschiedener Anwendungen und Infrastrukturkomponenten. Das gibt Unternehmen die Werkzeuge und Erkenntnisse an die Hand, mit denen sie Folgendes erzielen:

- → Zentralisierung und Erfassung
- → Überwachung und Visualisierung
- → Durchsuchung und Untersuchung
- → Warnung und Benachrichtigung


Mit dem richtigen Partner bekommen Sie das extreme Anwachsen der Daten in den Griff. Nutzen Sie Sumo Logic-Protokollanalysen, um schwarze Löcher in Ihren Daten in Ihre größte Wachstumschance zu verwandeln. Erfahren Sie mehr.

## Sumo Logic. Die unendliche Kraft der Protokollanalyse.

## Über Sumo Logic

Sumo Logic, Inc. (NASDAQ: SUMO) schafft die Grundlagen, um moderne, digitale Unternehmen zu realisieren. Über seine SaaS-Analyseplattform ermöglicht Sumo Logic es den Kunden, zuverlässige und sichere cloudnative Anwendungen bereitzustellen. Sumo Logics Continuous Intelligence Platform™ unterstützt Fachkräfte und Entwickler gleichermaßen, Anwendungszuverlässigkeit, Sicherheit und Schutz vor modernen Sicherheitsbedrohungen zu gewährleisten und Erkenntnisse über ihre Cloud-Infrastrukturen zu gewinnen. Kunden auf der ganzen Welt setzen auf Sumo Logic, um leistungsstarke Echtzeitanalysen und -erkenntnisse aus Beobachtungs- und Sicherheitslösungen für ihre cloudnativen Anwendungen zu erhalten. Besuchen Sie für weitere Informationen: SUMOLOGIC.COM

sumo logic