Datenschutzlösungen für Unternehmen im Überblick

Die sechs führenden Anbieter

Forcepoint

Broschüre

Inhalt:

03 Einführung

04 Bewertungskriterien: Worauf Sie achten müssen (und wie Sie danach fragen)

07 Ihre Optionen im Überblick: eine Wettbewerbsanalyse

08 Die Lösungen der führenden Unternehmen auf einen Blick

09 Was Forcepoint besonders macht

Die Relevanz von Datenschutz in Unternehmen kann in der heutigen Zeit gar nicht hoch genug bewertet werden. Hier geht es um sensible Werte: geistiges Eigentum, Wettbewerbsvorteile, den Wert einer Marke, finanzielle Stabilität und das Vertrauen der Kunden. Wenn so viel auf dem Spiel steht, ist die Auswahl eines Partners im Bereich Datenschutz (oder der Wechsel zu einem neuen Partner) eine Entscheidung, die gut überlegt sein will. Bei der Entscheidungsfindung soll Ihnen dieser Leitfaden eine Hilfe sein – hier erhalten Sie einen detaillierten Überblick über die marktführenden Lösungen für Unternehmen.

In dieser Broschüre erfahren Sie,

- welche Kriterien beim Vergleich von Lösungen besonders relevant sind
- wie Sie Ihre Fragen formulieren müssen, um eine aussagekräftige Antwort zu erhalten
- wie sich die Lösungen unterschiedlicher Anbieter konkret voneinander unterscheiden.

Worauf Sie achten müssen (und wie Sie danach fragen):

In den meisten Unternehmen erfolgt der Wechsel zu einer neuen Datensicherheitslösung nicht punktuell, sondern sukzessive. Daher sollten Sie genauestens darüber informiert sein, wie die Lösungen in den jeweiligen Phasen der Zusammenarbeit funktionieren.

Auf den folgenden Seiten finden Sie eine Zusammenfassung von 11 relevanten Aspekten, die Sie im Entscheidungsprozess berücksichtigen sollten. Es sind auch Formulierungsvorschläge für Fragen enthalten, mit denen Sie alle relevanten Informationen ermitteln können.

Unkomplizierte Implementierung

Die Implementierungen einer neuen Datenschutzlösung für Ihr Unternehmen muss kein gänzlicher Neustart sein. Achten Sie auf mögliche Schnittstellen mit Ihrer aktuellen Lösung und erfragen Sie, ob die neue Lösung mit den in Ihrem Unternehmen verwendeten Systemen kompatibel und darin integrierbar ist. Außerdem können Beratungsdienste Ihnen helfen, den Zugang zu Tools zu kontrollieren und neue Richtlinien durchzusetzen, für die keine oder nur wenige Anpassungen erforderlich sind – so können Sie möglichst die neue Lösung möglichst zeitnah implementieren.

Support und Service

Um möglichst schnell von einer neuen Lösung profitieren zu können, sollten Sie sich intensiv mit deren Funktionen befassen und gleichzeitig die nötigen Vorbereitungen für den Einsatz in Ihrem Unternehmen treffen. Der direkte Kontakt zu einem Account Manager kann hierbei ein entscheidender Faktor sein: Sie erhalten wertvolle Ratschläge, mit denen Sie das Potenzial Ihres neuen Tools schon bald voll ausschöpfen können. Auch die Entscheidung für ein Rundum-Serviceangebot zur kontinuierlichen Verwaltung, Bewertung und Optimierung Ihrer Konfiguration trägt zu einem größtmöglichen Nutzen bei.

Fragen Sie nach:
Wird unser Unternehmen von einem **Customer Success Manager oder einem Technical Account Manager betreut?**

Bereitstellungsmodelle

Viele Unternehmen möchten eine Datenschutzlösung zunächst lokal implementieren. Achten Sie dennoch darauf, dass Ihre Lösung auch Cloud- oder Hybridfunktionen unterstützt – so können Sie diese entsprechend skalieren und künftige Verzögerungen verhindern.

Benutzerfreundlichkeit

Für den Datenschutz in Ihrem Netzwerk, an Endpunkten und in der Cloud unterschiedliche Tools zu nutzen und zu verwalten ist umständlich. Eine lückenlose, effiziente Strategie lässt sich so kaum realisieren. Sie sollten sich für eine Lösung entscheiden, mit der Sie jederzeit nachvollziehen können, wie Ihre Daten auf Benutzerebene genutzt, bewegt und geschützt werden.

Fragen Sie nach:
Können die Richtlinien **für alle Bereiche unseres Unternehmens** zentral gesteuert werden?

Compliance

Die gesetzlichen Vorgaben sehen vor, dass Unternehmen alle Funktionen unabhängig prüfen, Berichte erstellen und den Datenfluss anhand vordefinierter Richtlinien kontrollieren können müssen. Wenn Sie Aktivitäten nach Benutzer und nicht nur einzelne Ereignisse nachvollziehen können, leisten Sie sogar mehr als das bloße Einhalten von Vorschriften. So können Sie Ihre Prozesse sicher verwalten.

Fragen Sie nach:
Können die für Audits und Compliance benötigten Berichte einfach verwaltet werden?

Prüfen und Abwehren

Gibt es Funktionen, mit denen Vorfälle von Datenverlusten im Nachhinein geprüft und Daten genau zum Zeitpunkt des Angriffs blockiert werden können, um diese kanalübergreifend zu schützen? Lernen Sie aus Fehlern der Vergangenheit, um Ihre Richtlinien zur Bedrohungsabwehr für die Zukunft zu optimieren.

Einblicke in Benutzeraktivitäten

Die Nachverfolgung individueller Benutzeraktivitäten ist entscheidend für die Erkennung von a) Versuchen, Daten über unterschiedliche Kanäle auszuschleusen (z. B. E-Mail, Cloud, Internet, Endpunkte) und b) Zugangsdaten, die durch Phishing oder andere Angriffe entwendet wurden.

Fragen Sie nach:
Kann ich Bedrohungen auf Benutzerebene erkennen?

Flexible Anpassung benutzerspezifischer Anwendungen

Alle benutzerspezifischen Anwendungen, die für die Zusammenarbeit mit anderen Unternehmen, Partnern bzw. Dritten genutzt werden, sollten in Ihrer Datenschutzstrategie berücksichtigt werden. Daher müssen auch in Ihrer neuen Lösung zeitnah Kontrollen für diese Anwendungen implementiert werden können.

Fragen Sie nach:
Wie transparent sind Ihre Cloud-Anwendungen und werden benutzerspezifische Anwendungen einbezogen?

Entwicklungsplan

Da Ihre Daten immer wieder neuen Bedrohungen ausgesetzt sind, bedarf es einer dynamischen Lösung, die sich stets an die Anforderungen des Marktes anpassen kann. Auch wenn eine Lösung aktuell Ihre Anforderungen erfüllt, sollten Sie erfragen, welche Maßnahmen für die Zukunft geplant sind, um die Relevanz von Innovation und Anpassung einzuordnen.

Leistungsanalysen

Analysten wie Gartner Inc. und Forrester Research kennen die Funktionen, Produktentwicklungspläne und weitere Details der unterschiedlichen Lösungen – Informationen, die Sie nur mit viel Glück auf einer Website oder im Rahmen eines Verkaufsgesprächs erhalten würden. Die Daten dieser Analysten erleichtern Ihnen einen aussagekräftigen Vergleich unterschiedlicher Tools.

Preistransparenz

Die Zusammensetzung der unterschiedlichen Lösungen ist komplex, zumal einige Funktionen (manchmal sogar die Funktion, die als Alleinstellungsmerkmal des Produkts beworben wird) möglicherweise nicht in allen Lizenzvarianten enthalten sind. Vergewissern Sie sich, ob im angebotenen Preis alle für Ihr Unternehmen relevanten Funktionen enthalten sind.

Wir möchten Sie mit der Vielzahl der zu beachtenden Aspekte nicht überfordern. Es ist jedoch wichtig, den Umfang der unterschiedlichen Lösungen grundlegend zu verstehen und mit den eigenen Bedürfnisse abgleichen zu können, *damit* Ihre Erwartungen nach der Implementierung nicht enttäuscht werden. Falls Sie unsicher sind, welchen Aspekt Sie zuerst ansprechen sollen, kann Ihnen die folgende Übersicht dabei helfen, weiter ins Detail zu gehen.

Ihre Optionen im Überblick

	DIGITAL GUARDIAN	FORCEPOINT	MCAFEE	NETSKOPE	PROOFPOINT	SYMANTEC
Priorisierung von Warnungen	●	●	●	●		●
Automatisierte Durchsetzung von Richtlinien	●	●	●	●	●	●
Schutz von Cloud-Anwendungen		●	●	●	●	●
Schutz der Cloud		●	●	●	●	●
Kompatibilität mit Anbietern von Datenklassifizierung		●				
Kombinierter Netzwerk- und Endpunktschutz	●	●	●			●
Unterstützung mehrerer Datenbanken		●	●			●
Datenerkennung in allen Umgebungen		●	●			●
Integration von Datenschutz in allen Bereichen – Internet, E-Mail, Netzwerke, Endpunkte und Cloud		●				
Drip-DLP		●	●			●
Native Verhaltensanalysen		●				
Native Behebungsmaßnahmen		●	●	●	●	●
Lokale, Cloud-basierte und Hybridlösung	●	●	●			●
Netzwerkexterne Durchsetzung von Richtlinien		●				
Risikogerechter Schutz		●	●			●
Risikobasierte Durchsetzung von Richtlinien		●				
Einfache Verwaltung in allen Umgebungen dank zentraler Konsole		●	●			●
Daten-Fingerprinting und optische Zeichenerkennung (strukturiert und unstrukturiert)	●	●	●			●
Einheitliche Durchsetzung von Richtlinien		●				●

Die Lösungen der führenden Unternehmen auf einen Blick

Digital Guardian ist eine Plattform für Datensicherheit, die lokal, in der Cloud und als Hybridlösung implementiert werden kann. Der zeitliche und logistische Aufwand für die Einrichtung einer Umgebung ist mit dem anderer Anbieter vergleichbar, allerdings sind die Funktionen weniger umfangreich. Daher ist diese Lösung in erster Linie für Unternehmen mit verhältnismäßig unkomplizierten Datenschutzanforderungen geeignet.

McAfee legte den Schwerpunkt bisher auf die Web-Sicherheit, konzentriert sich jetzt aber verstärkt auf Cloud- und Datensicherheit und bietet umfangreiche Datenschutz- und Antiviruslösungen mit separaten Konsolen zur Kontrolle von Netzwerken, Endpunkten und der Cloud. Diese Lösung priorisiert bedrohungsorientierte Richtlinien, die unabhängig vom Benutzerverhalten konsequent durchgesetzt werden.

Netskope ist eine CASB-Lösung mit URL-Filterfunktionen, die vor allem darauf ausgerichtet ist, Daten vor dem Herausschleusen aus der Cloud zu schützen. Da die umgebungsübergreifenden Funktionen dieser Lösung begrenzt sind, ist sie vor allem für Unternehmen geeignet, die ihre bestehende Lösung um eine Cloud-orientierte Lösung erweitern möchten.

Proofpoint ist eine Cyber-Sicherheitslösung für den Datenschutz in mobilen oder Remote-Umgebungen, z. B. Cloud, E-Mail, Internet oder Social Media. Die Stärken dieser Lösung liegen in den Bereichen E-Mail-Sicherheit und Abwehr von Phishing-Bedrohungen. Daher ist sie vor allem für Unternehmen geeignet, die eine Cloud-orientierte Lösung benötigen.

Symantec (NortonLifeLock Inc.) bietet eine umfassende Lösung für Datensicherheit mit zuverlässigen umgebungsübergreifenden Funktionen. Sicherheitsrichtlinien werden einheitlich, umgebungsübergreifend und unabhängig vom Benutzerverhalten oder von der Risikostufe durchgesetzt. Gerade für mittelständische Unternehmen könnte die Verwaltung dieser Lösung zeit- und ressourcenaufwändig sein.

Was Forcepoint besonders macht

Forcepoint kombiniert umgebungsübergreifende Data Loss Prevention, die Analyse von Benutzer- und Systemverhalten (UEBA) und die risikogerechte Durchsetzung von Richtlinien auf einzigartige Weise. Wir bieten Unternehmen, die aktuell oder in naher Zukunft eine digitale Transformation durchlaufen, daher im Vergleich die umfassendste Datensicherheitslösung. Nur wir können Richtlinien basierend auf der Risikostufe des Benutzers dynamisch anpassen und durchsetzen, das Herausschleusen von Daten verhindern, Fehlalarme reduzieren, Workflows optimieren und wertvolle Ressourcen dorthin zurückholen, wo sie von maximalem Nutzen sind.

Erste Schritte mit Forcepoint

Durch die schrittweise Implementierung von Forcepoint soll unser Partner möglichst schnell von der neuen Lösung profitieren. Dank unserer umfangreichen Bibliothek mit vordefinierten Richtlinien zur Regelung einer sicheren Datennutzung in Ihrem Netzwerk, an Endpunkten und in der Cloud richten Sie Ihre neue Lösung innerhalb kürzester Zeit und mit umfangreichen Anpassungsmöglichkeiten für eine stetige Optimierung ein.

Was wir bieten

- die branchenweit umfangreichste Bibliothek mit vordefinierten, anpassbaren Richtlinien für eine schnellere Implementierung in der Cloud, an Endpunkten und in Ihrem Netzwerk
- individuelles Account Management, das ganz auf Ihren Zeitplan und Ihre Bedürfnisse ausgerichtet ist
- direkten Kontakt zu Experten der Branche mit kontinuierlicher Beratung zu den Best Practices im Bereich Datenschutz

Ihre Vorteile

- Mit einem proaktiven Sicherheitsprofil gehen Ihre Möglichkeiten, Datenverluste im Unternehmen zu verhindern, über die reine Risikoanalyse hinaus.
- Durch den uneingeschränkten und kanalübergreifenden Zugriff auf Daten bei geringer Risikostufe des Benutzers wird die Produktivität Ihrer Mitarbeiter maßgeblich gesteigert.
- Durch unsere durchdachte Implementierungspartnerschaft mit Experten der Branche können Sie schnellstmöglich von der Investition profitieren.

Sie möchten wissen, wie Forcepoint eine risikogerechte, am Menschen orientierte Datenschutzlösung für Ihr Unternehmen umsetzen würde?

Wenden Sie sich an einen unserer Experten und besprechen Sie Ihre individuellen Bedürfnisse.

Forcepoint

forcepoint.com/contact

Über Forcepoint

Forcepoint ist einer der weltweit führenden Anbieter von Cyber-Sicherheit im Bereich Anwender- und Datenschutz und hat es sich zur Aufgabe gemacht, Organisationen zu schützen und gleichzeitig die digitale Transformation und das Wachstum voranzutreiben. Die verhaltensbasierten Lösungen von Forcepoint passen sich in Echtzeit an das Nutzerverhalten an und ermöglichen Mitarbeitern einen sicheren Datenzugriff bei voller Produktivität. Forcepoint mit Sitz in Austin, Texas, schafft sichere, vertrauenswürdige Umgebungen für Tausende von Kunden weltweit.