Logata
Digital Solutions

Produktgruppe: LogataNOC- ForcePoint

Forcepoint- DLP
Data Loss (Leak) Prevention

professioneller Datenschutz in einer Welt ohne Grenzen

Logata Digital Solutions GmbH - Hindenburgstraße 19 - 46395 Bocholt - www.logata.com - info@logata.com - +49 (0) 2871 2346 300
persönlicher Kontakt zur Produktgruppe: Peter Tiemann – peter.tiemann@logata.com - +49 (0) 2871 2346 346 Ver.07/2020

Produktgruppe: LogataNOC- ForcePoint

Forcepoint - Data Loss (Leak) Prevention (DLP)

Data protection in a zero-perimeter world (Datenschutz in einer Welt ohne Grenzen)

Beim Schutz der Unternehmensdaten steht der Mitarbeiter im Mittelpunkt

Datensicherheit ist eine unendliche Herausforderung. Einerseits müssen IT-Organisationen mit Vorgaben und Vorschriften Schritt halten, Schutz des geistigen Eigentums vor gezielten Angriffen und versehentlichen Verteilen vorsehen. Zum anderen müssen sie sich an „Makro-IT“ Anforderungen anpassen.
Neue Anforderungen, wie die Einführung von Cloud-Anwendungen, hybriden Cloud-Umgebungen und BYOD-Trends nehmen zu und hierdurch auch die Art und Weise, wie Daten Ihre Organisation verlassen können.
Diese wachsende Angriffsfläche stellt die größte Herausforderung für den Schutz kritischer Daten dar.

Datensicherheitsteams benehmen
Der scheinbar logischste Ansatz ist, Daten zu verfolgen: also Finden, Katalogisieren und Steuern.
Dieser traditionelle Ansatz zum Datenverlust Prävention ist heute nicht mehr wirksam, da er die größte Variable in der Datensicherheit schlicht weg ignoriert - Ihre Mitarbeiter.
Anstatt sich ausschließlich auf das Thema Daten zu konzentrieren, sollte Ihr Sicherheit-Konzept bereits bei den Menschen beginnen und auch enden. Der Schlüssel ist es, Einblick in den Benutzer zu gewinnen, Interaktionen mit Daten und Anwendungen zu beobachten und zu lernen. Sobald dieses erreicht ist, können Sie eine Steuerungsebene anwenden, die auf den spezifischen Arbeitsabläufen der Benutzer, des Risikos und der Sensitivität und/oder den Wert der Daten, basiert.
Das Datenschutzprogramm einer Organisation muss den menschlichen Punkt berücksichtigen - die Schnittstelle zwischen Benutzern, Daten und Netzwerken klar im Auge haben.
Darüber hinaus muss das Unternehmen wachsam gegenüber Daten bleiben, wenn diese sich im gesamten Unternehmen bewegen, und die Personen hervorheben, die Daten erstellen, benutzen und verbreiten.

Basis des Datenschutzes:

- **Sichern Sie unternehmenskritische Daten** mit einem einzigen zentralen Datenpunkt, den alle Applikationen welche Ihre Mitarbeiter zum Erstellen, Bearbeiten und Teilen von Daten nutzen müssen.
- **Schützen Sie geistiges Eigentum** durch die Nutzung unsers fortschrittlichen DLP Sytems, welches analysiert, wie Menschen Daten verwenden, Ihre Mitarbeiter anleitet gute Entscheidungen bei der Nutzung Daten und Prioritäten zu treffe, um Vorfälle nach Risiken zu minimieren.

Sichtbarkeit & Kontrolle überall dort, wo Menschen regelmäßig tätig sind und vorrübergehend arbeiten

- Cloud-Anwendungen (unterstützt von Forcepoint CASB)
- Endpunkt
- Netzwerk
- Entdeckung

Forcepoint DLP begegnet menschengemachte Risiken durch Sichtbarmachung und Kontrolle überall dort vor, wo Ihre Mitarbeiter arbeiten und wo sich genutzte Daten befinden. Sicherheitsteams bewerten individuelle Benutzerrisiken, um sich auf die wichtigsten Ereignisse zu konzentrieren und die Einhaltung von Unternehmenseigenen und globalen Datenvorschriften zu beschleunigen.

Produktgruppe: LogataNOC- ForcePoint

Beschleunigen Sie die Einhaltung Ihrer Schutzvorgaben

Moderne IT-Umgebungen überfordern Unternehmen in vielfältiger Weise bei der Einhaltung von firmeneigenen und globalen Datenschutzbestimmungen, insbesondere bei einer umfänglichen Nutzung von Cloud Anwendungen und beim Einsatz von mobilen Arbeitskräften.
Viele Sicherheitslösungen bieten eine einfache integrierte DLP-Lösung, die nur sehr unzureichend einen Schutz Ihrer Daten vornehmen kann.
Ihre Sicherheitsteams sind in vielen Fällen mit unerwünschter hoher Komplexität bei dem Thema konfrontiert und verursachen dadurch erhebliche Kosten bei der Durchsetzung und Verwaltung Ihrer Schutzrichtlinien für den Endpunkt-Bereich, Cloud-Anwendungen und in den genutzten Netzwerken.

Forcepoint DLP
beschleunigt Ihre Bemühungen zur Umsetzung firmeneigener und globaler Vorschriften, inkl. einer zentralen Kontrolle über Ihre IT-Umgebung
Forcepoint DLP
schützt sensible Kundendaten effizient, gibt Informationen zu regulierten Daten, damit Sie sicher sein und laufend Ihre Kontrollanstrengungen nachweisen können.

- Weitreichende Abdeckung bei Regularien, zur schnellen Erfüllung und Einhaltung von mehr als 370 Richtlinien an regulatorischen Anforderungen von 83 Ländern.
- Suchen und korrigieren Sie regulierte Daten in den Netzwerken inkl. Cloud- und Endpunkterkennung.
- Zentrale Kontrolle und konsistente Richtlinien in Ihrer gesamten IT-Umgebung.

Befähigen Sie Ihre Mitarbeiter, Daten zu schützen

DLP mit einer vorbeugenden Kontrolle frustrierter Benutzer, die mit der alleinigen Absicht agieren, ihre Sicherheitssysteme zu umgehen. Fehlende Beobachtung führt zu vermietbaren Risiken und ermöglicht ggf. „versehentliche“ Datenverbreitung.

Forcepoint DLP erkennt Unternehmensmitarbeiter als Hauptpunkt der heutigen Cyber-Bedrohungen.

- Finden und kontrollieren Sie Daten überall dort, wo diese sich befinden und bewegen; ob in der Cloud, im Netzwerk, per E-Mail und am Endpunkt.

- Trainieren Sie Mitarbeiter, nutzen Sie gezielte Infonachrichten an Ihre Mitarbeiter, um Sie klug bei Benutzeraktionen anzuleiten, schulen die Richtlinie Ihres Unternehmens und überprüfen Sie das Vorgehen der Mitarbeiter bei der Interaktion mit kritischen Daten.

- Arbeiten Sie sicher mit vertrauenswürdigen Partnern, über richtlinienbasierte automatische Verschlüsselung, zusammen, so können Sie Daten außerhalb Ihrer Organisation optimal schützen.

- Automatisieren Sie die Datenkennzeichnung und -klassifizierung durch Integration mit führenden Datenklassifizierungslösungen von Drittanbietern (z. B. Microsoft Information Protection, Titus, Boldon James).

Erweiterte Erkennung und Steuerung die folgenden Daten

Böswillige und versehentliche Datenverletzungen sind komplex Vorfälle, keine einzelnen Ereignisse.
Forcepoint DLP hat sich als Lösung bewährt, die Analysten wie Gartner, Radicati und andere dazu bewegten, sie als führend in der Branche zur bewerten.
Die DLP-Angebote von Forcepoint sind in zwei Versionen verfügbar:
„DLP für Compliance“ (Einhaltung von Richtlinien) und „DLP for Intellectual Property (IP) Protection“ (Schutz für geistiges Eigentum (IP)).

Logata
Digital Solutions

Produktgruppe: LogataNOC- ForcePoint

Forcepoint DLP for Compliance bietet Ihnen wichtige Informationen und befähigt Sie zur Einhaltung von Funktionen wie:

- Die optische Zeichenerkennung (OCR) identifiziert Daten /Datenbewegungen auch in Bild-Dateien
- Robuste Identifikation von persönlich identifizierbar Information (PII), bietet Datenvalidierungsprüfungen, Erkennung realer Namen, Näherungsanalyse und Kontext-IDs.
- Durch die benutzerdefinierte Verschlüsselungsidentifikation werden verborgene Daten angezeigt und ermöglichen die Entdeckung und anwendbare Kontrollen.
- Kumulative Analyse für eine Drip-DLP-Erkennung (das h. auch Daten, die langsam das System verlassen werden erkannt).
- Integration von „Microsoft Information Protection“ zur Analyse verschlüsselter Dateien und ermöglicht somit DLP zur Kontrolle solcher Daten.

Forcepoint DLP für IP-Schutz enthält ebenfalls die oben aufgeführten Funktionen, zusätzlich enthält sie die fortschrittlichste Erkennung und Kontrolle eines potenziellen Datenverlusts mit Funktionen wie:

- Durch maschinelles Lernen können Benutzer das System trainieren, relevante nie zuvor gesehene Daten zu identifizieren. Benutzer versorgen das DLP System mit positiven und negativen Beispielen zu Kennzeichen bei ähnlichen Geschäftsdokumenten, Quellcode und mehr.
- Fingerabdrücke ermöglichen eine klare Zuordnung von Dateneigentümern bei strukturierten und unstrukturierten Daten, Datentypen zu definieren und zu identifizieren und dieses über vollständige und teilweise Übereinstimmungen Geschäftsdokumente hinweg,
  Entwerfen Sie Pläne und Datenbanken und wenden Sie dann Kontrollmechanismen oder Richtlinie an, die mit den Daten übereinstimmen.
- Analytics identifiziert Änderungen im Benutzerverhalten bezieht sich auf Dateninteraktion (wie z.B. eine erhöhte Nutzung der persönlichen E-Mail).

Reagieren und Risiken beseitigen

Bei herkömmliche DLP Ansätzen werden regelmäßig die Benutzern mit „false positiv“ überlastet und überschatten die Angaben zu wirklich gefährdeten Daten. Forcepoint DLP bietet hingegen erweiterte Analyse zur Korrelation von nicht relevanten DLP Ereignisse bei priorisierten Vorfällen. Incident Risk Ranking (IRR), was mit Forcepoint DLP-fuses geliefert wird,ermöglicht, detektierte DLP Vorfälle (Indikatoren), durch die Nutzung von zentralen Datennetzwerken, in der Wahrscheinlichkeit von Datenrisikoszenarien (z. B. Daten Diebstahl und korrumpierte Geschäftsprozesse. Einzuschätzen und zu unterscheiden.

- Konzentrieren Sie Ihre Reaktionsteams auf das größte Risiko durch Hervorheben und Kenntlichmachung von Vorfällen mit Priorität, für die verantwortlichen Personen (z.B. kritische Risikodaten und allgemeine Verhaltensmuster zwischen Benutzern)
- Untersuchen und antworten Sie mit Workflows, die verknüpft sind mit den unterschiedlichen Ereignissen, Kontext der gefährdeten Daten zeigen. Stellen Sie den Analysten die Informationen zur Verfügung, die Ihr Team zum Handeln benötigt.
- Schützen Sie die Privatsphäre der Benutzer mit Anonymisierungsoptionen und Zugangskontrollen.
- Fügen Sie, durch eine tiefe Integration von „Forcepoint Insider Threat“ und „Forcepoint Behavioral Analytics“, den Datenkontext in eine breitere Benutzeranalyse ein.

Sichtbarkeit überall dort, wo Ihre Leute arbeiten; Kontrolle überall dort, wo sich Ihre Daten befinden

Die heutigen Unternehmen sind mit Herausforderungen konfrontiert, denen sich schutzwürdige Daten in unterschiedlichen Umgebungen befinden. Dieses erfordert einen Schutz von Daten an Orten, die nicht durch Sie verwaltet werden oder an deren Sie nicht Eigentümer sind. Forcepoint DLP for Cloud-Anwendungen erweitert Analyse- und DLP-Richtlinien auf kritische Clouds Anwendungen, damit Ihre Daten geschützt sind, wo immer sie sich befinden.

- **Identifizieren und Schützen von Daten** in Cloud-Anwendungen, Netzwerkdatenspeicher, Datenbanken und verwaltete Endpunkte.
- **Erhalten Sie Ihre Übersicht** bei Uploads und Downloads sowie bei Weitergabe von Daten (Teilen) und bei Speicherung von Daten durch die beliebtesten Unternehmens-Cloud-Apps wie: Office 365, Google verwendet Apps, Box, Salesforce und mehr.
- Vereinheitlichen Sie die Durchsetzung von Richtlinien über eine einzige Konsole, um Ihre Datenerkennungsrichtlinien auf alle Kanäle zu definieren und in der Cloud, Netzwerken und Endpunkten, anzuwenden.
- Eine von Forcepoint gehostete Lösung, biete eine DLP Lösung für Unternehmen mit erweiteren Funktionen wie Integration von Fingerabdrücken und maschinelles Lernen bei Cloud-Anwendungen.

Forcepoint DLP umfasst erweiterte Analyse- und Regulierungsfunktionen mit Richtlinienvorlagen für jeden Einsatz von einem einzigen Verwaltungspunkt aus. Unternehmen können wählen die bereitgestellten Optionen für ihre IT-Umgebung frei auswählen.

Produktgruppe: LogataNOC- ForcePoint

Anhang A und B) Übersicht über die Komponenten der DLP-Lösung

Forcepoint DLP – Endpoint (Endpunkt) schützt Ihre kritischen Daten auf Windows- und Mac-Endpunkten im und außerhalb des Unternehmensnetzwerks. Es umfasst erweiterten Schutz und Kontrolle für ruhende, bewegte und verwendete Daten. Es lässt sich umfänglich in Microsoft integrieren. Schutz von Informationen, Analysieren verschlüsselter Daten und Anwenden mit geeigneten DLP-Steuerelementen. Aktiviert die Selbstkorrektur von Mitarbeitern (Verbessert das Mitarbeiterverhalten)
Die Datenrisiko-Bewertung basierend auf den Leitlinien des DLP-Coaching-Dialogs. Die Lösung überwacht Web-Uploads, einschließlich HTTPS, sowie Uploads zu Cloud-Diensten wie Office 365 und Box Enterprise. Vollständige Integration mit Outlook-, Notes- und E-Mail-Clients.

Forcepoint DLP - Cloud- Applications (Anwendungen) wird von Forcepoint CASB unterstützt und erweitert die umfangreiche Analyse und Einzelsteuerung von Forcepoint DLP für die wichtigen Cloud-Anwendungen, einschließlich Office 365, Salesforce, Google Apps, Box, ServiceNow und mehr.

Forcepoint DLP – Discovery (Suche) identifiziert und sichert vertrauliche Daten in Ihrem Netzwerk sowie in der Cloud gespeicherte Daten sowie Dienste wie Office 365 und Box Enterprise. Die fortschrittliche Fingerabdrucktechnologie identifiziert und reguliert schutzbedürftige Daten.
Gespeichertes schutzwürdiges Daten-Eigentum wir durch Anwendung geeigneter Verschlüsselungen und Kontrollen gesichert.

Forcepoint DLP - Network (Netzwerk) liefert die starken Durchsetzungsposition, um den Diebstahl von Daten im Versand per E-Mail und über Web-Kanäle zu stoppen. Die Lösung hilft dabei, böswilligen und versehentlichen Datenverlust durch Angriffe von außen oder über das Internet sowie über wachsende Insider-Bedrohungen zu identifizieren und zu verhindern. OCR (Optical Character Recognition) ermöglicht DLP die Erkennung von Daten in einem Bild. Stoppen Sie den Diebstahl von Datensätzen in einer Reihenfolge und erkennen Sie andere Benutzerverhalten mit hohem Risiko.

Funktionstabelle der DLP-Lösungskomponenten

	Forcepoint DLP – Endpoint	**Forcepoint DLP – Cloud Applications**	**Forcepoint DLP – Discover**	**Forcepoint DLP – Network**
Was sind die Primärfunktion?	Sammlung von Informationen zum Endpunkt des Benutzers	Erkennen von Daten und Durchsetzung von Richtlinien in der Cloud oder mit Cloud-bereitgestellten Anwendungen	Entdecken, Scannen und Korrektur von Daten ohne Client-beeinflussung im Rechenzentren	Sichtbarmachen und Kontrolle von Daten bei Ihrer Bewegung über das Web und E-Mail-Verkehr
Wo werden die Daten entdeckt und final geschützt?	Windows-Endpunkte MacOS-Endpunkte Linux-Endpunkte	Exchange Online Sharepoint Online Box	Lokale Dateiserver (File-Server) und Netzwerkspeicher-Systeme Sharepoint Server Exchange Server	
Wo werden Daten bei ihren Bewegungen geschützt?	E-Mail, Web: HTTP (S), Drucker, Wechselmedien, Mobile Geräte, Dateiserver / NAS	Uploads, Downloads & Sharing für Office 365, Google Apps, Salesforce.com, Box & ServiceNow		E-Mail / Mobile E-Mail / ActiveSync-Proxy Web: HTTP (S) ICAP
Wo werden Daten bei ihrer Verwendung geschützt?	IM, VOIP-Dateifreigabe, Anwendungen (Cloud-Speicher Clients), OS-Zwischenablage	Während der Zusammenarbeit Aktivitäten mit Cloud-Anwendung		
Incident Risk Ranking * (Verminderung von Risiken)	Inklusive	Inklusive	Inklusive	
Optical Character recognition OCR) (optische Buchstaben-Erkennung)			Inklusive	Inklusive
Datenklassifizierung & Kennzeichnungsintegrationen	Microsoft-Informationsschutz, Boldon James, Titus			
Welche Daten können Fingerabdruck geschützt sein? *	Strukturiert (Datenbanken), unstrukturiert (Dokumente), binär (nicht textuelle Dateien)			
Einheitliches Regelwerk-Management	Richtlinienkonfiguration und Durchsetzung über eine einzige Konsole			
Robuste Richtlinienbibliothek	Ermittlung und Durchsetzung aus einer breiten Bibliothek von Compliance-Richtlinien			

Es ist Zeit für menschlich-orientierte Online-Sicherheit.