PRODUKTÜBERSICHT

Datenerfassungstechnologie

LogRhythm
The Security Intelligence Company

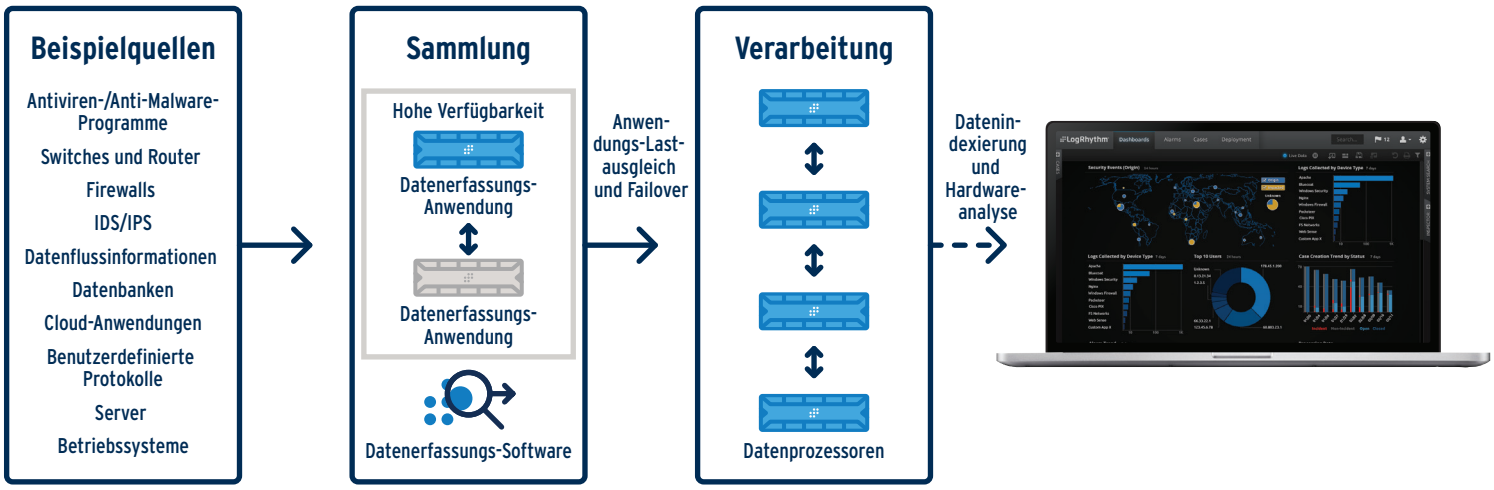
Die Datenerfassungstechnologie von LogRhythm unterstützt die Aggregation von Protokolldaten, Sicherheitsereignissen und sonstigen Maschinendaten. Die Datensammler können lokal oder remote arbeiten und werden zentral überwacht und verwaltet, um die Bereitstellung und Verwaltung zu vereinfachen. Dank Anwendungs-Lastverteilung zwischen den Datenprozessoren lässt sich die Lösung noch leichter skalieren.

Die Daten werden von den Datensammlern über eine authentifizierte und verschlüsselte TLS-Verbindung übertragen, die komprimiert werden kann, um die Breitbandnutzung zu minimieren. Die Datensammler können für unidirektionale Netzwerk-Kommunikationspfade konfiguriert werden und unterstützen somit auch besonders schutzwürdige Umgebungen sowie Compliance-Ziele.

Die Datensammler stellen die Integrität der Daten bei einem Netzwerkausfall sicher, indem volatiler UDP-Datenverkehr auf intelligente Weise gespoolt und der Status nicht-volatiler Daten verfolgt wird. Das automatische Failover zwischen den Datenprozessoren stärkt die Widerstandsfähigkeit zusätzlich.

Data Collector Appliance: : Ermöglicht die leistungsstarke Remote-Erfassung sämtlicher Maschinendaten, einschließlich Protokollmeldungen, Anwendungsdaten, Sicherheitsereignissen und Datenflüssen im Netzwerk. Eine einzige Collector Appliance kann bis zu 10.000 Meldungen pro Sekunde von tausenden Geräten erfassen und übermitteln.

Data Collector Software: Die lokale, agentenbasierte Erfassung wird von System Monitor ausgeführt, einer Software, die auch als Endpunktüberwachung fungiert. System Monitor kann auf Servern und virtuellen Maschinen unter Windows, Linux oder UNIX installiert werden. System Monitor konsolidiert und sammelt Protokoll- und Maschinendaten aus Remote- Umgebungen und der Cloud-Infrastruktur. Ein einzelner Agent, der als Datensammler agiert, kann tausende von Meldungen pro Sekunde von dutzenden von Geräten sammeln.



Universelle Erfassung

Die Datensammler sind mit zahlreichen Geräten und Formaten kompatibel, einschließlich benutzerdefinierter Protokollquellen, und unterstützen die folgenden Methoden:

- UDP/TCP und sicheres Syslog
- SNMP
- Flussdaten (z. B. IPFIX, NetFlow, sFlow, J-Flow, SmartFlow)
- LogRhythm Universal Database Log Adapter für System- und benutzerdefinierte Protokolle, die in Datenbanktabellen geschrieben werden (z. B. Oracle, SQL Server, MySQL) (ODBC- und JDBC-Protokolle)
- Windows-Ereignisprotokolle (einschließlich benutzerdefinierter Ereignisprotokolle)
- Flache Dateien (einzeilig und mehrzeilig, komprimiert oder unkomprimiert)
- Herstellerspezifische APIs (Beispiele):
  - AS/400 und iSeries
  - Checkpoint OPSEC/LEA
  - Cisco SDEE
  - Sourcefire eStreamer
- Vulnerability Scanner (Beispiele):
  - Qualys
  - Rapid7
  - Tenable Security Center
- Cloud-/SaaS-Lösungen (Beispiele):
  - Amazon AWS
  - Box
  - Cradlepoint
  - Office 365
  - Salesforce