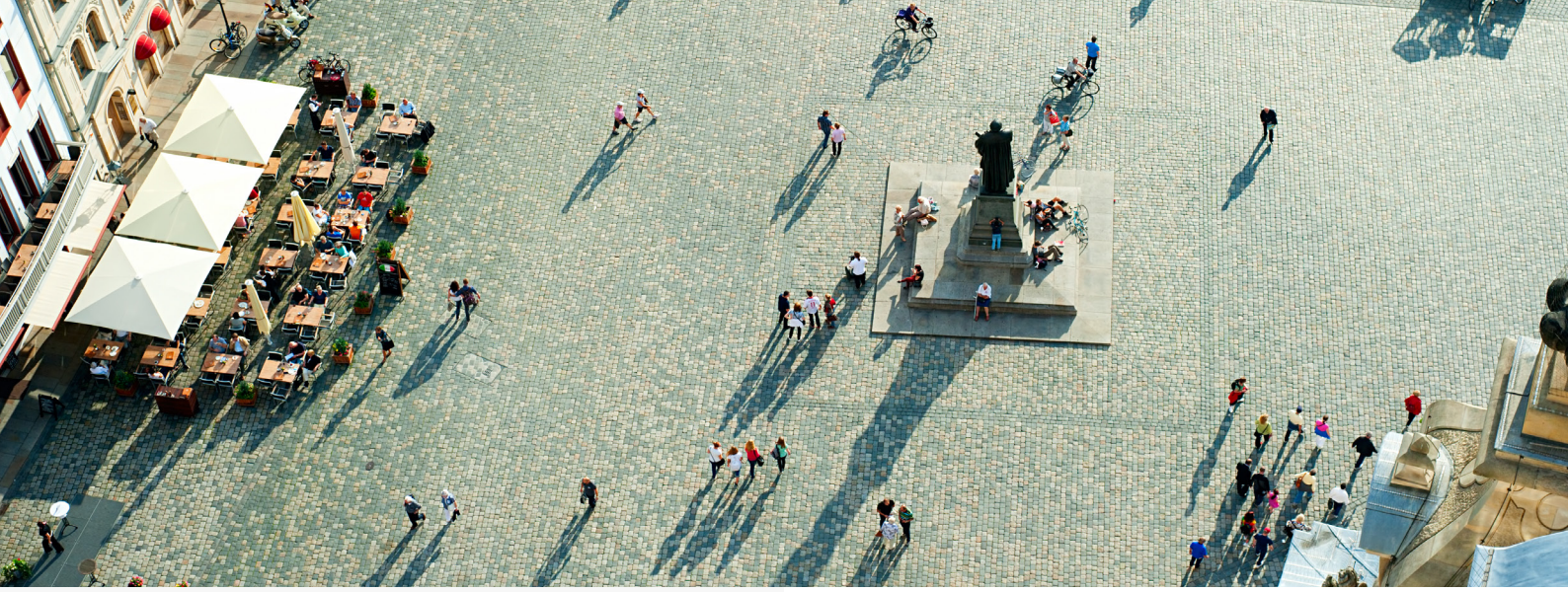
Käuferleitfaden

Welche Sicherheitsplattform eignet sich für Sie am besten?

Stellen Sie die richtigen Fragen. Erhalten Sie die richtigen Antworten.

IBM Security

IBM



Auswahl der richtigen Sicherheitsplattform

Die Suche nach der richtigen Sicherheitsplattform für Ihre Organisation kann eine schwierige Aufgabe sein. Beim Thema Cybersicherheit ist der Begriff „Plattform“ mittlerweile überstrapaziert, was es schwierig macht, die Spreu vom Weizen zu trennen und zu verstehen, welche Faktoren bei der Auswahl der besten Option für Ihr Unternehmen wirklich wichtig sind. Die Plattform, für die Sie sich heute entscheiden, kann in den nächsten Jahren das Fundament für die Lage Ihrer Sicherheitsreife sein und sollte daher sorgfältig ausgewählt werden.

Unternehmenssicherheitsteams stehen vor der Herausforderung, dass zu viele Daten, zu viele Tools und zu wenige Ressourcen vorhanden sind. Daher wird es Zeit, Sicherheitsdaten, Tools und Teams auf andere Weise zu vereinheitlichen. Alles muss unbedingt zentral verbunden werden – und eine integrierte Sicherheitsplattform bietet dafür ideale Voraussetzungen.

Worauf Sie bei einer Sicherheitsplattform achten sollten

Bei der Suche nach einer ganzheitlichen, integrierten Cybersicherheitsplattform, die jetzt und in Zukunft effektiv sein kann, sollten Sie Folgendes berücksichtigen:

- Überlegungen rund um das Verschieben Ihrer Daten
- Optionen für die Bereitstellung
- Erforderliche Verbindungen zu anderen Tools
- Offenheit und Anpassungs-fähigkeit der Plattform
- Unterstützte Funktionalität und Services

Die folgenden Schlüsselfragen helfen Ihnen, Ihre Optionen bei der Auswahl einer Sicherheitsplattform besser zu verstehen und herauszufinden, welche Plattform für Ihre Organisation am besten geeignet ist.

1 Müssen Sie Ihre Daten verschieben, um eine Wertschöpfung zu ermöglichen?

Bei vielen Sicherheitsplattformen müssen Sie alle Ihre Daten auf diese Plattform verschieben, um darauf zugreifen zu können. Zwar scheint es ein sinnvoller Lösungsansatz zu sein, alle ihre Daten an einem Ort zu verwalten – doch oft ist dies auch eine komplexe und kostenintensive Aufgabe. Zudem müssen Sie sich möglicherweise um wichtige Fragen in Sachen Datenschutz und Datenspeicherort kümmern.

Aus Kosten- und Komplexitätsgründen kann es für eine Plattform von Vorteil sein, eine Verbindung mit Ihren Daten dort herzustellen, wo sie sich bereits befinden, sodass sie nicht verschoben werden müssen. Dieser Ansatz kann Ihre vorhandenen Tools ergänzen und Ihnen helfen, bereits getätigte Investitionen zu maximieren, während weiterhin eine zentralisierte Ansicht und ein zentraler Zugriff auf Daten der unterschiedlichsten Tools ermöglicht wird.

2 Können Sie die Plattform lokal, in einer öffentlichen Cloud oder einer privaten Cloud bereitstellen?

Viele Sicherheitsplattformen stehen nur als cloudbasierte SaaS-Lösungen (Software as a Service) zur Verfügung. Während dies für Sie der richtige Ansatz sein mag, sind viele Organisation noch nicht für eine ausschließliche Cloudlösung bereit und benötigen vielleicht die Flexibilität einer hybriden Multicloud-Architektur. Da die Verarbeitungsprozesse vieler Organisationen noch immer lokal stattfinden, kann eine Sicherheitsplattform, die die Flexibilität einer Ausführung vor Ort, in einer öffentlichen Cloud oder in einer privaten Cloud ermöglicht, von Vorteil sein. Begrenzen Sie sich also nicht auf eine Bereitstellungsoption, sondern suchen Sie nach einer flexiblen Architektur, die in hybriden Multicloud-Umgebungen bereitgestellt werden kann.

3 Unterstützt die Plattform Verbindungen mit und die Integration in Tools von anderen Anbietern?

Da Organisationen heute die unterschiedlichsten Sicherheitstools verwenden, ist es unwahrscheinlich, dass diese alle von einem Anbieter stammen. Einige Sicherheitsplattformen sind so konzipiert, dass sie nur die Tools eines bestimmten Anbieters integrieren können, wodurch Sie möglicherweise eingeschränkt sind. Wenn Sie Sicherheitstools von vielen verschiedenen Anbietern verwenden, suchen Sie nach einer Plattform, die offene Verbindungen zu verschiedenen Sicherheits- und IT-Tools unterstützt. Suchen Sie nach einer Option, die Folgendes umfasst:

- Ein großes Ökosystem an Partnern
- Ein offenes Software-Development-Kit (SDK)
- Support Services zum Hinzufügen Ihrer eigenen benutzerdefinierten Verbindungen

Mit diesem Ansatz können Sie leichter feststellen, ob die Plattform für Ihre Tools geeignet ist, damit Sie vorhandene Tools nicht mit hohem Aufwand vollständig ersetzen müssen.

4 Passt sich die Plattform an, wenn sich Ihr Sicherheitsprogramm ändert?

Achten Sie bei der Auswahl Ihrer Plattform darauf, dass sie offen und flexibel genug ist, um Ihr Sicherheitsprogramm zu unterstützen, wenn sich dieses ändert. Prüfen Sie, ob sie Folgendes bietet:

- Offene Standards
- Open-Source-Technologie
- Offene Verbindungen

Eine offene Plattform stellt eine Verbindung zu den Tools anderer Anbieter her und unterstützt benutzerdefinierte Verbindungen und Entwicklungen. Mit diesem Ansatz können Sie die Abhängigkeit von einem Anbieter verringern und die Interoperabilität mit mehreren Sicherheits- und IT-Tools fördern.

5 Bietet sie zentrale Orchestrierungs-, Automatisierungs- und Reaktionsfunktionen?

SOAR-Lösungen (Security Orchestration, Automation and Response) sind oft selbst als Plattform positioniert. Doch SOAR-Funktionen können leistungsstärker sein, wenn sie in Ihre Hauptsicherheitsplattform integriert sind und nicht separat angeboten werden. Suchen Sie nach einer Sicherheitsplattform, die SOAR als Kernfunktion umfasst, um die Effizienz Ihres Sicherheitsteams bei den unterschiedlichsten Workflows und Sicherheitsanwendungsfällen zu fördern.

6 Wie unterstützt sie die Integration von Bedrohungsdaten?

Sicherheitsanalysten verwenden häufig eine Vielzahl von Feeds für Sicherheitsbedrohungen sowie verschiedene Produkte, um die Bedrohungsdaten zu durchsuchen und ihre Rechercheabteilung sowie Entscheidungsträger zu informieren. Prüfen Sie, ob die Plattform Berichte zu Bedrohungsdaten bereitstellt und wie die Daten in andere Leistungsmerkmale integriert sind. Die Integration von Bedrohungsdaten in Ihre Sicherheitsplattform kann einen Sicherheitsanalysten entlasten und ermöglicht promptere sowie fundiertere Entscheidungen.

7 Erhalten Sie von Ihrem Anbieter neben der Software auch Services?

Eine Sicherheitsplattform ist zwar ein leistungsstarkes Tool, doch möglicherweise benötigen Sie zusätzliche Services, die auf Ihre Organisation oder Ihr Sicherheitsprogramm zugeschnitten sind. Es gibt die unterschiedlichsten Sicherheitsservices, doch wenn Sie diese von einem Anbieter erhalten, der gleichzeitig zusätzliche Sicherheitsservices anbietet, können Sie diese Services einfacher ergänzen und in Ihre Sicherheitsplattform integrieren.

Verstehen, was Ihre Kernsicherheits-plattform benötigt und erfordert

Plattformansätze sind eine Möglichkeit, Sicherheitsdaten, -tools und -teams zu optimieren. Da jedoch viele verschiedene Optionen angeboten werden, müssen Sie die Antworten auf diese Schlüsselfragen kennen, wenn Sie nach der richtigen Sicherheitsplattform für Ihre Organisation suchen:

- Können Ihre Daten weiterhin am aktuellen Speicherort bleiben?
- Kann Ihre Bereitstellung hybride Multicloud-Architekturen unterstützen?
- Benötigen Sie offene Integrationen und Verbindungen zu anderen Sicherheits- oder IT-Tools?
- Ist eine einfache Anpassung möglich, wenn sich Ihr Sicherheitsprogramm ändert?
- Würden Sie von SOAR-Funktionen (Security Orchestration, Automation and Response) profitieren?
- Wie werden Bedrohungsdaten integriert?
- Erhalten Sie von Ihrem Anbieter neben der Software auch Services?

IBM Cloud Pak for Security: Vernetzte Sicherheit für eine hybride Multicloud-Welt

IBM Cloud Pak for Security ist eine offene, integrierte Sicherheits-plattform, die aussagekräftige Informationen zu Bedrohungen in mehreren Umgebungen bereitstellt – heute und in Zukunft. Sie können nach Bedrohungen suchen, Aktionen orchestrieren und Reaktionen automatisieren, ohne Ihre Daten migrieren zu müssen.

Durch offene Standards und IBM Innovationen ermöglicht Ihnen IBM Cloud Pak for Security den Zugriff auf Tools von IBM und anderen Herstellern, damit Sie nach Anzeichen von Bedrohungen an Cloud- oder lokalen Standorten suchen können. IBM hat die in IBM Cloud Pak for Security verwendete Open-Source-Technologie beigetragen und über die OASIS Open Cybersecurity Alliance Partnerschaften mit zahlreichen Unternehmen aufgebaut, um mehr Interoperabilität zu schaffen und die Abhängigkeit von einem Anbieter zu reduzieren.

IBM Cloud Pak for Security besteht aus containerisierter Software, die in die Unternehmensanwendungsplattform Red Hat OpenShift vorintegriert ist. Durch diese Integration kann die Plattform lokal und in privaten oder öffentlichen Clouds ausgeführt werden. Dank der integrierten SOAR-Leistungsmerkmale ermöglicht Ihnen IBM Cloud Pak for Security die Orchestrierung und Automatisierung Ihrer Sicherheitsreaktionen.

Weitere Informationen zu IBM Cloud Pak for Security

Auf der Webseite von IBM Cloud Pak for Security erfahren Sie mehr darüber, wie Sie versteckte Bedrohungen aufdecken und fundierte, risikobasierte Entscheidungen treffen können, um Prioritäten für die Zeit Ihres Teams festzulegen.

Und wenn Sie zusätzliche Kompetenz und Kenntnisse zur Unterstützung Ihres Teams benötigen, nutzen Sie die IBM Security-Services, um eine solide Strategie aufzubauen und Ihr Sicherheitsprogramm zu transformieren.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com