FORCEPOINT
POWERED BY Raytheon

Datenblatt

FORCEPOINT Data Guard

Mehr und mehr Unternehmen setzen sich mit dem zweischneidigen Problem des effektiven Datenschutzes bei gemeinsamer Nutzung von Daten auseinander, und die Notwendigkeit einer sicheren Datenübertragung wird immer deutlicher. Aus einer Vielzahl von Quellen werden Daten üblicherweise zur Verarbeitung und Analyse in geschützte Bereiche übertragen. Damit die sensiblen Anforderungen unserer Kunden schnell, genau und präzise umgesetzt werden können, ist eine gemeinsame Nutzung dieser Daten unerlässlich. Die anhaltende Bedrohung durch Cyber-Angriffe, die das Ziel haben, in fremde Netzwerke einzudringen und Daten zu stehlen, erfordert, dass nur die sichersten Methoden für das Übertragen und gemeinsame Nutzen von Daten in Anwendung kommen.

Forcepoint Data Guard, das neueste Produkt in der Palette der domänenübergreifenden Lösungen (Cross Domain Solutions, CDS) von Forcepoint, erfüllt die Anforderungen an eine sichere Datenübertragung für Kunden, die sich ein Höchstmaß an Schutz für ihre vertraulichen Daten wünschen. Forcepoint Data Guard wurde speziell für die hohen Sicherheitsanforderungen vor allem in behördlichen und kritischen Infrastrukturumgebungen entwickelt. Die Lösung fungiert als bidirektionaler, automatisierter Wächter von Datenübertragungen, der die sichere Übermittlung strukturierter Daten zwischen verschiedenen Domänen oder Netzwerken ermöglicht.

Ein flexibler Ansatz

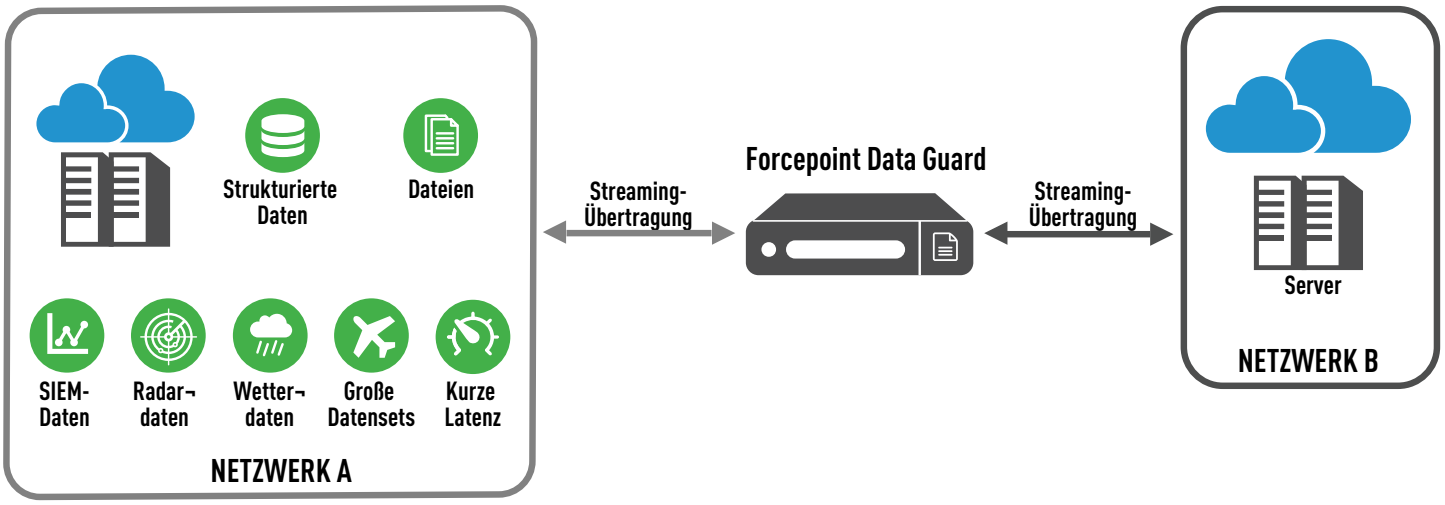
Forcepoint Data Guard basiert auf einem Betriebssystem mit Unterstützung mehrerer Stufen, das eine sehr zuverlässige Netzwerktrennung und Steuerung der Abläufe ermöglicht. Forcepoint Data Guard bietet detaillierte Inhaltsuntersuchung, Datenvalidierung und -filterung auf Byte-Ebene und kann an kundenspezifische Sicherheitsrichtlinien, -anforderungen und -risiken angepasst werden.

Das Betriebssystem ist vom sicheren Betriebssystem Red Hat Enterprise Linux 7 mit SELinux-Modulen (Security Enhanced Linux) abgeleitet und auf Evaluation Assurance Level (EAL) 4+ gemäß Common Criteria in Operating System Protection Profile (OSPP) zertifiziert.

Forcepoint Data Guard bietet eine flexible und dennoch umfassende Möglichkeit, Datenströme entsprechend den Sicherheitsrichtlinien des Kunden bis hinunter auf die Byte-Ebene zu untersuchen. Das für Sie zuständige Team von Forcepoint arbeitet mit Ihnen zusammen, um Ihre Datenübertragungsanforderungen zu bewerten und spezifische Richtlinien und Regeln zu entwickeln, die den Projekterfolg sicherstellen.

Durchsetzung von Sicherheitsrichtlinien

Die Engine zur Umsetzung von Richtlinien (Policy Implementation Engine) von Forcepoint Data Guard sorgt dafür, dass Richtlinien durchgesetzt werden. Sie unterstützt die vollständige Anpassung von Prüffunktionen und ermöglicht die Definition komplexer Sicherheitsrichtlinien. Dadurch sind für jede Installation spezifische Prüfungen und Einschränkungen möglich.



Übertragungsmechanismen

Forcepoint Data Guard unterstützt die folgenden sicheren Übertragungsmethoden, die an spezifische Aufgabenstellungen angepasst oder erweitert werden können: TCP und UDP über IP, File Drop Box (Dateiablageordner), XML-Filterung und Schemavalidierung.

TCP und UDP über IP

Forcepoint Data Guard unterstützt die Übertragung der meisten TCP- und UDP-basierten Protokolle. Dieser Übertragungsmechanismus wird auch zum Erstellen kundenspezifischer Protokolle genutzt, um bestimmte Datenanforderungen zu erfüllen.

File Drop Box

Dieser Übertragungsmechanismus ermöglicht Forcepoint Data Guard das Überwachen externer Dateiserver auf übertragungsbereite Dateien. Der Wächter überwacht Ordner auf Quellservern und ruft Dateien zur Überprüfung und Inhaltsfilterung ab, ehe sie an Zielserver weitergeleitet werden. Dateien, die aufgrund von Richtlinienverstößen nicht übertragen werden, können auf dem Quellsystem zur weiteren Analyse und Überprüfung isoliert werden. Beim Mechanismus „File Drop Box“ wird Secure Copy (SCP) zum Übertragen von Dateien zwischen dem Wächter und den externen Servern verwendet. *Für die Nutzung von File Drop Box ist eine optionale Lizenz erforderlich.*

XML-Filterung und Schemavalidierung

Beim Übertragen von XML-Inhalten durch den Wächter wird die XML-Filter-API benötigt, um die entsprechenden Regeln zu schreiben. Die XML-Regeln ermöglichen die vollständige Überprüfung und Modifizierung von XML-Inhalten, während sie den Wächter durchlaufen. Der Inhalt von XML-Dokumenten kann mit der Filter-Engine abgerufen und bearbeitet werden. Die zugehörige XML-Schemavalidierungs-API validiert XML-Dokumente im Abgleich mit einer oder mehreren Schemadateien. *Für die Nutzung der XML-Filterung und Schemavalidierung ist eine optionale Lizenz erforderlich.*

Protokollierung und Auditing

Forcepoint Data Guard wird mit einer Standardkonfiguration für das Auditing bereitgestellt, die an jede Bereitstellung angepasst werden kann. Diese besondere Auditing-Funktion wird von der Policy Implementation Engine gesteuert, die es der Sicherheitsrichtlinie ermöglicht, geeignete Daten jederzeit an den Audit-Trail zu übermitteln. Forcepoint Data Guard unterstützt die lokale Zusammenführung von Protokollen, d. h. des standardmäßigen Syslogs des Betriebssystems sowie der binären Auditing- und Datenübertragungsprotokolle. Über die Protokollanzeige kann auf Protokolldateien des Systems und des Wächters zugegriffen werden.

Anwendungsfälle

Forcepoint Data Guard bietet umfassenden Schutz für Ihre geschäftskritischen Daten und gewährleistet die bestmögliche Sicherheitsüberwachung. Diese ist oft ein Pflichtbestandteil gesetzlicher oder normativer Richtlinien zur Absicherung nationaler Sicherheitsdaten und -netze.

Gemeinsame Nutzung von Flugzeugüberwachungsdaten

Flugbetriebszentralen müssen für eine Koordinierung zwischen staatlich oder militärisch kontrollierten Flugsicherungssystemen und solchen unter ziviler Kontrolle sorgen, um die Sicherheit des zivilen Luftraums zu gewährleisten und das Öffnen und Schließen des militärischen Luftraums für die zivile Nutzung zu verwalten. Die von Radarsystemsensoren gesammelten ASTERIX-Daten müssen zwischen diesen Systemen streng kontrolliert und sicher übertragen werden.

Aufgrund der besonderen Bedeutung dieser Daten und der definierten Struktur des Datentyps ist Forcepoint Data Guard bestens geeignet, diese mehrstufige Koordination effektiv zu ermöglichen.

Zusammenführung von SIEM-Daten von Unternehmen

Netzwerkumgebungen staatlicher Stellen werden häufig unter Einsatz einer (oft zwingend vorgeschrieben) physisch getrennten, mehrstufigen Netzwerkarchitektur eingerichtet, damit verschiedene Geheimhaltungs-/Vertraulichkeitsstufen oder Netzwerke streng getrennt bleiben. Dieses Modell ist zwar ideal für den Daten- und Netzwerkschutz, die Verwaltung aber kann es enorm belasten. Das gilt für Security Operations Centers (SOCs) und Defensive Cyber Operations Centers (DCOCs) und die Tools, die sie zur Überwachung und Verwaltung von System-Audits und -warnungen verwenden.

Administratoren nutzen häufig eine SIEM-Lösung (Security Information & Event Management), um Bedrohungen auszumachen, Risiken in den Griff zu bekommen und einen ganzheitlichen Überblick über ihre Sicherheitslage zu erhalten. Daten, die sich in den einzelnen Netzwerken befinden, müssen nicht nur getrennt aufbewahrt werden – oft muss ihre Verwaltung sogar durch unterschiedliche Personen erfolgen, da die Daten teils streng vertraulich oder gar geheim sind. Dies führt zu einer großen Anzahl getrennter Überwachungs-Tools, was es erschwert, die betrieblichen Abläufe im gesamten Unternehmen zu überblicken.

Die Einbindung von Forcepoint Data Guard in die SIEM-Architektur bietet die Möglichkeit, Daten aus mehreren, untergeordneten Netzwerken in ein zentrales, übergeordnetes Netzwerk zu übertragen. Das Ergebnis ist eine Überwachungszentrale für das gesamte Unternehmen, die Administratoren einen umfassenden Überblick über die Grenzen einzelner Netzwerke hinweg bietet.

Automatisierung der Kommunikation zwischen Zählern und SCADA-Systemen

Umspannwerke für Fertigungsanlagen sind in der Regel vom SCADA-IP-Netzwerk isoliert, was sie zwar sicher, aber nicht sehr effizient macht. Manuelle Prozesse sind erforderlich, um auf Stromverbrauchsinformationen, Erzeugungs-/Verteilungseinstellungen und Rückmeldungen von Zählern zuzugreifen und diese zu justieren.

Durch das Einbinden von Forcepoint Data Guard in die Architektur kann eine sichere automatisierte M2M-Kommunikation (Maschine-zu-Maschine) zwischen Zählern und Umspannwerk erreicht werden. Der Wächter überprüft alle Datenübertragungen auf Anwendungs- bzw. Datenebene und lässt nur gültige Befehle und Datensets, die für den Betrieb benötigt werden, zu. Transaktionen, die den Sicherheitsrichtlinien von Forcepoint Data Guard nicht explizit entsprechen, werden bei der Prüfung abgelehnt (z. B. wird Schreibzugriff auf die Zähler abgeblockt). Mit Forcepoint Data Guard wird eine automatisierte bidirektionale Kommunikation sicher ermöglicht, wodurch manuelle Prozesse entfallen können und die Datensicherheit und -zuverlässigkeit erhöht werden.

KONTAKT
www.forcepoint.com/contact

[DATASHEET_FORCEPOINT_DATA_GUARD] 100072.020818