SOLUTION BRIEF

Schutz von OT-Infrastrukturen in Echtzeit mit automatisierter Endpoint-Security

Zusammenfassung

Die Infrastrukturen von Betriebstechnologie (OT) und Informationstechnologie (IT) wachsen zunehmend zusammen. Diese Entwicklung betrifft auch Cyber-Security-Experten, von denen laut einer Studie 70 % die Konvergenz von OT und IT unterstützen.[1] Besonders der CISO spielt dabei eine zentrale Rolle: 65 % der Befragten halten ihn beim Schutz einer konvergierten Infrastruktur für den Hauptzuständigen.[2]

CISOs stehen bei der Erfüllung dieser Erwartungen zahlreichen Herausforderungen gegenüber, darunter die Sicherung von OT-Endpunkten. FortiEDR bietet eine robuste Lösung für die OT-Endpoint-Security mit einem effektiven Bedrohungsschutz in Echtzeit, der sowohl vor als auch nach einer Infektion greift. Unternehmen, die FortiEDR auf OT-Endpunkten bereitstellen, profitieren einer schnelleren Bedrohungsabwehr, automatisierten Aktionen und der Vermeidung von Produktionsstörungen.

FortiEDR bietet einen überlegenen Endpunkt-Schutz für Produktionsumgebungen mit:

- Bedrohungserkennung in Echtzeit
- Schutz nach Kompromittierungen
- Beseitigung von Infektionen ohne Produktionsstörungen
- virtuellem Patching
- Unterstützung von Air-Gapped-Systemen und älteren Windows-Systemen
- Optionen für die On-Premises-Implementierung

Cyber-Angriffe auf kritische Infrastrukturen nehmen zu: Laut einer Umfrage rechnen 54 % der Befragten in den nächsten 12 Monaten mit einem Angriff auf kritische Infrastrukturen.[3]

Anfällige Endpunkte in der Betriebstechnologie (OT)

OT-Infrastrukturen in den Bereichen Fertigung, Transport, Versorgung, Öl und Gas sowie in anderen Branchen werden zunehmend zum Ziel hochkomplexer Cyber-Angriffe. Die Waffe der Wahl ist Cryptoware – eine Ransomware-Variante, die in wenigen Sekunden wichtige Steuerungsinformationen verschlüsseln und so Produktionslinien und Sicherheitssysteme stören oder sogar herunterfahren kann. Die Motive für solche Angriffe sind unterschiedlich: Einige streben nach finanziellem Gewinn durch Lösegeldzahlungen, andere wollen kritische Infrastrukturen lahmlegen und in einer Stadt oder Region möglichst viel Chaos anrichten.

In der Vergangenheit waren OT-Infrastrukturen in sich geschlossen – auch als „Air-Gapped-Systeme“ bezeichnet – und daher relativ isoliert von internetbasierten Bedrohungen. Durch die Konvergenz von OT- und IT-Systemen werden nun veraltete, ungepatchte OT-Endpunkte quasi zur „Einladung“ für Cyber-Kriminelle. Verschärft wird dieses Problem durch die älteren Betriebssysteme und begrenzten Systemressourcen, mit denen ein Großteil der Betriebstechnologie heute noch arbeitet. Das alles erschwert den Schutz von OT-Endpunkten mit herkömmlichen Endpoint-Security-Lösungen erheblich.

Als Reaktion auf diese Sicherheitsprobleme haben viele Unternehmen unterschiedlichste isolierte Einzellösungen für die Security installiert, von denen jede aber immer nur ein Risiko abdeckt. Die Folge ist eine steigende Komplexität bei gleichzeitiger Schwächung des Sicherheitsprofils. So bezeichneten bei einer Umfrage 55 % der Befragten „isolierte und fragmentierte Systeme“ als erhebliche Herausforderung beim Security-Management von Betriebstechnologie (OT).[4]

FortiEDR für OT-Umgebungen

FortiEDR löst diese und weitere Probleme mit einem intelligenten Bedrohungsschutz, der in Echtzeit funktioniert und sowohl vor als auch nach einer Infektion sämtliche OT-Endpunkte abdeckt. Bei FortiEDR handelt es sich um eine schlanke Next-Generation-Endpoint-Security-Lösung mit umfassenden EDR-Funktionen, die sich selbst auf älteren OT-Geräten mit begrenzten Systemressourcen einfach implementieren lässt.

Zu den wichtigsten Funktionen von FortiEDR gehören ein Virenschutz der nächsten Generation (Next-Generation-Antivirus, NGAV), Kontrolle über die Anwendungskommunikation, eine automatische Endpoint Detection und Response (EDR), die Blockierung von Bedrohungen in Echtzeit sowie die Bedrohungssuche, Incident Response und ein virtuelles Patching (Abbildung 1). FortiEDR nutzt die Architektur der Fortinet Security Fabric und lässt sich mit Security-Fabric-Komponenten wie FortiGate, FortiNAC, FortiSandbox und FortiSIEM integrieren.

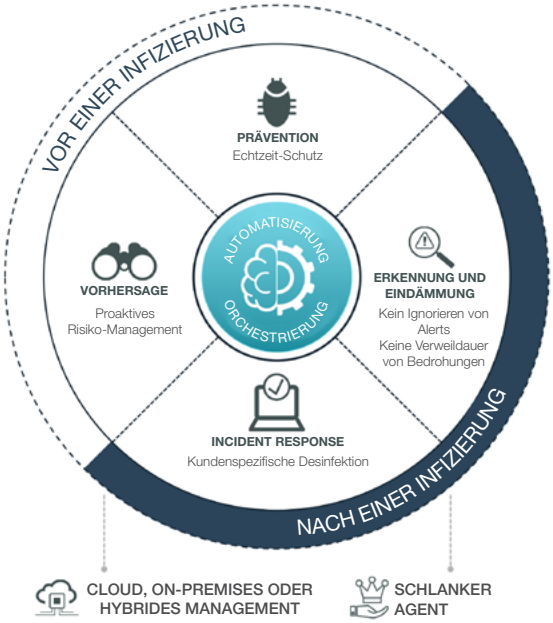


Abbildung 1: Funktionen von FortiEDR

Wesentliche Vorteile von FortiEDR

Mit Vorteilen wie einer automatisierten Bedrohungsabwehr in Echtzeit, Produktionskontinuität und unterbrechungsfreier Risikominderung bietet FortiEDR OT-Unternehmen einen spürbaren geschäftlichen Nutzen.

Automatisierte Bedrohungsabwehr in Echtzeit

Erkennt FortiEDR potenziell bösartige Prozesse, werden diese in Echtzeit mit der automatischen Blockierung sofort eingedämmt. Gleichzeitig sammelt der Fortinet Cloud Service weitere Beweise und validiert und klassifiziert Sicherheitsvorfälle. Mit anpassbaren Playbooks können Security-Teams automatisierte Aktionen nach Kriterien wie Endpunkt-Gruppe, geschäftliche Kritikalität oder Bedrohungskategorie einrichten. Zu den automatisierten Reaktionen und Gegenmaßnahmen gehören das Beenden von Prozessen, das Entfernen schädlicher oder infizierter Dateien, das Entfernen dauerhafter Infektionen (Persistenz-Bereinigung), das Informieren von Benutzern und die Ticket-Erstellung.

FortiEDR sichert Endpunkte sowohl vor als auch nach einer Infektion in Echtzeit und beseitigt so die Gefahr, dass wichtige Alerts übersehen werden und zu Sicherheitsvorfällen führen. Auch werden Incident-Response-Abläufe standardisiert und die Verwendung von Security- und Betriebsressourcen wird optimiert.

Keine Unterbrechung der Produktion

Automatische Echtzeit-Reaktionen können jedoch ein Problem darstellen, das viele Security-Experten nur zu gut kennen: Legitime Anwendungsaktivitäten lösen plötzlich die Bedrohungserkennung aus und erzeugen Fehlalarme. Ist die Bedrohungsabwehr zu „scharf“ eingestellt, können Anwendungen unterbrochen werden oder schlimmstenfalls abstürzen und geschäftskritische Produktionssysteme lahmlegen.

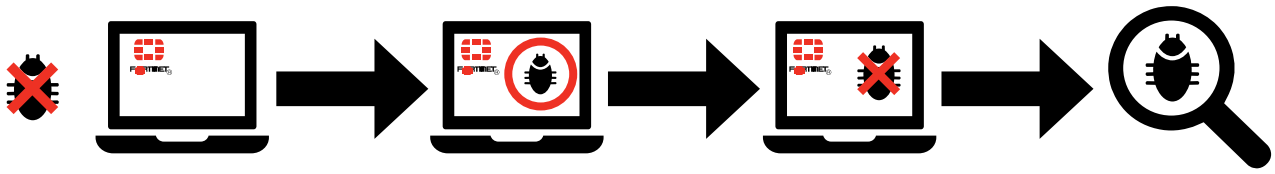
Statt Prozesse zu beenden und Endpunkte unter Quarantäne zu stellen, entschärft FortiEDR Bedrohungen, indem es die ausgehende Kommunikation und Zugriffe auf das Dateisystem blockiert. Stellt sich ein verdächtiger Prozess als harmlos heraus, hebt FortiEDR die Blockierung wieder auf – alles mit minimalen Auswirkungen auf Produktionssysteme. Bei einer begründeten Bedrohung oder einem Sicherheitsvorfall behebt FortiEDR die Infektion, ohne den Computer vom Netz zu nehmen. Die Fertigungssysteme bleiben online und die Benutzer sind nicht betroffen. Diese Funktion ist besonders wichtig für konvergierte IT-OT-Infrastrukturen, da Security-Teams schnell und effektiv Maßnahmen zur Sicherung von OT-Geräten ergreifen und unbeabsichtigte Konsequenzen für die IT vermeiden können.

Unterbrechungsfreie Risikominderung

Das Patching von OT-Systemen kann schwierig sein. Um Produktionsstörungen zu vermeiden, müssen Betriebsteams oft vorgeschriebene Änderungsprozesse im geplanten Wartungsfenster befolgen, was aber nur eine Eindämmung des Problems erlaubt. In der Zwischenzeit sind die Systeme anfällig für Angriffe.

FortiEDR löst dieses Problem mit einer kontinuierlichen Anwendungs- und Schwachstellenbewertung. Das Security-Team kann so Risiken durch virtuelles Patching proaktiv minimieren. Dieser vorausschauende Ansatz reduziert die Gefährdung und verhindert, dass in der Produktion genutzte Rechner zwischen geplanten Wartungsfenstern vom Netzwerk genommen werden müssen.

Wie FortiEDR OT-Endpunkte schützt



Der FortiEDR-Agent auf dem Endgerät blockiert die meiste dateibasierten Malware vor ihrer Ausführung, um eine Infektion zu verhindern.

Tritt eine Infektion auf, erkennt und entschärft FortiEDR die Bedrohung in Echtzeit, um den Schaden einzudämmen.

Ist die Bedrohung eingedämmt, koordiniert FortiEDR die Incident Response anhand von Playbooks und cloudbasierten Informationen.

FortiEDR erhält den RAM-Inhalt, erstellt Snapshots und bietet Anleitungen für forensische Untersuchungen.

Abbildung 2: Wie FortiEDR funktioniert

Entdecken und vorhersagen

FortiEDR erkennt proaktiv die Angriffsfläche des Endpunkts und wehrt Bedrohungen ab. Verdächtige Geräte und -Anwendungen werden gemeldet, Schwachstellen in Systemen und Anwendungen identifiziert und Risiken durch virtuelles Patching proaktiv minimiert.

Vorbeugen

Der kernelbasierte NGAV verhindert automatisch die Ausführung von dateibasierter Malware. Durch Kombination mit kontinuierlich aktualisierten Bedrohungsdaten aus cloudbasierten Feeds und maschinellem Lernen lernt FortiEDR im Laufe der Zeit dazu, um Bedrohungen noch effektiver zu identifizieren.

Erkennen und entschärfen

Mit einer verhaltensbasierten Erkennung ist FortiEDR die einzige Lösung auf dem Markt, die auch nach einer Infektion schützt und Sicherheitsverletzungen sowie Ransomware-Schäden in Echtzeit verhindert.

Reagieren und beheben

Security-Teams können mit anpassbaren Playbooks die Reaktion auf Sicherheitsvorfälle koordinieren, Incident-Response- und Remediation-Prozesse optimieren und automatisieren sowie betroffene Computer online halten. Durch diesen Ansatz werden Störungen von Benutzern und Geschäftsabläufen vermieden, ohne das Netzwerk einem Risiko auszusetzen.

Untersuchen und suchen

FortiEDR liefert detaillierte Informationen zu Bedrohungen für forensische Untersuchungen. Die einzigartige geführte Benutzeroberfläche bietet hilfreiche Anleitungen und Best Practices und schlägt Security-Analysten die nächsten logischen Schritte vor.

In der weltweiten Versorgungswirtschaft bezeichnen 64 % der Entscheidungsträger Cyber-Angriffe als große Herausforderung.[5]

Implementierungs- und MDR-Services von Fortinet:

- Fortinet Professional Services bietet Expertenunterstützung für die Implementierung, Konfiguration, Einrichtung und Anpassung von Playbooks und viele weitere Aufgaben.
- FortiResponder, der MDR-Service von Fortinet, bietet 24/7 eine Bedrohungsüberwachung, Alert-Sichtung und Infektions-beseitigung per Fernzugriff.
- Zertifizierte Fortinet MSSP-Partner erbringen MDR-Services bis hin zum kompletten SOC-Management.

Fazit

Angesichts der stetig wachsenden Anzahl und Komplexität fortschrittlicher Bedrohungen – insbesondere von Ransomware – müssen Unternehmen ihre Security auf breiter Front verstärken. Das gilt besonders für Endgeräte in der Betriebstechnologie, die sogenannten OT-Endpunkte. FortiEDR bietet einen schlanken Endpunkt-Schutz der nächsten Generation, der sich einfach auf OT-Geräten mit begrenzten Ressourcen bereitstellen lässt. Mit FortiEDR können Security-Teams die Sicherheit von Endgeräten erhöhen und so die Incident Response beschleunigen, Security-Abläufe optimieren und kostspielige Störungen der Produktionsanlagen und Benutzerproduktivität vermeiden.

[1] „Safety, Security & Privacy in the Interconnected World of IT, OT & IIoT". Ponemon Institute, Februar 2019.

[2] Ebd.

[3] Ebd.

[4] „Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?". Siemens und Ponemon Institute, 2019.

[5] Ebd.

FORTINET

www.fortinet.com/de

29. Juni 2020, 13:10 Uhr

579128-0-0-DE