Check Point + Accellion

kiteworks - sichere File-Sharing-Plattform

Accellion kiteworks und Check Point SandBlast Threat Prevention bieten Unternehmen Sicherheit und Kontinuität bei der Datenübertragung, um das Risiko einer Infiltration durch Malware zu verhindern.

Produktvorteile

- Flexibilität bei der Integration von Sicherheit in eine Vielzahl von Geschäftsprozessen, bei denen es um den Datentransfer geht.
- Erlaubt Unternehmen das sichere Senden und Empfangen von Informationen in Übereinstimmung mit internen Richtlinien und gesetzlichen Bestimmungen.
- Bietet einheitlichen Zugriff auf alle Informationen im Unternehmen, sowohl vor Ort als auch in der Cloud.
- Verbessert die Nutzung gesicherter Datenquellen im Umgang mit nicht vertrauenswürdigen Quellen.
- Vereinfachter Schutz vor Bedrohungen über verschlüsselte Protokolle wie HTTPS und SFTP.

Produkteigenschaften

- Granulare Kontrollen, die mit den bestehenden Richtlinien für Threat-Reporting und Quarantäne abgestimmt sind.
- Detaillierte Informationen zu Gefahrenquellen und Regelverstößen.
- Zentralisiertes Auditing bei Regelverstößen.
- SSL/TLS sichere Kommunikation.
- Mehrstufige On-Premise- und hybride Cloud-Bereitstellungsoptionen.

HERAUSFORDERUNG

Da Technologiefortschritte mehr und mehr Daten generieren und Unternehmen zunehmend auf externe Partner angewiesen sind, um die betriebliche Effizienz zu steigern, wird der Datentransfer in Unternehmen immer wichtiger für den geschäftlichen Erfolg. Da jedoch mehr Daten über Unternehmensgrenzen hinweg ausgetauscht werden, steigt das Risiko eines Datenschutzverstoßes oder einer anderen Form des unbefugten Zugriffs auf sensible Informationen. Das Eindringen von Ransomware oder anderer Malware kann zu Datenverlust, Bußgeldern, Markenerosion, Rechtsstreitigkeiten und anderen weitreichenden, langfristigen Folgen führen. Daher ist die Fähigkeit, Daten außerhalb des Unternehmens sicher zu übertragen und gleichzeitig zu gewährleisten, dass alle Daten, die in das Unternehmen gelangen, frei von Malware sind, von entscheidender Bedeutung für die Geschäftstätigkeit.

GEMEINSAME LÖSUNG

Accellion kiteworks und Check Point SandBlast arbeiten zusammen, um die Verbreitung von Malware zu verhindern. Durch die Integration mit Check Point SandBlast bietet kiteworks Unternehmen ein integriertes Governance-Framework für alle Daten, die in das Unternehmen gelangen und es verlassen, um das Risiko des Eindringens von Malware in das Unternehmensnetzwerk zu verhindern. Die granulare Transparenz und Kontrolle der Informationen, die über die kiteworks-Plattform laufen, ermöglicht es Unternehmen, Bedrohungen durch schädliche Daten zu analysieren und entweder zu blockieren oder einfach zu melden.

Das Leitmotiv von Accellion besteht darin, die Informationen eines Unternehmens sicher mit den Personen und Systemen zu verbinden, die Teil der kritischen Geschäftsprozesse sind. Die sichere File-Sharing-Governance-Plattform kiteworks gewährleistet, dass diese Informationen sicher ausgetauscht werden. Sie bietet einen detaillierten und zentralisierten Audit Trail, der die Einhaltung interner Richtlinien und gesetzlicher Vorschriften nachweist.

Check Point SandBlast bietet fortschrittlichen Schutz vor Zero-Day-Angriffen und implementiert eine Reihe einzigartiger Technologien, die den Einsatz modernster Umgehungsmethoden erkennen und verhindern. Dazu gehören unter anderem die Prüfung auf CPU-Ebene sowie eine Threat Extraction Engine.

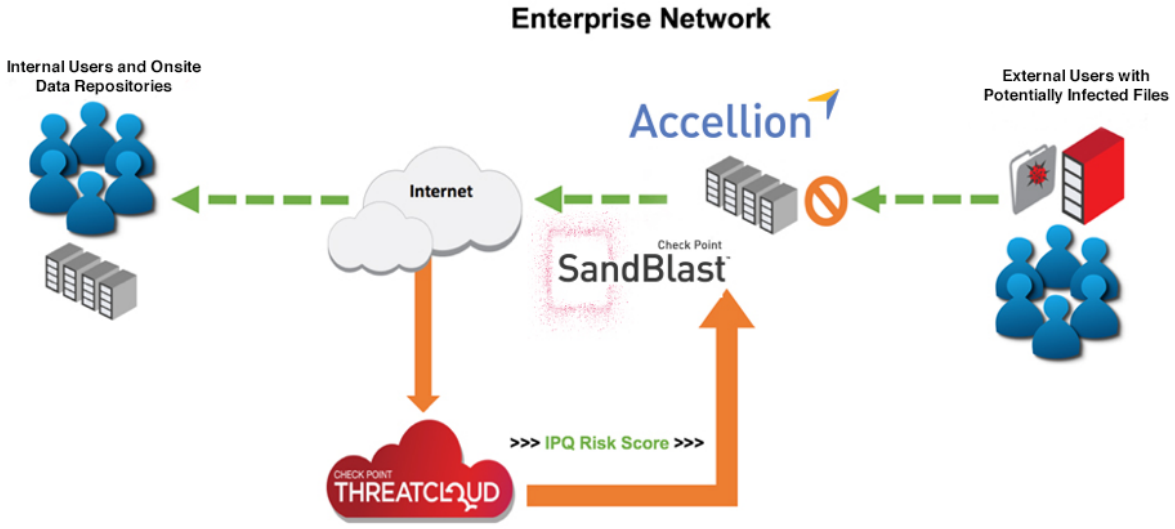
Mit Accellion und Check Point werden alle Informationen auf Malware analysiert, bevor sie in den Geschäftsbetrieb gelangen. Die gemeinsame Lösung hindert Hacker daran, sich der Erkennung zu entziehen und in das Netzwerk eines Unternehmens einzudringen, wodurch das Risiko teurer Datenschutzverstöße, Datenverlust oder Ausfallzeiten reduziert wird.

Über eine einfache webbasierte Administrationsoberfläche kann kiteworks mit minimalem Aufwand konfiguriert werden, um alle Dateien in das SandBlast-System zu senden und einen vollständigen Sicherheits-Scan durchzuführen. Alle Regelverstöße werden sowohl in Check Point als auch in den Protokollierungs- und Reporting-Lösungen von kiteworks angezeigt und können in die bestehende SIEM-Infrastruktur eines Unternehmens integriert werden.

Zusammengefasst bietet kiteworks einen sicheren Kanal für den Datentransfer über Unternehmensgrenzen hinweg und nutzt eine Vielzahl gängiger Protokolle wie SFTP, HTTPS und vereinfachte Automatisierung. Durch die Integration von SandBlast Threat Emulation haben Unternehmen jetzt die Möglichkeit und die Sicherheit, Informationen sicher auszutauschen und das Risiko einer Malware-Infektion oder eines Datenverlusts zu minimieren.

BESSERER SCHUTZ DER GESCHÄFTSPROZESSE

Durch die Nutzung der vorhandenen Infrastruktur und Richtlinien eines Unternehmens stellen kiteworks und Check Point SandBlast sicher, dass jede eingehende Datei frei von schädlicher Software ist, unabhängig von deren Quelle oder Ziel. Neu entdeckte Bedrohungen werden an die ThreatCloud Intelligence-Datenbank gesendet und jede neu entdeckte Bedrohungssignatur wird über das ThreatCloud-Ökosystem verteilt, um die kiteworks-Umgebung zu schützen. Die Flexibilität der kiteworks-Plattform bietet Unternehmen eine sichere, gesetzeskonforme und effiziente Möglichkeit, Informationen über eine Vielzahl von Protokollen, Plugins und Diensten zu senden und zu empfangen. Dies geschieht jedoch erst, nachdem jede eingehende oder ausgehende Datei über den SandBlast Thread-Emulationsdienst gesendet wurde, um jegliche Bedrohung durch bösartigen Code zu erkennen. Nach dem Scannen wird ein Protokoll erstellt und der Empfänger kann auf die Datei zugreifen.



GANZHEITLICHE SICHERHEITSLÖSUNGEN

Die meisten File-Sharing-Lösungen sind auf eine bestimmte Methode der Datenübertragung von einem Ort zum anderen beschränkt. Einige Lösungen schränken beispielsweise alle Dateiübertragungen ein, die über den Webbrowser ausgeführt werden sollen. Mit kiteworks wird nicht nur das Web effektiv für den Datentransfer genutzt, sondern auch ein natives SFTP (Secure File Transfer Protocol), eine Reihe nativer und eingebetteter Produktivitätstreiber, eine sichere mobile Applikation sowie anpassbare Automatisierungsagenten sind verfügar, um den Endbenutzern maximale Funktionalität zu bieten. Unabhängig davon, welches Protokoll für den Zugriff auf Dateien verwendet wird, wendet das kiteworks Security Framework native und integrierte Sicherheits- und Governance-Schichten nahtlos an, basierend auf den von der Organisation festgelegten Richtlinien und Konfigurationen. Alle Dateien werden gescannt, protokolliert, genehmigt oder unter Quarantäne gestellt, indem die Leistungsfähigkeit des Check Point SandBlast-Systems zum Schutz des Unternehmens genutzt wird. Aufgrund der einfachen Integration verfügen Administratoren nicht nur über eine einfache Methode zur Berichterstellung und Beseitigung von Bedrohungen, sondern sie können Endbenutzern auch eine effektive und flexible Methode zur Zusammenarbeit und Anforderung von Informationen aus Quellen außerhalb des Unternehmens bieten.

KONTAKT CHECK POINT

Unternehmenssitz weltweit | 5 Ha'Solelim Street, Tel Aviv 67897, Israel |Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | E-Mail: info@checkpoint.com
Unternehmenssitz USA | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: +1 800-429-4391; 650-628-2000 | Fax: +1 650-654-4233 | www.checkpoint.com

KONTAKT ACCELLION

Unternehmenssitz USA | Accellion, Inc. 1804 Embarcadero Road Palo Alto, CA 94303 | Tel.: +1 650 485 4300 | E-Mail: sales@accellion.com
EMEA | Accellion GmbH, Löwen-Markt 5, 70499 Stuttgart, Deutschland | Tel.: +49 711 252861-0 | E-Mail: emea-sales@accellion.com | www.accellion.com