FORCEPOINT
POWERED BY Raytheon

Datasheet

APX Data Loss Prevention (DLP)-Module

VERSCHAFFEN SIE SICH EINEN ÜBERBLICK, UND KONTROLLIEREN UND SICHERN SIE IHRE EIN- UND ABGEHENDEN VERTRAULICHEN DATEN, INDEM SIE ENTERPRISE DLP-FUNKTIONALITÄT AUF IHRE WEB- UND E-MAIL-KANÄLE ERWEITERN

Von einer Schädigung des Rufs bis hin zu behördlich auferlegten Bußgeldern und Strafen – eine Datenpanne kann verheerende Auswirkungen auf Ihr Unternehmen haben. Und da Mitarbeiter immer mobiler werden, benötigen Sie unbedingt einen Überblick über die vertraulichen Daten, die in Ihr Netzwerk gelangen bzw. dieses verlassen.

Um Datendiebstahl zu verhindern, die Einhaltung von Compliance-Vorschriften nachzuweisen und Ihre Marke sowie Ihr geistiges Eigentum zu schützen, müssen Ihre IT-Schutzmaßnahmen auch außerhalb Ihres Unternehmens funktionieren. Sie müssen Ihre vertraulichen Daten in Web- und E-Mail-Kanälen, die von Ihren mobilen Mitarbeitern außerhalb des Netzwerks verwendet werden, absichern. Indem Sie Ihre Schutzmaßnahmen um Enterprise-DLP-Funktionen erweitern, können Sie dies für sowohl Web- als auch E-Mail-Kanäle sowie in vielen weiteren Bereichen erreichen.

WARUM FORCEPOINT™ WEB- UND E-MAIL-DLP-MODULE?

Die Forcepoint Web-DLP- und E-Mail-DLP-Module nutzen eine äußerst präzise, branchenführende Technologie, um Compliance-Anforderungen und behördliche Vorschriften problemlos zu erfüllen, indem sie DLP-Funktionalität der Enterprise-Klasse auf Web- und E-Mail-Kanäle erweitern. Sie bieten jederzeit einen vollen Überblick über die Übertragung vertraulicher Daten - sowohl in Echtzeit als auch vergangenheitsbezogen. Mit einer ganzen Reihe einzigartiger Funktionen wie einer optischen Zeichenerkennung (OCR) oder einer Identifizierung individueller Verschlüsselungen hebt Forcepoint DLP der Enterprise-Klasse auf ein ganz neues Niveau.

- Anhand einer umfangreichen Bibliothek vordefinierter Templates können Sie Richtlinien zeitnah einrichten und implementieren, um einen potenziellen Diebstahl Ihrer wichtigsten Daten zu identifizieren und zu verhindern.
- Mit dem benutzerfreundlichen Assistenten ist Ihr bestehendes Personal in der Lage, die DLP-Web- und E-Mail-Module spielend leicht zu implementieren.
- Verschaffen Sie sich einen Überblick über die Daten, die über Web- und E-Mail-Kanäle in Ihr Netzwerk gelangen und dieses verlassen.
- Verhindern Sie mit „Drip-DLP“ einen langsamen Diebstahl von Kreditkarten- oder anderen Datensätzen, die jeweils einzeln oder in geringen Mengen ausgeschleust werden.
- Stoppen Sie Bedrohungen durch Innentäter dank verhaltensorientierter Analysen, die sämtliche Personen identifizieren, die eine Gefahr für Ihr Unternehmen darstellen könnten.
- Eine optische Zeichenerkennung (OCR) identifiziert Text in Bilddateien und verhindert so, dass Daten über Screenshots, Fotos oder andere Bilddateien gestohlen werden.
- Mit AP-EMAIL können Sie DLP-Richtlinien auf Microsoft Office 365-Datenverkehr anwenden. So können Sie neue Technologien einführen, ohne die Sicherheit Ihrer vertraulichen Daten zu gefährden.
- Durch eine Bereinigung vertraulicher Daten erhalten Sie die Möglichkeit, diese, sobald sie gefunden werden, zu prüfen, zu blockieren, zu erlauben, in Quarantäne zu stellen*, zu verschlüsseln* oder eine Warnmeldung bzw. sonstige Mitteilung zu verschicken. (*Nur für das E-Mail-DLP-Module)

EINE LÖSUNG, DIE SICH SCHNELL IMPLEMENTIEREN LÄSST UND VERHINDERT, DASS MEINE VERTRAULICHEN DATEN MEIN NETZWERK ÜBER WEB- ODER E-MAIL-KANÄLE VERLASSEN

Dank einer umfangreichen Bibliothek vordefinierter Templates und Richtlinien ist das System schnell aufgesetzt und beginnt sofort, Ihre vertraulichen Daten zu schützen.

VERWALTUNG SOLL VON BESTEHENDEN MITARBEITERN ÜBERNOMMEN WERDEN

Die Forcepoint TRITON-Architektur ist vollständig integriert und führt das Berichtswesen und die Daten- und Richtlinienverwaltung für all Ihre Web-, E-Mail-, Daten-, Cloud- und Mobil-Lösungen in einer einzigen Benutzeroberfläche zusammen.

NUTZER MIT RISKANTEM VERHALTEN IDENTIFIZIEREN UND AUFKLÄREN

Verhaltensorientierte Analysen identifizieren und kennzeichnen Personen, die das Unternehmen aufgrund von schlechten Angewohnheiten bei der IT-Nutzung gefährden könnten, ebenso wie unzufriedene Mitarbeiter.

ICH MÖCHTE WISSEN, WELCHE DATEN WIE MEIN NETZWERK VERLASSEN

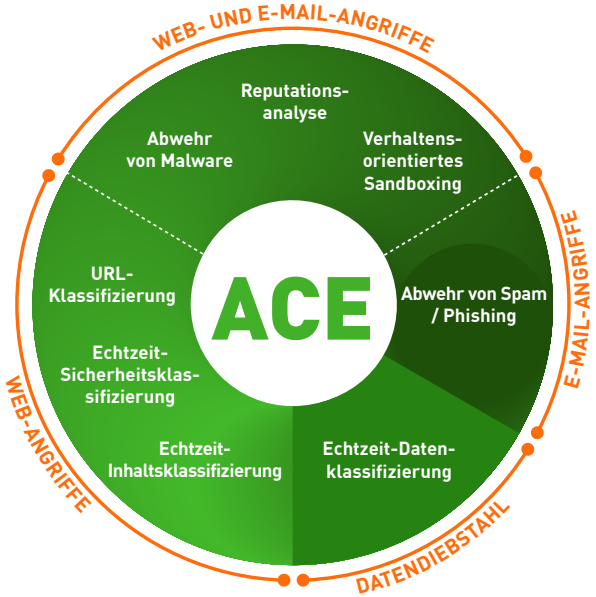
Mit Forcepoint Web- und E-Mail-DLP erhalten Sie einen Überblick darüber, welche vertraulichen Daten über Ihre Web- und E-Mail-Kanäle kommen und gehen.

ÜBERBLICK ÜBER VERTRAULICHE DATEN IN BILDDATEIEN EINGESCANNTER ÄLTERER DATENSÄTZE

Die von Forcepoint gebotene optische Zeichenerkennung (OCR) identifiziert Text in Bilddateien und kann Richtlinien durchsetzen, die verhindern, dass in gescannten Bildern gefundene vertrauliche Daten Ihr Netzwerk verlassen.

ICH MUSS SICHERSTELLEN, DASS REGULIERTE DATEN MEIN NETZWERK NICHT IN GERINGEN MENGEN VERLASSEN

Stoppen Sie tröpfchenweisen, allmählichen Datenabfluss mit Forcepoint Drip-DLP. Durch eine Untersuchung kumulativer Ereignisse über einen längeren Zeitraum hinweg werden langsame Datenlecks („Data Drip“) erkannt, bei denen Datensätze oder Kreditkartennummern einzeln oder in sehr geringen Mengen ausgeschleust werden.



DER FORCEPOINT-UNTERSCHIED:

ACE (Advanced Classification Engine)

Forcepoint ACE bietet integrierte, kontextbezogene Echtzeit-Verteidigungsmaßnahmen für Web-, E-Mail-, Daten- und mobile Sicherheit. Das System nutzt eine kombinierte Risikobeurteilung sowie vorausschauende Analysen, um eine maximal effektive Sicherheit zu gewährleisten. Zudem ermöglicht es eine Eindämmung potenzieller Schäden durch eine Analyse ein- und abgehenden Datenverkehrs über datensensitive Maßnahmen, die branchenführenden Schutz vor Datendiebstahl bieten. Klassifizierungen für Echtzeitsicherheit sowie Daten- und Inhaltsanalysen, die aus vielen Jahren der Forschung und Entwicklung hervorgegangen sind, versetzen ACE in die Lage, jeden Tag mehr Bedrohungen zu erkennen als herkömmliche Antivirus-Programme (der Nachweis hierzu wird täglich unter http://securitylabs.Forcepoint.com aktualisiert). ACE ist die primäre Schutzstruktur, auf der alle Forcepoint TRITON®-Lösungen aufbauen. Sie wird durch die Forcepoint ThreatSeeker® Intelligence Cloud unterstützt.

KONTAKT

www.forcepoint.com/contact

ERFAHREN SIE MEHR

[DATASHEET_MODULE_DLP_DE]-100007DE.011416

FORCEPOINT
TRITON® APX