MATRIX42

AUTOMATED ENDPOINT SECURITY

DAS EINDRINGEN VON VIREN IST OFT NICHT VERMEIDBAR, EIN UNAUTORISIERTER DATENTRANSFER SCHON.

Wenn selbst umfassender Schutz versagt, hilft Automated Endpoint Security, die Auswirkungen von Cyber-Attacken zu verhindern. Automated Endpoint Security konzentriert sich darauf, Angreifer am Erreichen ihres eigentlichen Ziels zu hindern: Stehlen, Manipulieren oder Verschlüsseln von Endpunkt- und Serverdaten.

Endpoint Security neu gedacht

Die IT-Sicherheit steht vor einem grundlegenden Paradigmenwechsel: Wurden digitale Arbeitsplätze bislang durch eine möglichst zuverlässige Abschirmung vor Angriffen geschützt, folgt die Idee der Post Infection Protection einer gänzlich anderen IT-Sicherheitsstrategie: Da bisherige Security-Maßnahmen wie Firewalls und Antivirentools keinen ausreichenden Schutz mehr vor Viren und Ransomware liefern, fokussiert sich Post Infection Protection darauf, die Ausbreitung von Schadsoftware zuverlässig zu verhindern, nachdem sie eingedrungen ist. enSilo, innovatives Cyber Security Start-up, das von Gartner im Digital Workplace Security Market Report 2016 als „Cool Vendor“ bezeichnet wurde, hat sich genau darauf spezialisiert und eine real-time Data Protection Plattform entwickelt.

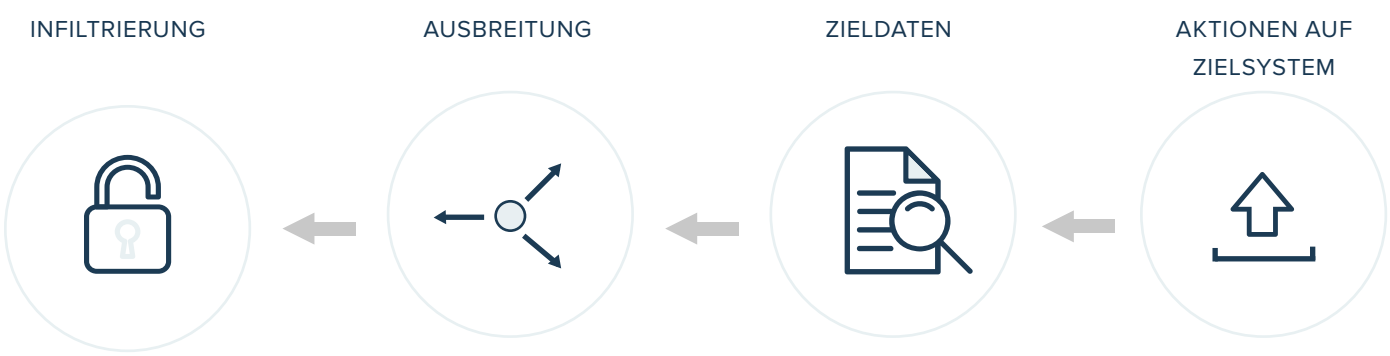
Matrix42, führender Anbieter für Workspace Management Lösungen, hat eine strategische Partnerschaft mit enSilo abgeschlossen und bietet ab sofort die Produkte des innovativen Security-Unternehmens exklusiv in Zentraleuropa an und integriert enSilo in die ganzheitliche Digital Workspace Management Suite.

Echtzeit-Datenschutz

enSilo ist keine herkömmliche Endgeräte-Sicherheitslösung, die auf die Vereitelung von Infiltrierungsversuchen abzielt.

enSilo ist eine Plattform für Datenschutz, die die Funktionen einer Endpoint Prevention Platform (EPP) mit denen einer Endpoint Detection and Response (EDR) kombiniert und die Steuerung der Kommunikation der Applikationen ermöglicht – und das in Echtzeit.

KEHREN SIE DIE CYBER KILL CHAIN UM



Ende der Abwehr

Beginn der Abwehr

Eine Infiltrierung ist nicht immer zu verhindern. Während viele Cybersicherheitsanbieter den Fokus auf die Prävention von Infiltrierungen legen, konzentriert sich enSilo dagegen auf die Sicherung der Ausgangspunkte, damit Ihre Daten nicht verschlüsselt, manipuliert oder entwendet werden können. Das verschafft Ihrer IT Security genügend Zeit, die Eingangstore auf mögliche Sicherheitslücken zu überprüfen und Gegenstrategien zu entwickeln.

„Zunächst müssen der unautorisierte Datentransfer und die Ausbreitung der Angreifer im Netzwerk gestoppt werden. Danach müssen die Eindringlinge daran gehindert werden, Daten zu stehlen und sich die Rechte eines Domänen-Admins zu verschaffen.“

SANS

Datendiebstahl in Echtzeit verhindern

enSilo schützt Ihre Daten in Echtzeit vor einem Diebstahl durch Angreifer, da es auf der Ebene des Betriebssystems arbeitet.

Echtzeitschutz gegen Ransomware

enSilo hält Angreifer auf, bevor diese Ihre Daten in böswilliger Absicht verschlüsseln können. Es arbeitet auf Ebene des Betriebssystems und ist damit die einzige Universallösung.

Reibungslose Sicherheit verhindert Datendiebstahl in Echtzeit

Cybersicherheit sollte keine negativen Auswirkungen auf Ihre Geschäftsabläufe haben. Selbst mit einem kompromittierten System sollten Sie weiterarbeiten können.

Eine Warnmeldung pro aktiver Bedrohung

enSilo warnt Sie erst, nachdem es eine schädliche Outbound-Kommunikation, Dateimanipulation oder unauthorisierte Verschlüsselung unterbunden hat.

Der enSilo Collector kann auf folgenden Betriebssystemen (sowohl 32-Bit- als auch 64-Bit-Versionen) installiert werden:

- Windows XP SP2/SP3, 7, 8, 8.1 und 10
- Windows Server 2003 R2 SP2, 2008 R2 SP2, 2012, 2012 R2 und 2016
- MacOS Versionen: Maverick (10.9), Yosemite (10.10), El Capitan (10.11) und Sierra (10.12)
- Linux Versionen: RedHat Enterprise Linux, CentOS 6.8, 7.2 und 7.3, 64-bit
- VDI Environments: VMware Horizons 6 und Citrix XenDesktop 7

FUNKTIONSWEISE

ENSILO COLLECTOR

BEI VERBINDUNGSAUFBAU

BEI DATEIMODIFIZIERUNG

MIT KONSEQUENZ VERBUNDENE AKTIVITÄTEN

ENSILO CORE

SCHRITT 1:
Der auf dem Rechner installierte enSilo Collector erfasst Betriebssystem-Metadaten.

SCHRITT 2:
Wird der Aufbau einer Verbindung oder eine Dateimodifizierung angefordert, sendet der Collector eine Momentaufnahme der Anforderung zusammen mit den zugehörigen Betriebssystem-Metadaten an enSilo Core.

SCHRITT 3:
Unter Nutzung der Technologie von enSilo analysiert enSilo Core die Betriebssystem-Metadaten mit der Anforderung und setzt die Richtlinien zur Verhinderung eines Datendiebstahls bzw. Ransomware-Angriffs um.

SCHRITT 4:
Es werden nur legitime Verbindungen oder Dateimodifizierungen zugelassen.

ENSILO WURDE 2016 VON GARTNER ALS „COOL VENDOR IN DIGITAL WORKPLACE SECURITY“ AUSGEZEICHNET.

„Chief Information Security Officers und andere Entscheidungsträger für IT-Sicherheit sollten neue Anbieter von Sicherheitstechnologien in Erwägung ziehen, die einen sicheren digitalen Arbeitsplatz unterstützen.“*

Gartner, Cool Vendor 2016

* Quelle: Gartner, Inc.: „Cool Vendors in Digital Workplace Security“, 2016, Ayal Tirosh, Lawrence Pingree, Avivah Litan, Lawrence Orans, Adam Hils, Felix Gaehtgens, Brian Reed, Peter Firstbrook. Haftungsausschluss von Gartner: Gartner unterstützt keine Anbieter, Produkte oder Dienstleistungen, die in seinen Marktforschungsberichten genannt werden. Ebenso wenig rät Gartner Technologieanwendern, nur Anbieter mit den höchsten Bewertungen oder anderen Auszeichnungen auszuwählen. Marktforschungsberichte von Gartner geben lediglich die Meinung des Unternehmens wieder und sollten nicht als Tatsachenaussage ausgelegt werden. Gartner lehnt jegliche ausdrückliche oder stillschweigende Gewährleistung hinsichtlich des vorliegenden Forschungsberichts ab, insbesondere in Bezug auf handelsübliche Qualität oder die Eignung für einen bestimmten Zweck. Das Gartner Cool Vendor Logo ist eine Marke und Dienstleistungsmarke von Gartner, Inc. und/oder seinen Tochtergesellschaften und wird mit Genehmigung verwendet. Alle Rechte vorbehalten.

Standorte

Hauptsitz Deutschland
Elbinger Straße 7
60487 Frankfurt am Main
Deutschland
Telefon: +49 69 66773-8380
Fax: +49 69 66778-8657
info@matrix42.com

Niederlassung Schweiz und Österreich
Matrix42 Helvetia AG
Poststrasse 30
6300 Zug
Schweiz
Telefon: +41 41 720 42 20
info@matrix42.ch

Über Matrix42

Matrix42 ist einer der Top-Anbieter von Software für das Arbeitsplatzmanagement. Unter dem Motto „Reimagine Workspace Management“ bietet das Unternehmen zukunftsorientierte Lösungen für moderne Arbeitsumgebungen. Mit den Lösungen von Matrix42 können Unternehmen physische, virtuelle oder mobile Arbeitsbereiche einfach und effizient bereitstellen und verwalten. Mehr als 3.000 Kunden – darunter BMW, Infineon und Carl Zeiss – verwalten mit den Workspace Management Lösungen von Matrix42 über 3 Millionen Arbeitsplätze weltweit.

Matrix42 hat den Hauptsitz in Frankfurt am Main in Deutschland und ist in sieben weiteren Ländern erfolgreich aktiv – Österreich, Schweiz, Frankreich, Niederlande, Vereinigtes Königreich, Australien und Vereinigte Staaten von Amerika.

Matrix42 bietet seine Lösungen branchenübergreifend Organisationen an, die Wert auf ein zukunftsorientiertes und effizientes Arbeitsplatzmanagement legen. Dabei arbeitet das Unternehmen auch erfolgreich mit Partnern zusammen, die die Matrix42 Kunden vor Ort beraten und betreuen.

www.matrix42.com