Forcepoint Zero Trust Content Disarm and Reconstruction

Abwehr von bekannten und unbekannten Bedrohungen, Zero-Day-Angriffen und Malware

Forcepoint

Broschüre

Forcepoint Zero Trust Content Disarm and Reconstruction

Abwehr von bekannten und unbekannten Bedrohungen, Zero-Day-Angriffen und Malware

Technologie erzeugt die digitalen Informationen, die die wichtigste Voraussetzung für jedes Unternehmen sind, ob E-Mail-Verkehr, Internet, Social-Media-Interaktionen oder Datei-Uploads und Web-Anwendungen. Diese digitalen Informationen werden mit Geschäftspartnern, Kunden, Lieferketten sowie lokalen und Remote-Mitarbeitern geteilt und kommuniziert. Ein Informationsaustausch in dieser Größenordnung liefert Cyber-Kriminellen eine riesige Angriffsfläche, um Malware in alltäglichen Dateien, Dokumenten und Bildern einzuschleusen.

Um diesem Problem Herr zu werden, wurden immer mehr Abwehrtechnologien entwickelt. All diese Abwehrmechanismen beruhen jedoch in gewissen Maße auf dem Konzept der Erkennung. Das Problem von Abwehrmechanismen, die einzig und allein auf der Erkennung beruhen, ist, dass sie nur ihnen bekannte Bedrohungen erkennen. Es wurde schon versucht, diese Schutzmechanismen zu verstärken. Sandboxes können helfen. Angreifer haben jedoch gelernt, sie zu erkennen, und zudem beruht auch diese Abwehr auf der Erkennung und Identifizierung von Bedrohungen. Künstliche Intelligenz und maschinelle Lernalgorithmen sind zwar nützlich, bedienen sich jedoch auch nur der vorhandenen Rechenleistung, um eine bereits bekannte Bedrohung schneller zu erkennen. Cyber-Kriminelle wiederum suchen ständig nach Möglichkeiten, Unternehmen mithilfe von Malware anzugreifen, die die Abwehrmechanismen noch nicht kennen und daher als sicher einstufen.

Auf Erkennung beruhende Abwehrmechanismen allein haben keine Chance.

Forcepoint Zero Trust Content Disarm and Reconstruction (CDR) ist anders. Diese Technologie versucht nicht, Malware zu erkennen, sondern stuft alles zunächst einmal als nicht vertrauenswürdig ein. Legitime geschäftliche Informationen werden dabei aus Dateien extrahiert (wobei die Originaldateien gelöscht oder gespeichert werden). Dann wird geprüft, ob die extrahierten Informationen eine gültige Struktur haben. Anschließend werden neue, voll funktionsfähige Dateien erstellt, mit denen die Informationen an ihr Ziel weitergeleitet werden. Zero Trust CDR ist eine bahnbrechende Technologie, die das Risiko selbst von sehr komplexen Zero-Day-Angriffen und Exploits stark verringert. Dieser Wechsel von der Erkennung zum vorbeugenden Schutz ist insbesondere vor dem Hintergrund der jüngsten Entwicklungen im Bereich der hybriden Arbeitsplätze und digitalen Transformation und der sich daraus ergebenden Tatsache wichtig, dass Inhalte und elektronische Informationen heutzutage überall genutzt werden.

Malware-Schutz muss:

- **Immer sichere und voll funktionsfähige Inhalte bereitstellen,** damit Benutzer sich wirklich darauf verlassen können, dass Dateien aus externen Quellen sicher sind.
- **Zero-Day-Bedrohungen abwehren**, ohne dass die Abwehr über die neuesten Patches oder Signaturen verfügen muss.

Angriffsvektoren, die geschützt werden müssen:

- **Surfen im Internet**
- **Downloads aus dem Internet**
- **Web-Mail**
- **Soziale Medien**
- **Datei-Uploads**
- **E-Mail**
- **Web-Anwendungen**
- **Datenaustausch**

Malware-freie Daten

Pixelperfekte, vollständig bearbeitbare Dateien

Keine Fehlalarme

Keine Latenz

Abwehr aller Bedrohungen

Cyber-Kriminelle nutzen für Malware-Angriffe und Exploits bevorzugt digitale Inhalte. Ob Surfen im Internet, Internet-E-Mail oder Datei-Uploads und Social Media – digitale Inhalte werden regelmäßig mit bekannten, Zero-Day-Bedrohungen und sogar nicht erkennbaren Bedrohungen gespickt. Diese verbergen sich in Dateien und Bildern, die wir bei der Arbeit ständig verwenden.

Über 25 Jahre lang wurden diese Bedrohungen standardmäßig mit Abwehrmechanismen bekämpft, die auf dem Erkennungsprinzip beruhen. Diese Erkennung lässt sich jedoch einfach umgehen. Dazu muss man einfach nur die Signatur des Exploits ändern und schon kann die Malware ungehindert die Sicherheitsgrenze passieren. Erkennung allein reicht nicht mehr aus, um Mitarbeiter vor bekannten und unbekannten Bedrohungen, Zero-Day-Angriffen und Malware zu schützen.

Forcepoint Zero Trust CDR verhindert, dass dateibasierte Malware in das Unternehmen eindringen kann, ganz ohne Erkennungsmechanismus. Da Zero Trust CDR auf einzigartige Weise unbedenkliche Daten aus einer Datei extrahiert und weiterleitet und nicht versucht, bösartige Elemente zu erkennen, sind Benutzer selbst vor Zero-Day-Angriffen und völlig unbekannter Malware geschützt. Dieser Ansatz zur Abwehr von Malware kommt ohne ständige Aktualisierung der Signaturen der neuesten Bedrohungen und Zero-Day-Malware aus, um die Abwehr auf dem neuesten Stand zu halten.

Verbesserte Benutzererfahrung

Unternehmen suchen nach neuen, wirksameren Lösungen, um dem Problem von versteckter Malware Herr zu werden. Dabei laufen sie jedoch das Risiko, die Benutzererfahrung zu beeinträchtigen. Wenn eingehende Dateien mehrere Virenscanner oder Sandboxing-Prüfungen durchlaufen müssen, sorgt das für zusätzliche Latenz in Unternehmensprozessen. Wenn das ursprüngliche bearbeitbare Format von Dateien in ein festgelegtes, nicht bearbeitbares Format geändert wird, um die Dateien sicher zu machen, hat dies zur Folge, dass Mitarbeiter die Dokumente nicht ohne Weiteres austauschen, bearbeiten oder aktualisieren können. Die Absichten sind meist gut, doch im Endeffekt werden die Unternehmensprozesse dadurch langsamer und die Frustration bei Mitarbeitern wächst.

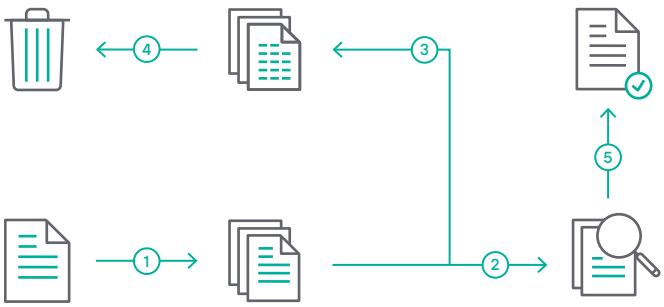
Forcepoint Zero Trust CDR verbessert die Benutzererfahrung, ohne bei der Sicherheit Kompromisse zu machen. Zero Trust CDR setzt nicht auf Erkennung, d. h. es entstehen keine Wartezeiten, weil das System Dateien noch auf bekannte Bedrohungen prüfen muss. CDR setzt auch keine Sandboxes ein, somit werden auch wichtige Unternehmensprozess nicht verzögert, weil Dateien in einer isolierten Umgebung geprüft werden müssen. Der Zero Trust CDR-Prozess dauert nur den Bruchteil einer Sekunde und erfüllt dennoch den Informationsbedarf eines Unternehmens – auf sichere Weise und ohne Latenz. Mit Zero Trust CDR können Benutzer schnell auf die benötigten Dateien zugreifen. Darüber hinaus verbessert Zero Trust CDR die Benutzererfahrung und liefert pixelperfekte, vollständig bearbeitbare Dateien, die garantiert Malware-frei sind.

Entlastung des SOC-Teams

Selbst in Unternehmen mit der besten erkennungsbasierten Abwehr kostet es viele Security Operations Center (SOC)-Teams immer noch zu viel Zeit und Geld, um Cyber-Sicherheitsvorfälle, die durch versteckte Malware in eingehenden Dateien verursacht werden, zu verhindern, zu erkennen und zu analysieren sowie entsprechend zu reagieren.

Forcepoint Zero Trust CDR befreit das SOC-Team von den täglichen Aufgaben, die bei der Verarbeitung von Quarantäne-Warteschlangen, Verwaltung von Fehlalarmen, Anwendung von Signatur-Updates und Verarbeitung von Meldungen potenzieller Verletzungen anfallen. Jede eingehende Datei durchläuft den Zero Trust CDR-Prozess, unabhängig davon, ob sie Malware enthält oder nicht. Jede Datei wird so bearbeitet, dass sie keine Bedrohungen enthält.

Funktionsweise



1. Zero Trust CDR identifiziert keine bekannte Malware, sondern extrahiert die nützlichen Informationen aus den Daten.
2. Die extrahierten Informationen werden in ein Zwischenformat umgewandelt und geprüft.
3. Dieser fortschrittliche Bedrohungsschutz soll sicherstellen, dass keine Bedrohungen oder Angriffe die nächste Ebene erreichen.
4. Die Originaldaten werden mit bekannter oder unbekannter Malware gespeichert oder gelöscht.
5. Die neuen Daten werden anschließend in ein normalisiertes Format gebracht, das die geprüften Informationen enthält. Die neuen Daten sind ein Replikat der Originaldaten, enthalten jedoch keine mögliche eingebettete Malware und sind garantiert sicher.

Unvergleichlicher Schutz

- Liefert bedrohungsfreie Daten mit höchster Garantie – pixelperfekt und vollständig bearbeitbar
- Nicht einmal sehr komplexe Angriffe sind eine Bedrohung
- Keine Gefährdung durch sogenannte „Zero-Day"-Bedrohungen

Extrem vielseitig

- Ist mit bestehenden Abwehrmechanismen und Technologien an der Netzwerkgrenze kompatibel
- Wandelt eine Vielzahl der beliebtesten Dateiformate um, einschließlich aller Office-Dateien, Bilder und PDF-Dateien (die von Angreifern am häufigsten verwendeten Formate)
- Schützt eine Vielzahl von Angriffsvektoren, einschließlich Internet, E-Mail und Datei-Uploads

Verschiedene Bereitstellungsoptionen

- Lokale oder virtuelle Bereitstellung und Bereitstellung in der Cloud
- Kann innerhalb von Minuten bereitgestellt werden und einsatzbereit sein

Anhang A: Übersicht über die Komponenten der Lösung

Forcepoint Zero Trust CDR für Web-Gateways	Forcepoint Zero Trust CDR für Web-Gateways schützt Internetnutzer vor Malware, die sich in Downloads aus dem Internet, Internet-E-Mail und Social Media versteckt. Die Lösung wird an der Netzwerkgrenze bereitgestellt und kann in den bestehenden Secure Web-Gateway (SWG) integriert werden. Mithilfe von Richtlinien im Web-Gateway wird bestimmt, welche Dateitypen zur Verarbeitung an Forcepoint Zero Trust CDR weitergeleitet werden.
Forcepoint Zero Trust CDR für Remote-Browser-Isolation	Forcepoint Zero Trust CDR für Remote-Browser-Isolation sorgt dafür, dass Benutzer, die über Remote-Browser-Isolation im Internet surfen, Dateien sicher auf den physischen Host herunterladen und sich sicher sein können, dass die Dateien keine Malware enthalten.
Forcepoint Zero Trust CDR für Datei-Uploads	Forcepoint Zero Trust CDR für Datei-Uploads schützt Unternehmen vor Malware in Dateien, die aus dem Internet hochgeladen werden. Die Lösung kann zusammen mit einem Reverse-Web-Proxy oder als Teil einer Cloud-basierten Web-Anwendungen bereitgestellt werden.
Forcepoint Zero Trust CDR für E-Mail	Forcepoint Zero Trust CDR für E-Mail schützt Benutzer vor versteckter Malware in E-Mail-Nachrichten und Anhängen. Die Lösung wird normalerweise zwischen dem E-Mail-Sicherheitsmechanismus am Netzwerkrand und dem E-Mail-Server des Unternehmens bereitgestellt.
Forcepoint Zero Trust CDR für File-Sharing	Forcepoint Zero Trust CDR für File-Sharing stellt sicher, dass Dateien, die zwischen Dateispeichern in unterschiedlichen Netzwerken verschoben werden, keine dateibasierte Malware enthalten.
Forcepoint Zero Trust CDR für Web-Anwendungen	Forcepoint Zero Trust CDR für Web-Anwendungen stellt sicher, dass strukturierte Daten, die zwischen Netzwerken verschoben werden, ausschließlich vordefinierten Schemata entsprechen, die sicherstellen, dass Web-Anwendungen nicht als Angriffsvektor missbraucht werden können.
Forcepoint Zero Trust CDR Cloud APIs	Forcepoint Zero Trust CDR kann nicht nur lokal, sondern auch über Cloud-basierte APIs für Entwickler bereitgestellt werden, die Content Disarm and Reconstruction (CDR) auch in Ihre Web-Anwendungen und Workflows integrieren müssen.

Anhang B. Dateitypen, die von Forcepoint Zero Trust CDR bedrohungsfrei gemacht werden

Die folgenden Dateitypen werden umgewandelt und von Forcepoint Zero Trust CDR bedrohungsfrei gemacht:

OFFICE-DATEIEN	
DATEITYP	**ERWEITERUNG**
Bitmap-Bild	BMP
Microsoft Office X-Dokument	DOCX
Microsoft Enhanced Metafile	EMF
E-Mail-Nachricht	EML
GIF-Bild	GIF
HTML-Datei	HTML
ICAL-Datei	ICAL
JPEG 2000	JP2K
JPEG-Bild	JPEG
MIME HTML-Archiv	MHT
Multipurpose Internet Mail Extensions	MIME
Adobe PDF	PDF
PNG-Bild	PNG
Microsoft Office X PowerPoint	PPTX
Rich Text	RTF
Reiner Text	TXT
TIFF-Bild	TIFF
Microsoft Windows-Metadatei	WMF
Microsoft Office X Excel	XLSX
Zip-Archiv	ZIP

STRUKTURIERTE DATENDATEIEN	
DATEITYP	**ERWEITERUNG**
Kommaseparierte Werte	CSV
JSON strukturierte Daten	JSON
Google Protocol Buffers 3	Proto3
XML strukturierte Daten	XML

Auch die folgenden Dateiformate werden durch vorherige Konvertierung in ein Zwischenformat bedrohungsfrei gemacht:

FORMAT	ORIGINAL	ÜBERSETZT	ENDFORMAT
Veraltetes Microsoft Word	DOC	DOCX	DOC
Veraltetes Microsoft PowerPoint	PPT	PPTX	PPT
Veraltetes Microsoft Excel	XLS	XLSX	XLS
OpenDocument-Text	ODT	DOCX	ODT
OpenDocument-Tabelle	ODS	XLSX	ODS
OpenDocument-Präsentation	ODP	PPTX	ODP
Rich Text	RTF	DOCX	RTF
eXtensible Paper Specification	XPS	PDF	XPS
EPUB Book Reader-Format	EPUB	PDF	EPUB
Mobipocket E-Book-Format	MOBI	DOCX	-
Computer Graphics Metafile	CGM	PDF	-
Adobe Photoshop	PSD	PNG	PSD
Microsoft One Note	ONE	PDF	-
AutoCAD Drawing	DWG	PDF	-
Veraltetes AutoCAD Drawing	DXF	PDF	-
Veraltetes Microsoft Visio	VSD	PDF	-
Microsoft Visio	VSDX	PDF	-
XLS Formatting Object	FO	PDF	-
7Zip-Archiv	7Zip	ZIP	7Zip
BZip2-Archiv	BZip2	ZIP	BZip2
GZIP-Archiv	Gzip	ZIP	GZip
Z-Archiv	Z	ZIP	Z
TAR-Archiv	TAR	ZIP	TAR
Microsoft CAB-Archiv	CAB	-	ZIP

Forcepoint

forcepoint.com/contact

Über Forcepoint

Forcepoint ist einer der weltweit führenden Anbieter von Cyber-Sicherheit im Bereich Anwender- und Datensicherheit und hat es sich zur Aufgabe gemacht, Organisationen zu schützen und gleichzeitig die digitale Transformation und das Wachstum voranzutreiben. Die auf menschlichem Verhalten basierenden 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.

[FP-Zero Trust CDR-Brochure-DE] 10Mar2022