Forcepoint

Datenblatt

Forcepoint Data Security

DLP der Enterprise-Klasse, die auf allen wichtigen Kanälen einheitlich ist und einfach über die Cloud verwaltet wird.

Heutzutage ist Datensicherheit ein geschäftskritischer Teil der Strategie eines jeden Unternehmens. Aber gerade wenn Ihr Unternehmen das Gefühl hat, dass in puncto Datensicherheit Bescheid weiß, kommt die neueste Sicherheitsherausforderung: die sichere Verwendung von GenAI-Anwendungen. Angesichts der weiten Verbreitung von Daten auf Geräten und Cloud-Umgebungen und dem Aufkommen von GenAI-Anwendungen kann der Schutz sensibler Daten in einer KI-Welt wie eine unmögliche Aufgabe erscheinen.

Forcepoint Data Security ist eine cloud-native DLP-Lösung, die speziell für moderne Unternehmen entwickelt wurde. Diese DLP-SaaS-Lösung schützt sensible Informationen, verhindert Datenverletzungen und ermöglicht die Einhaltung von Datenschutzbestimmungen weltweit. Durch die schnelle Bereitstellung und Richtlinienverwaltung optimiert sie den Datenschutz und bietet ein einheitliches Management für GenAI- und Cloud-Apps, Internet, E-Mail und Endpunkte. Mit Forcepoint Risk-Adaptive Protection bietet diese Lösung Echtzeit-Einblicke in Benutzerrisiken. Profitieren Sie mit Forcepoint Data von reduzierten Kosten, verringerten Risiken und gesteigerter Produktivität.

Leistungsstarke Enterprise DLP Datenidentifikation auf allen Kanälen

- → Über 1.700 standardmäßige vordefinierte Klassifikatoren, Vorlagen und Richtlinien.
- → NVerarbeitung natürlicher Sprache (Natural Language Processing, NLP)
- → Erweiterte Erkennung echter Dateitypen, die über 900 Dateitypen abdeckt.

GenAI-Apps sicher nutzen

Starten Sie Ihre KI-Transformation noch heute mit Forcepoint. Steigern Sie die Produktivität und Effizienz mit der sicheren Verwendung von GenAI-Apps wie ChatGPT, Copilot, Gemini und vielen anderen. Mit Forcepoint Data Security können Sie Benutzer darin coachen, wie sie GenAI-Apps richtig verwenden, sensible Informationen beim Upload und Einfügen prüfen und blockieren (und zwar automatisch) und Versuche zum Missbrauch sensibler Daten protokollieren.

Einheitliche Verwaltung – „One policy to rule them all"

Sie können alle Forcepoint Services nahtlos über die Forcepoint Data Security Schnittstelle verwalten. Kontrollieren Sie alle Kanäle (CASB, SWG, E-Mails und Endbenutzer) mit einer einzigen Richtlinie, damit alle wichtigen Ausgangspunkte einheitlich sind. Implementieren Sie mit einem einzigen Klick eine neue Richtlinie oder wenden Sie eine vorhandene Richtlinie auf allen wichtigen Kanälen an. Überwachen Sie DLP-Vorfälle bequem von einem einheitlichen Dashboard aus und verschaffen Sie sich einen umfassenden Überblick über die Datensicherheit in Ihrem Unternehmen.

Einfache Richtlinienkonfiguration

- → Optimieren Sie die Verwaltung mittels Over-the-Air-Updates für die neuesten vordefinierten Richtlinien, Klassifikatoren und Vorlagen.
- → Erstellen Sie Richtlinien mit nur wenigen Klicks und implementieren Sie sie innerhalb von Minuten anstatt Stunden.
- → Profitieren Sie von standardmäßigen Compliance-Richtlinien für über 160 Regionen und 90 Länder, um die Einhaltung von Datenschutzbestimmungen in jeder wichtigen globalen Region zu gewährleisten.

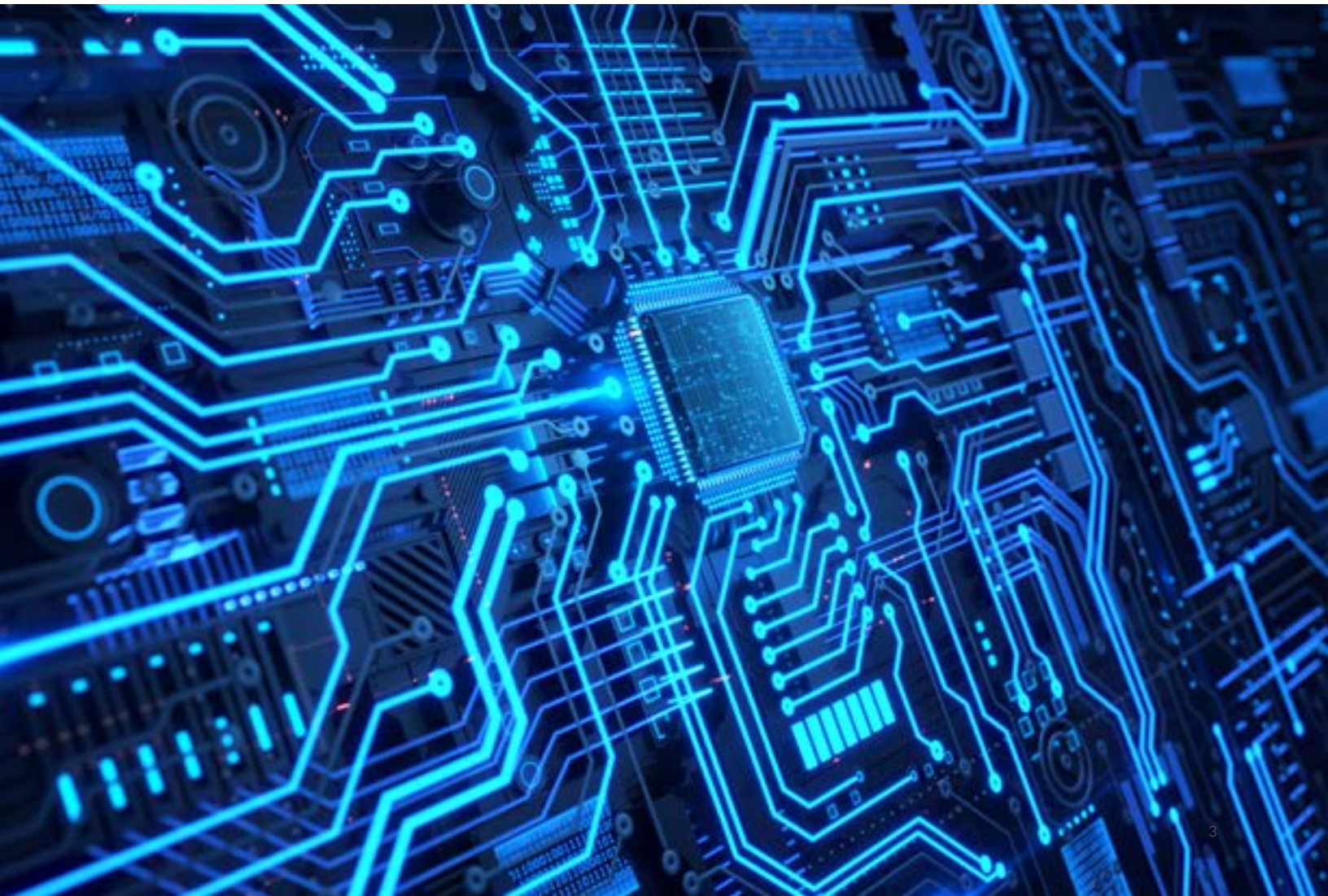
Einfache Verwaltung von Vorfällen und Warnmeldungen

Auf dem Reporting-Dashboard haben Sie einen vollständigen Überblick über alle Vorfälle und Warnmeldungen in nahezu Echtzeit. Dank integriertem Reporting erhalten Admins einen ganzheitlichen Überblick über Cloud-Anwendungen, Web-Traffic, E-Mails und Endgeräte. Native Device Control verbessert die Datensicherheit und die Zugriffskontrolle für Wechselmedien wie USB-Laufwerke. Forcepoint Data Security lässt sich nahtlos in Risk-Adaptive Protection integrieren – es bietet Echtzeit-Kontext und ein Verständnis der Benutzerabsicht, indem es sich auf Verhaltensweisen und Dateninteraktionen konzentriert. Forensische Funktionen ermöglichen tiefere Einblicke in die Datenbewegungen und ermöglichen eine effektive Untersuchung von Sicherheitsvorfällen, um die Durchsetzung von Richtlinien zu verbessern und die Compliance zu optimieren. All dies wird über einen einzigen Agenten und eine Benutzeroberfläche verwaltet.

*Die Integration mit Risk-Adaptive Protection (Endgerät für die Information der Risikobewertung erforderlich) erfordert eine separate SKU (Add-on zu Forcepoint Data Security).

Cloud-native SaaS-Lösung

- → Geringere Gesamtkosten.
- → Keine lokalen Hardware- und Software-Setup-Kosten.
- → Eine Cloud-native Lösung bietet eine bessere und effizientere Skalierbarkeit.
- → Einfache Datensicherheitsverwaltung mit kontinuierlichen Updates mit neuen Funktionen, Fehlerbehebungen und Sicherheitspatches.
- → Automatisierte Over-the-Air-Updates für Endbenutzer.
- → Wird auf AWS weltweit mit einer Betriebszeit von 99,99 % ohne geplante Ausfallzeiten bereitgestellt.
- → Basiert auf AWS IoT, für eine einfache Skalierung auf hunderttausende Endgeräte.



Forcepoint Data Security bietet eine umfassende Lösung für die Verwaltung globaler Richtlinien über alle Kanäle hinweg, einschließlich GenAI- und Cloud-Apps, Internet, E-Mail und Endpunkte. Mit einer umfangreichen Palette vordefinierter Vorlagen, Richtlinien und Klassifikatoren vereinfachen wir Ihre Arbeitslast, sorgen für ein optimiertes Incident-Management und ermöglichen es Ihnen, kritische Aufgaben zu priorisieren.

FUNKTIONEN	VORTEILE
Über 1.700 standardmäßig vordefinierte Klassifikatoren, Vorlagen und Richtlinien	Optimieren Sie die anfängliche DLP-Bereitstellung und die laufende Richtlinienverwaltung mit vordefinierten Richtlinien/Vorlagen/Klassifikatoren
Verarbeitung natürlicher Sprache (Natural Language Processing, NLP)	Unübertroffene Genauigkeit bei der Erkennung gängiger Datentypen (PII, PHI, PCI) auf der Grundlage von beschriebenen Inhalten mit über 300 vordefinierten Skripten in natürlicher Sprache
Erweiterte Erkennung echter Dateitypen	Identifizieren Sie über 900 Dateitypen – auch wenn sie umbenannt wurden, um nicht entdeckt zu werden – einschließlich OCR und Text in Bildern
Einheitliche Richtlinienkontrolle für CASB, SWG, E-Mails und Endgeräte	Verwalten Sie alle Kanäle von einer einzigen Richtlinie aus. Einmal schreiben, auf allen Ausgangskanälen bereitstellen
Einheitliche Berichterstattung über CASB, SWG, E-Mail und Endgeräte	Einheitliche Berichterstattung über CASB, SWG, E-Mail und Endgeräte
Standardmäßige Compliance-Richtlinien für über 150 Regionen weltweit, 90 Länder	Richtlinien sofort verfügbar, um die Einhaltung von Datenschutzbestimmungen in jeder wichtigen Region weltweit zu ermöglichen
Automatisierte Updates	Vereinfachen Sie die Datensicherheitsverwaltung mit automatisierten Updates der aktuellsten vordefinierten Richtlinien, Klassifikatoren und Vorlagen
Schneller Zugriff auf Warnmeldungen im Reporting-Dashboard (Cloud-Portal)	Sehen Sie alle Vorfälle und Warnmeldungen in nahezu Echtzeit von einem effizienten, organisierten Dashboard
Integriertes Reporting	Sehen Sie alle Berichte von DLP, Device Control und Risk-Adaptive Protection in einer integrierten Benutzeroberfläche
Vorfallspriorisierung	Sehen Sie sich die zehn wichtigsten Aktionen an, die sofortige Aufmerksamkeit erfordern. In Kombination mit Risk-Adaptive Protection kann die Anzahl der Vorfälle und der Schweregrad der Benutzer enthalten sein, um den Workflow zu priorisieren
Forensik	Bietet Transparenz in die Datenbewegungen, um Sicherheitsvorfälle zu untersuchen, die Ursache von Datenschutzverletzungen besser zu verstehen, detaillierte Vorfalluntersuchungen durchzuführen, die Richtlinieneffektivität zu verbessern und rechtliche / Compliance-Anforderungen zu unterstützen.
Over-the-Air-Upgrades	Beseitigt die Notwendigkeit, mit der IT bei Agentenupdates zu interagieren, verkürzt die Zeit für die Veröffentlichung von Updates
Transparenz der Agentenverwaltung	Verschaffen Sie sich einen Einblick in den Bereitstellungsstatus Ihrer Endgeräte und erkennen Sie Probleme mit Agenten schnell
Netzwerkverbindung für die Endbenutzer-Durchsetzung nicht erforderlich	Es muss keine Verbindung mit dem Netzwerk hergestellt werden, damit Endbenutzer einen Einblick in Sicherheitsverletzungen haben. Daten sind immer geschützt, unabhängig von der Netzwerkkonnektivität
Integration in die Gerätesteuerung	Erweitert die Datensicherheit und die Zugriffskontrolle für Wechselmedien auf einen einzigen Agenten und eine Benutzeroberfläche
Integration in Risk-Adaptive Protection	Kontextsensitive automatisierte Durchsetzung von Richtlinien in Echtzeit sowie Vorfallmanagement von einem einzigen Agenten/einer Benutzeroberfläche Erfordert eine separate SKU für Risk-Adaptive Protection (Add-on zu Forcepoint Data Security)
99,99 % Betriebszeit ohne geplante Ausfallzeiten	Wird weltweit auf AWS mit einer Betriebszeit von 99,99 % bereitgestellt