Forcepoint

Die Lösung im Überblick

Forcepoint Zero Trust Content Disarm and Reconstruction für Web-Gateways

Sorgenfreies Surfen im Internet

Herausforderungen

- Unternehmen sind Zero-Day-Bedrohungen ausgesetzt, die in das Unternehmen eindringen, bevor erkennungsbasierte Abwehrmechanismen greifen. Auch völlig unbekannte Bedrohungen können in Unternehmen eindringen, ohne jemals richtig identifiziert zu werden.
- Downloads aus dem Internet können Bedrohungen enthalten, die zu Anwendungsfehlern führen und Angreifern die Kontrolle über Unternehmenssysteme geben.
- Uploads ins Internet können mehr Informationen enthalten, als ein Unternehmen eigentlich preisgeben möchte. Wenn dadurch geistiges Eigentum nach außen dringt, könnte das dem Unternehmen schaden.

Lösung

- Die einzigartige Zero-Trust-CDR-Technologie von Forcepoint geht davon aus, dass alle Daten nicht sicher und nicht vertrauenswürdig sind und versucht gar nicht erst, gut von böse zu unterscheiden. Dadurch ist dies eine echte Zero-Trust-Lösung.
- Zero Trust CDR lässt sich innerhalb weniger Minuten in Ihre bestehende Internetschutzlösung integrieren.

Vorteile

- Stellt immer sichere, bedrohungsfreie Inhalte an allen Internetschnittstellen bereit
- Abwehr unbekannter Bedrohungen
- Revolutionierung Ihrer Internetsicherheit
- Besseres Surferlebnis im Internet
- Nahtlose Integration
- Abwehr von Malware
- Bekämpfung von Steganografie
- Unvergleichlicher Schutz

Unternehmen nutzen das Internet zum Teilen von Informationen, als Informationsquelle für wichtige Unternehmensprozesse und zur Durchführung von Transaktionen. Bestehende Internetschutzmechanismen am Netzwerkrand (Web-Gateways und Firewalls) sind nicht in der Lage, die zahlreichen bekannten, unbekannten und Zero-Day-Bedrohungen zu bewältigen, die sich in geschäftlichen Dokumenten und Bildern verstecken. Wenn dieser Angriffsvektor nicht überwacht wird, ist dies eine existenzielle Gefahr für Unternehmen. Die Dokumente und Bilder, die Mitarbeiter aus dem Internet herunterladen, können Bedrohungen enthalten, die zu Anwendungsfehlern führen und Angreifern die Kontrolle über Unternehmenssysteme geben können. Die Dokumente und Bilder, die Mitarbeiter ins Internet hochladen, können mehr Informationen enthalten, als ein Unternehmen eigentlich preisgeben möchte. Wenn dadurch geistiges Eigentum nach außen dringt, könnte das dem Unternehmen schaden. Bisher ist es niemandem gelungen, die Flut von Bedrohungen einzudämmen.

Abwehr unbekannter Bedrohungen

Bestehende Internetschutzmechanismen am Netzwerkrand, Gateways und Firewalls sind die erste Verteidigungslinie und sollen bekannte Bedrohungen erkennen, indem nach Signaturen von bisher aufgetretenen Exploits und nach unsicheren Verhaltensweisen gesucht wird. Unternehmen sind jedoch immer wieder Zero-Day-Bedrohungen ausgesetzt, die in das Unternehmen eindringen, bevor erkennungsbasierte Abwehrmechanismen greifen. Auch völlig unbekannte Bedrohungen können in Unternehmen eindringen, ohne jemals richtig identifiziert zu werden.

Zero Trust Content Disarm and Reconstruction (CDR) für Web-Gateways ist die einzige Lösung, die nicht nur vor bekannten Bedrohungen, sondern auch vor Zero-Day- und unbekannte Bedrohungen in Inhalten schützt, die über Internetschnittstellen eindringen, da diese Technologie nicht auf Erkennung oder der Ausführung in einer Sandbox-Umgebung beruht. Daten werden stattdessen in einem einzigartigen Verfahren so umgewandelt, dass ein umfassender Schutz gewährleistet ist.

Revolutionierung Ihrer Internetsicherheit

Zero Trust CDR für Web-Gateways extrahiert beim Surfen im Internet die geschäftlichen Informationen aus den Dokumenten und Bildern. Die Daten, die Informationen enthalten, werden zusammen mit potenziellen Bedrohungen verworfen. Anschließend werden neue Dokumente und Bilder erstellt und dem Benutzer bereitgestellt. Somit werden nur sichere Inhalte an den Benutzer weitergeleitet. Angreifer bleiben draußen und Unternehmen bekommen die Informationen, die sie brauchen.

Dieser Prozess wird Transformation genannt. Dieses Verfahren ist unschlagbar: Das Sicherheitsteam ist zufrieden, weil die Bedrohung entfernt wird, und die Benutzer im Unternehmen sind zufrieden, weil sie die benötigten Informationen bekommen.

Zero Trust CDR ist die einzige Möglichkeit, Bedrohungen in Inhalten zuverlässig zu entfernen. Die einzigartige Forcepoint-Technologie Zero Trust CDR verzichtet auf die unzuverlässigen Verfahren der Bedrohungserkennung und -isolierung. Die Technologie geht davon aus, dass alle Daten nicht sicher und nicht vertrauenswürdig sind und versucht gar nicht erst, gut von böse zu unterscheiden.

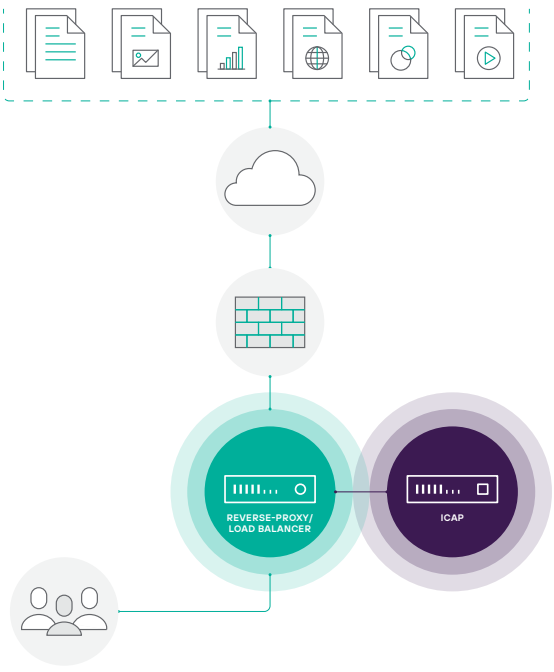
Besseres Surferlebnis im Internet

Sicherheitsteams müssen sich kontinuierlich mit Cyber-Angreifern auseinandersetzen, die ihnen, wie es scheint, immer einen Schritt voraus sind. Doch es sind die Geschäftsanwender, die darunter zu leiden haben. Die zeitraubende Behandlung von Fehlalarmen oder das Warten auf die Prüfung und Freigabe von Dokumenten behindert Unternehmensprozesse und beeinträchtigt die Produktivität. Und wenn ein Angriff Erfolg hat, ist die Problembehebung kostspielig und zeitaufwändig.

Zero Trust CDR für Web-Gateways verbessert das Benutzererlebnis im Internet und den sozialen Medien. Benutzer erhalten schnell Zugriff auf die benötigten geschäftlichen Informationen und können sie lesen, teilen und Transaktionen durchführen und sich darauf verlassen, dass die von ihnen genutzten Inhalte keinerlei Gefahren enthalten.

Sicherstellen von digital sauberen Inhalten

Das Internet und die sozialen Medien sind wichtige Tools in jedem Geschäftsbereich. Daher ist es heute wichtiger denn je, dafür zu sorgen, dass die Inhalte sicher, unverfälscht und bedrohungsfrei sind. Jedes Unternehmen, das seinen Benutzern, Geschäftspartnern und Kunden Zugriff auf saubere, unverfälschte Geschäftsinhalte garantieren kann, wird sich in einer Internetlandschaft durchsetzen können, die zunehmend durch Gesetzlosigkeit geprägt ist.



Genau das macht Zero Trust CDR für Web-Gateways – es stellt sicher, dass Unternehmen von den Vorteile profitieren können, die die Nutzung des Internets und der sozialen Medien bietet, und zwar in dem Wissen, dass die angebotenen Inhalte bedrohungsfrei sind.

Nahtlose Integration in bestehende Abwehrmechanismen

Zero Trust CDR für Web-Gateways lässt sich mit dem branchenüblichen Protokoll ICAP nahtlos in bestehende Internetschutzmechanismen am Netzwerkrand, Web-Gateways und Anwendungs-Firewalls integrieren. Die Lösung wird gewissermaßen als Zweitlösung bereitgestellt und so konfiguriert, dass der Web-Gateway oder die Firewall Dokumente und Bilder über ICAP an einen Forcepoint Gateway eXtension (GX)-Server leitet, wo sie umgewandelt werden, um potenzielle verborgene Bedrohungen zu entfernen. Anschließend werden sie wieder an den Gateway zurückgegeben und dem Benutzer bereitgestellt.

Die Integration in den bestehenden Internetschutz am Netzwerkrand dauert nur wenige Minuten. Es gibt für viele beliebte Web-Gateways und Firewalls vorgefertigte Integrationsdateien, um den Prozess noch einfacher zu machen.

Verhindern von Infiltration von Malware in Inhalten

Office-Dokumente, Dokumente im Adobe Portable Document-Format (PDFs) und Bilder sind die häufigsten Träger von Malware. Durch die Komplexität dieser Dateiformate und die Anwendungen, mit denen sie bearbeitet werden, sind sie ein beliebtes Ziel für Angreifer. Unabhängig von der Malware – ob Ransomware, Banktrojaner oder Remote-Zugriffskits und Keylogger – Cyber-Kriminelle wissen, wo sie die neuesten Zero-Day-Bedrohungen in einem ganz gewöhnlichen Geschäftsdokument am besten verstecken können. Durch Techniken wie die Verwendung von dateiloser Malware und Polymorphismus von Dateien ist es noch schwieriger, mit herkömmlicher erkennungsbasierter Internetsicherheit Bedrohungen zu beseitigen. Zudem ist das Internet der perfekte Vektor zum Einschleusen von Malware.

Zero Trust CDR für Web-Gateways stellt sicher, dass Unternehmensbenutzer Geschäftsdokumente und Bilder sorgenfrei ins Internet hoch- und aus dem Internet herunterladen können. Der Schlüssel liegt im einzigartigen Verfahren zur Transformation von Daten. Jedes Dokument und Bild wird umgewandelt und ist dadurch bedrohungsfrei.

Schutz vor Datenverlust durch Bild-Steganografie

Steganografie bezeichnet das Verbergen von Daten in scheinbar harmlosen Dateien. Dabei wird eine geheime Nachricht in einer anderen Nachricht, dem sogenannten Träger, verschlüsselt, sodass nur der gewünschte Empfänger die Nachricht lesen kann. Derzeit ist Stegware, mit der Cyber-Angreifer Steganografie als Waffe einsetzen können, auf dem Vormarsch. Im Darkweb wird sie standardmäßig als Malware-as-a-Service-Kits angeboten. Sie wurde in sogenannten Malvertising-Kampagnen eingesetzt, um von tausenden von Benutzern Geld zu erpressen und namhafte Nachrichtenseiten in die Knie zu zwingen. Sie wurde in Verbindung mit Social-Media-Websites eingesetzt, um mittels scheinbar harmloser Bilder Vermögenswerte zu stehlen. Das sind keine guten Nachrichten für IT-Experten, die Tools zur Identifizierung unsicherer Daten verwenden, denn Steganografie lässt sich nicht erkennen.

Zero Trust CDR für Web-Gateways stellt sicher, dass jedes Bild, das von einem Benutzer beim Surfen im Internet angesehen wird, und jegliche Kommunikation über Social Media keine Inhalte enthält, die mit Stegware versteckt wurden. Der Transformationsprozess zerstört versteckte Inhalte, sodass das Bild für den Angreifer nutzlos wird. Zero Trust CDR für Web-Gateways ergänzt bestehende Data-Loss-Prevention- und Governance-Initiativen, wie die Datenschutz-Grundverordnung (DSGVO), da verborgener Datenverlust durch Bild-Steganografie komplett unterbunden wird.

Unterbinden von Command-and-Control-(CnC)-Kanälen

Bei besonders ausgeklügelten und gefährlichen Cyber-Angriffen wird normalerweise versucht, einen Command-and-Control-(CnC)-Kanal zwischen dem Remote-Angreifer und einer oder mehreren Workstations im Unternehmensnetzwerk einzurichten. Dies gelingt meist dann, wenn eine zuvor unterwanderte Workstation einen Remote-Server kontaktiert, beispielsweise über ein Bild auf einer Social-Media-Website, oder wenn eine zuvor unbekannte Malware als legitimes Geschäftsdokument eingeschleust wird.

Zero Trust CDR für Web-Gateways stellt sicher, dass Versuche zur Einrichtung eines CnC-Kanals unterbunden werden. Der Transformationsprozess beseitigt sämtliche Bedrohungen, die sich in Dokumenten oder Bildern aus dem Internet und sozialen Netzwerken verstecken könnten. Mit einem forensischen Dashboard ist es möglich, die Vorher- und Nachher-Kopien der Dokumente und Bilder anzuzeigen, um die Erkennung von verdächtigem Verhalten zu ermöglichen und Benutzer zur Verantwortung zu ziehen.

Entwickeln einer erfolgreichen Lösung

Zusammen mit seinen Vertriebspartnern bietet das Forcepoint-Lösungsteam eine breite Palette an professionellen Dienstleistungen an, die Ihnen helfen, Ihre Investition in Zero Trust CDR-Technologie zu maximieren. Wir können Sie bei der Bedarfsermittlung, Planung, Installation, Konfiguration und Verwaltung Ihrer Zero Trust CDR für Web-Gateways-Lösung unterstützen.

Stellen Sie mithilfe des technischen Supports von Forcepoint sicher, dass während und nach der Bereitstellung alles reibungslos funktioniert. Unser hochqualifiziertes Lösungsteam verfügt über fundiertes Fachwissen und Informationen und ist ein zuverlässiger Partner, der Ihr internes Team ergänzen kann.

Zusammenfassung: Unvergleichlichen Schutz genießen

Wir stehen kurz vor einer technologischen Revolution. Aufgrund zahlreicher, gut organisierter Cyber-Angriffe sind Unternehmen gezwungen, jeden Aspekt ihrer digitalen Prozesse für Anschaffung, das Teilen von Informationen und für Transaktionen neu zu bewerten.

Weitere Informationen finden Sie unter Forcepoint Zero Trust CDR

forcepoint.com/contact