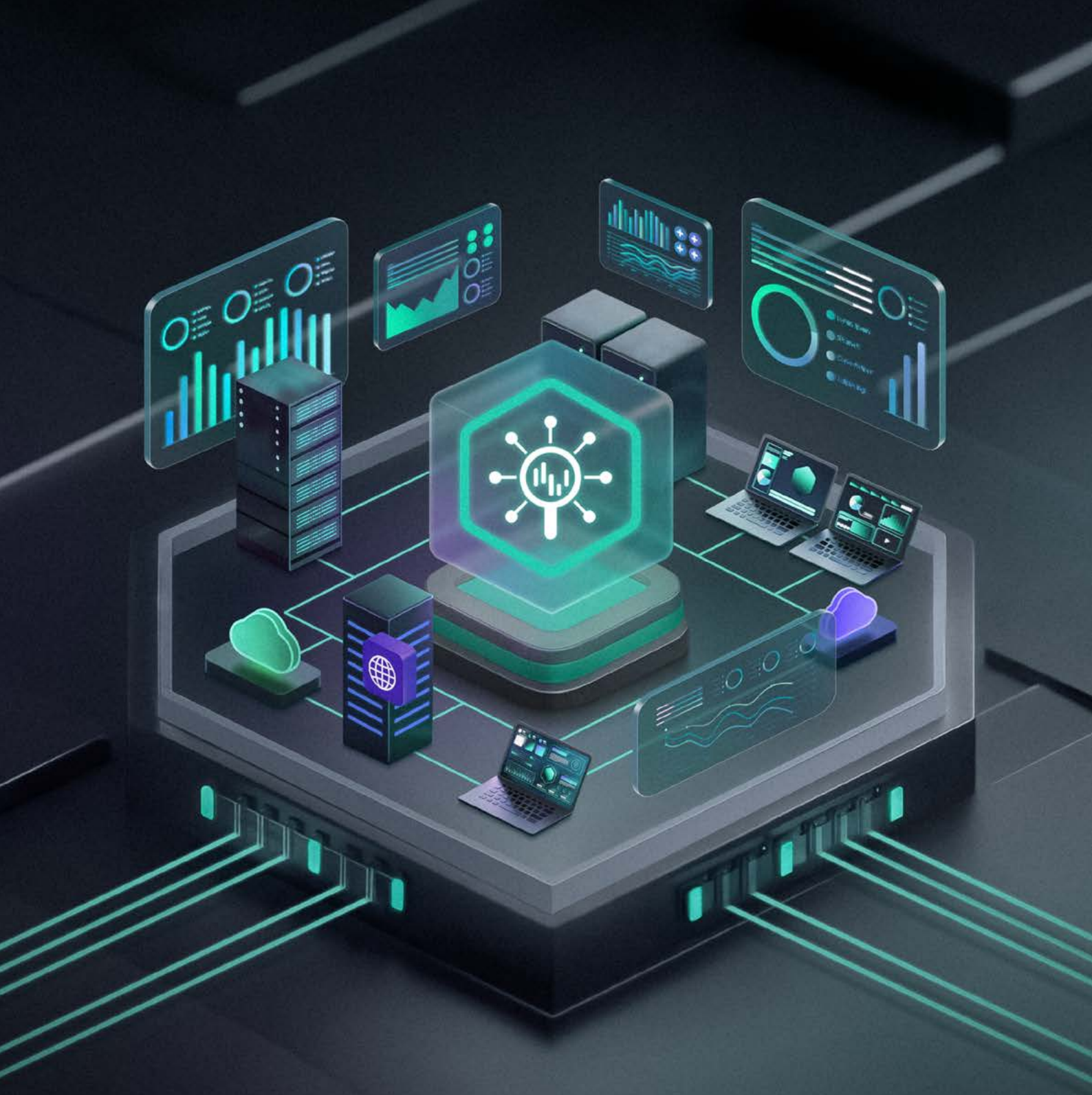


Datenblatt

Kaspersky Log Collector

Zentrale Protokollerfassung ohne Komplexität

kaspersky cybersecurity true to business



Aufbauend auf der bewährten SIEM-Technologieplattform von Kaspersky unterstützt Kaspersky Log Collector Unternehmen bei:

- Der Protokollierung und Verwaltung von Protokollen über verteilte Umgebungen hinweg
- Beim Start der wesentlichen Funktionen für die Protokollverwaltung
- Vereinfachung der zukünftigen Migration zu erweiterten SIEM-Funktionalitäten
- Sicherung der Betriebskontinuität bei Weiterentwicklung der Sicherheitsanforderungen
- Reduzierte Komplexität bei Bereitstellung und Verwaltung

Vereinfachte Protokollverwaltung in Ihrer Umgebung

Unternehmen generieren heute zunehmende Mengen an Sicherheits- und Betriebsprotokollen – über Endpoints, Server, Netzwerkgeräte, Anwendungen und cloudbasierte Systeme hinweg. Gleichzeitig nehmen die Compliance-Anforderungen, zu denen die DSGVO, NIS 2 und interne Richtlinien zur Datenaufbewahrung gehören, sowie der Bedarf an Vorfalluntersuchungen weiter zu. Das übt zusätzlichen Druck auf IT- und Sicherheitsteams aus.

Für viele KMU kann die Implementierung einer vollständigen SIEM-Plattform unnötige Komplexität, Infrastrukturkosten und operativen Mehraufwand mit sich bringen. Teams benötigen oft eine einfachere und kostengünstigere Möglichkeit, um Protokolle zu zentralisieren, aufzubewahren und zu verwalten. Gleichzeitig müssen sie die Transparenz über ihre Umgebungen hinweg wahren und Compliance-Anforderungen erfüllen.

Kaspersky Log Collector begegnet diesen Herausforderungen mit einer schlanken On-Premise-Lösung, die für die zentrale Erfassung und Speicherung von Protokolldaten konzipiert ist. Dies hilft Unternehmen, die Transparenz zu verbessern, die Protokollaufbewahrung zu vereinfachen und Initiativen zur Einhaltung gesetzlicher Bestimmungen zu unterstützen.

Entwickelt für effiziente, skalierbare Protokollverwaltung

Kaspersky Log Collector eignet sich ideal für KMU mit Umgebungen von bis zu 500 Geräten. Die Lösung wurde speziell für die zentrale Erfassung, Speicherung und Durchsuchung von Protokolldaten konzipiert. Die Lösung enthält keine SIEM-Korrelationsregeln, automatische Warnungen oder Arbeitsabläufe zur Vorfallreaktion. Dadurch können Unternehmen die Komplexität der Implementierung sowie den operativen Mehraufwand reduzieren. Das sind die Vorteile auf einen Blick:

1

Erfassen und zentralisieren

Sie Protokolle von IT- und Sichereitsquellen

2

Speichern Sie Protokolle sicher, um betriebliche Transparenz

und Compliance-Anforderungen zu gewährleisten.

3

Vereinfachen Sie die Bereitstellung

und Administration mit einer fokussierten, schlanken Architektur.

4

Reduzieren Sie den Infrastruktur- und Betriebsaufwand

im Vergleich zu vollständigen SIEM-Implementierungen.

5

Sorgen Sie für einen klaren Migrationspfad

hin zur vollen Kaspersky SIEM-Funktionalität, während sich die Anforderungen weiterentwickeln.

Protokolle über Ihren gesamten IT- und Sicherheits-Stack hinweg erfassen und speichern

Die Lösung unterstützt die Erfassung von Endpoints, Servern, Netzwerkgeräten, Anwendungen, Datenbanken und Sicherheitslösungen von Drittanbietern unter Verwendung gängiger Protokolle und Übertragungsmechanismen. Sie kann vollständig vor Ort betrieben werden und unterstützt Unternehmen mit strikten Anforderungen an Datensouveränität oder interne Anforderungen.

Unternehmen, die erweiterte Korrelations-, Detection Engineering- und automatisierte Reaktionsfunktionen benötigen, können nahtlos in die vollständige Kaspersky SIEM-Funktionalität migrieren. Sie müssen ihre Infrastruktur nicht neu aufbauen oder bereits erfasste Protokolldaten migrieren.

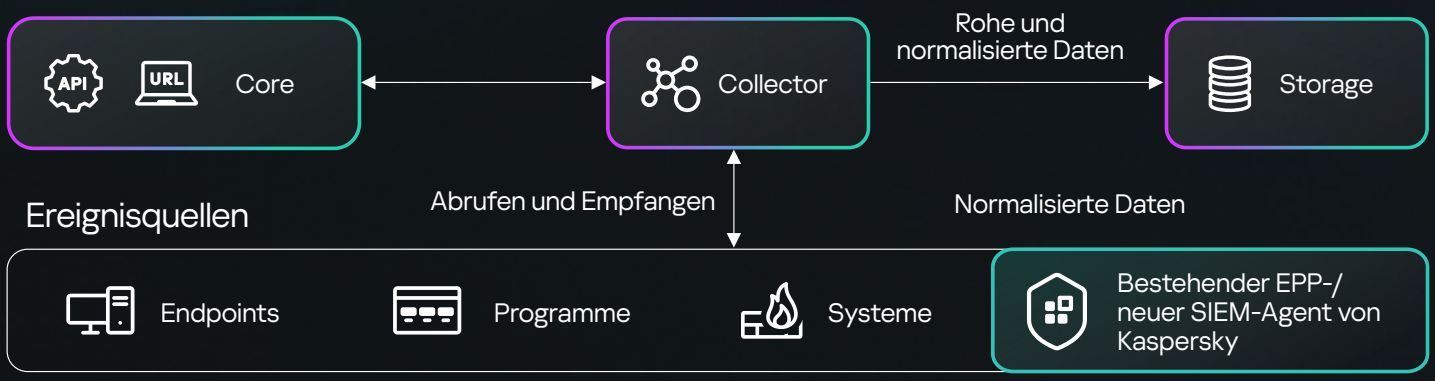
Mit einer Kaspersky SIEM-Lizenz können Organisationen sofort erweiterte SIEM-Funktionen – einschließlich Korrelation, Alarmierung und Detection-Workflows – auf Basis bereits erfasster historischer Daten nutzen.

Unterstützt Compliance- und Prüfungsanforderungen

Kaspersky Log Collector unterstützt Unternehmen dabei, Anforderungen im Zusammenhang mit der DSGVO, NIS 2, PCI DSS, internen Audit- und Vorfallreaktionsprozessen sowie unternehmensinternen Richtlinien zur Protokollaufbewahrung zu erfüllen. Er zentralisiert und sichert Protokolle über verteilte IT-Umgebungen hinweg.

Die Lösung trägt dazu bei, die Integrität und Verfügbarkeit der erfassten Protokolldaten zu gewährleisten, und unterstützt somit die Auditierbarkeit sowie die Anforderungen an die Log-Datenspeicherung.

Funktionsweise



Wie Kaspersky SIEM nutzt auch Kaspersky Log Collector eine Architektur auf Basis von Microservices, um Protokolle aus verschiedenen Infrastruktur- und Sicherheitsquellen zu erfassen, zu normalisieren und sicher zu speichern.

Die modulare Architektur vereinfacht Bereitstellung und Verwaltung und bietet gleichzeitig die Skalierbarkeit und Zuverlässigkeit, die für moderne IT-Umgebungen erforderlich sind.

Schnelle Untersuchung von Vorfällen mit flexibler Protokollierung

Zusätzlich zur zentralisierten Erfassung und Speicherung von Protokollen bietet Kaspersky Log Collector flexible Suchfunktionen, die IT- und Sicherheitsteams bei der Untersuchung betrieblicher und sicherheitsrelevanter Ereignisse unterstützen.

Unternehmen können historische Protokolle schnell durchsuchen für:

- Verdächtige Benutzeraktivitäten untersuchen
- Authentifizierungs- und Anmeldeverlauf überprüfen
- Suche nach Indikatoren im Zusammenhang mit bösartigen IP-Adressen oder Domänen
- Analysieren von Netzwerk- und Systemereignissen in verteilten Umgebungen
- Unterstützung bei internen Untersuchungen und Prüfungsanfragen

Die Lösung ermöglicht eine effiziente Protokollanalyse – ohne die Komplexität vollständiger SIEM-Korrelations- und Warnungsabläufe.

Wichtigste Vorteile

Nahtlose Integration mit dem Kaspersky-Ökosystem

Kaspersky Log Collector integriert sich direkt in Kaspersky-Sicherheitslösungen, einschließlich unserer Endpoint-Lösungen und Kaspersky Security Center.

Unternehmen, die bereits Produkte von Kaspersky nutzen, können ihre bestehende Telemetrie und Infrastruktur weiterverwenden und gleichzeitig die Bereitstellung sowie den Betrieb durch ein einheitliches Anbieter-Ökosystem und Supportmodell vereinfachen.

Die Nutzung desselben Agenten und derselben Technologieplattform wie bei Kaspersky SIEM trägt dazu bei, den Implementierungsaufwand und die operative Komplexität zu reduzieren:

Einfache Bereitstellung

Gezielte Funktionalität ermöglicht eine schnellere Implementierung und eine vereinfachte tägliche Verwaltung.

Umfassende Integrationsunterstützung

Unterstützt die Protokollerfassung von diversen IT-Infrastrukturkomponenten und Sicherheitssystemen.

Hohe Verfügbarkeit inklusive

Alle Lizenzen unterstützen standardmäßig eine hochverfügbare Bereitstellung, ohne dass eine zusätzliche Lizenzierung erforderlich ist.

Zukunftssichere Architektur

Bietet einen unkomplizierten Upgrade-Pfad zur vollen Kaspersky SIEM-Funktionalität, während sich die organisatorischen Anforderungen weiterentwickeln.

Kostengünstige Protokollverwaltung

Eine effiziente Alternative für Unternehmen, die eine zentralisierte Protokollerfassung benötigen – ohne die Betriebskosten einer vollständigen SIEM-Implementierung.

Anders als bei den von der Community unterstützten Open-Source-Tools für Protokollverwaltung bietet Kaspersky Log Collector kommerziellen Herstellersupport, eine planbare Lizenzierung und die Integration in das umfassende Sicherheits-Ökosystem von Kaspersky.

Unternehmen profitieren von einer vereinfachten Bereitstellung, professionellen Support-Dienstleistungen und einem zukunftssicheren Migrationspfad zu erweiterten SIEM-Funktionalitäten.

Bereit, die Erfassung und Speicherung von Protokollen zu vereinfachen?

Kontaktieren Sie uns für eine Produktpräsentation, eine Demo-Session oder eine Evaluierung von Kaspersky Log Collector in Ihrer Umgebung.

www.kaspersky.de

© 2026 AO Kaspersky Lab.
Eingetragene Marken und Servicemarken sind Eigentum ihrer jeweiligen Rechtsinhaber.

Kontakt

#kaspersky
#truetobusiness