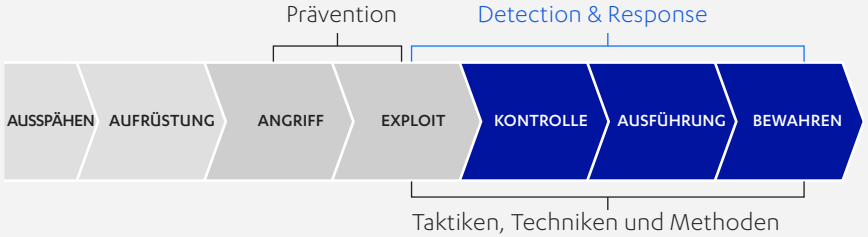
GEZIELTE ANGRIFFE STOPPEN

F-Secure Rapid Detection & Response

F-Secure

UNTERNEHMEN UND DATEN VOR KOMPLEXEN CYBERATTACKEN SCHÜTZEN

Ein effektiver Bedrohungsschutz, der Angriffe blockt, ist der Kern aller Cybersicherheit. Auf präventive Maßnahmen allein dürfen sich Unternehmen, die sich und ihre Daten vor den Taktiken, Techniken und Methoden der Angreifer schützen wollen, aber nicht verlassen.



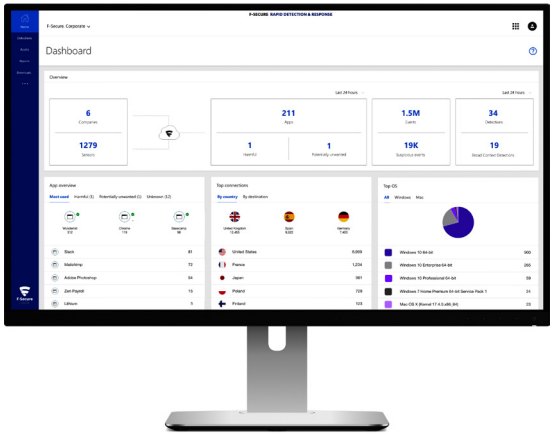
Die sich ständig verändernde Bedrohungslandschaft und Regelwerke wie die DSGVO erfordern, dass Unternehmen auch auf die nachträgliche Erkennung von Sicherheitsverletzungen vorbereitet sind. Konkret muss sichergestellt sein, dass Sie schnell auf komplexe Angriffe reagieren können.

F-Secure Rapid Detection & Response ist eine Lösung, die von einem erfahrenen Threat-Hunter-Team trainiert wird.

Damit kann Ihre IT-Abteilung oder ein zertifizierter Dienstleister Ihr Unternehmen vor komplexen Bedrohungen schützen. Mithilfe der erstklassigen Cybersicherheitsexperten von F-Secure können Ihre IT-Profis schnell und effektiv auf Vorfälle reagieren. Wenn Sie sich ganz auf Ihr Kerngeschäft konzentrieren wollen, überlassen Sie Detection und Response getrost einem Dienstleister und greifen im Angriffsfall auf die Unterstützung von Experten zurück.

AUTOMATISIERT UND ANGELEITET GEZIELTE AN-GRIFFE STOPPEN

Wie können Sie komplexe Angriffe erkennen? Indem Sie die fortschrittlichsten Analysetechniken und maschinellen Lernverfahren nutzen, die Ihr Unternehmen vor komplexen Cyber-bedrohungen und Sicherheitsverletzungen schützen.



Die marktführende Lösung End-point Detection & Response (EDR) von F-Secure gibt Ihnen kontextuellen Ein-blick in komplexe Bedrohungen und ermöglicht Ihnen, automatisiert und unter Anleitung zu reagieren.

Wenn es zu einer Sicherheitsverlet-zung kommt, brauchen Sie mehr als nur einen Alarm. Damit Sie optimal reagie-ren können, müssen Sie die Struktur des Angriffs verstehen. Mit unserer Broad Context Detection™, zertifizierten Dienstleistern und integrierter Auto-matisierung stoppen Sie die Angriffe schnell und bekommen konkrete, umsetzbare Anleitungen zur weiteren Problemlösung.

FUNKTIONSWEISE

Stets zu Diensten: branchenführende Technologie und Sicherheitsexperten von F-Secure

1. Ressourcenschonende Sensoren auf allen Endgeräten überwachen Verhaltensereignisse auf Anwenderseite und geben sie zur Echtzeitanalyse sowie an unsere Broad Context Detection™ weiter, um böswilliges Verhalten von normalem Benutzerverhalten zu unterscheiden.

2. Warnmeldungen mit Risikoeinstufung und visualisiertem Kontext über alle betroffenen Hosts hinweg erleichtern die Bestätigung der Erkennung, ob durch den F-Secure Partner oder das eigene IT-Team. Optional sind automatisierte Reaktionsmaßnahmen und die Eskalation an F-Secure.

3. Nach einer bestätigten Erkennung gibt die Lösung Ratschläge und Handlungsempfehlungen für die erforderlichen Schritte, mit denen Sie die Bedrohung schnell eindämmen und beheben können.

DIE NADEL IM HEUHAUFEN – EIN BEISPIEL AUS DER PRAXIS

Die Erkennung komplexer Bedrohungen aus den winzigen Einzelereignissen, die bei Angriffen ausgelöst werden, gleicht der Suche nach einer Stecknadel im Heuhaufen.

Bei einer Kundeninstallation mit 325 Knoten hatten unsere Sensoren in einem Monat etwa 500 Millionen Ereignisse gemeldet. Nach der Rohdatenanalyse in unseren Backend-Systemen reduzierte sich diese Zahl auf 225.000.

Nach der weiteren Analyse verdächtiger Vorfälle durch unsere Broad Context Detection™ blieben davon noch 24 Ereignisse übrig. Diese wurden im Detail ausgewertet und lediglich sieben davon wurden letztlich als echte Bedrohungen identifiziert.

IT- und Sicherheitsteams können sich also auf weniger, aber präzisere Erkennungsergebnisse konzentrieren und dadurch bei realen Cyberangriffen schneller und effektiver reagieren.

500 MIO.
Sicherheitsereignisse/Monat
Erfasst von 325 Endgerätesensoren

225.000
verdächtige Ereignisse
nach Echtzeit-Verhaltensanalyse der Ereignisse

24
Erkennungen
nach Analyse der Ereignisse im breiteren Kontext

7
echte Bedrohungen
nach Bestätigung der Erkennungen als tatsächliche Bedrohungen

TRANSPARENZ

Unmittelbarer Einblick in IT-Umgebung und Sicherheitsstatus

- Verbesserte Transparenz von IT-Umgebung und Sicherheitsstatus durch Inventarisierung der Anwendungen und Endgeräte.
- Identifizierung verdächtiger Aktivitäten durch Erfassung und Korrelation von Verhaltensereignissen, die über übliche Malware hinausgehen.
- Warnungen mit Hintergrundkontext und Informationen zur Kritikalität erleichtern die Vorfallreaktion.

ERKENNUNG

Schutz des Geschäfts durch die rasche Erkennung von Sicherheitsvorfällen

- Minimierung von Ausfallzeiten und negativen Auswirkungen auf die Markenreputation durch schnelle Erkennung und Beendigung zielgerichteter Angriffe.
- Implementierung binnen Stunden – so sind Sie sofort optimal geschützt.
- Compliance mit Standards (PCI, HIPAA und DSGVO), die die Meldung von Sicherheitsvorfällen innerhalb von 72 Stunden vorschreiben.

REAKTION

Schnelle Reaktion mit Anleitung und Automatisierung

- Dank integrierter Automation und Analyse kann sich Ihr Team auf relevante Bedrohungen konzentrieren.
- Die Warnungen umfassen Anleitungen zur Vorfallsreaktion; rund um die Uhr aktive, automatisierte Reaktionen sind ebenfalls möglich.
- Expertise und Ressourcen, die Ihnen fehlen, kann ein zertifizierter und von F-Secure unterstützter Dienstleister zur Verfügung stellen.

MERKMALE

Endgerätesensoren

Diskrete Monitoring-Tools, die mit allen Endgeräte-Sicherheitslösungen zusammenarbeiten

- Ressourcenschonende Sensoren, die auf allen relevanten Computern Ihres Unternehmens laufen
- Übergreifende Single-Client- und Management-Infrastruktur mit Endgeräte-sicherheitslösungen von F-Secure
- Datenschutzgerechte Verhaltenserfassung auf den Endgeräten

Broad Context Detection™

Die spezielle Erkennungstechnologie von F-Secure, die es einfach macht, das Ausmaß eines zielgerichteten Angriffs zu verstehen

- Verhaltens-, Reputations- und Big-Data-Analyse in Echtzeit mit maschinellem Lernen
- Automatische Kontexteinordnung von Erkennungen, Visualisierung auf der Zeitleiste
- Einbeziehung von Daten zu Risikostufen, zur Kritikalität des betroffenen Hosts und zur jeweiligen Bedrohungslandschaft

Anwendungstransparenz

Durchblick bei IT-Umgebung und Sicherheitsstatus, einfacher denn je

- Ermittlung von schädlichen und un-erwünschten Anwendungen sowie der externen Adressen von Cloud-Services
- Reputationsdaten von F-Secure zur Identifi-zierung potenziell gefährlicher Anwendungen
- Blockierung fraglicher Anwendungen und Cloud-Services, und zwar vor einer Kompromittierung

Angeleitete Reaktion

Abwehr selbst komplexer Cyberangriffe mit dem vorhandenen Personal

- Integrierte Schritt-für-Schritt-Anleitungen und Remote-Aktionen zur Unterbindung von Angriffen
- Vorfallreaktion mit Anleitung und Unterstützung durch zertifizierte Dienstleister
- Elevate to F-Secure: unsere einzig-artige Bedrohungsanalyse und Expertenunterstützung als Option

Automatisierte Reaktion

Reduzierung der Folgen gezielter Cyberangriffe durch automatisierte Reaktionen rund um die Uhr

- Automatische Gegenmaßnahmen auf der Grundlage von Kritikalität, Risikostufe und definiertem Zeitplan
- Priorisierung von Abwehrmaßnahmen auf der Basis von Kritikalität und Risikostufen
- Schnelle Eindämmung und Blockierung, auch außerhalb der Geschäftszeiten

Weitere Informationen finden Sie auf

f-secure.com/RDR

ÜBER F-SECURE

Niemand hat besseren Einblick in echte Cyberangriffe als F-Secure. Wir schließen die Lücke zwischen Erkennung und Reaktion. Wir nutzen dazu unübertroffene Bedrohungsinformationen von Hunderten der besten technischen Berater unserer Branche, von Millionen von Geräten, die unsere preisgekrönte Software nutzen, sowie fortlaufende Innovationen im Bereich maschinelles Lernen. Führende Banken, Fluggesellschaften und Unternehmen vertrauen auf unser Engagement bei der Bekämpfung der gefährlichsten Bedrohungen der Welt.

Zusammen mit unserem Netzwerk an Top-Channel-Partnern und über 200 Serviceanbietern ist es unsere Mission, all unseren Kunden maßgeschneiderte unternehmensfähige Cybersicherheit zur Verfügung zu stellen. F-Secure wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd gelistet.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure