DEM ANGREIFER IMMER EINEN SCHRITT VORAUS

F-Secure Rapid Detection & Response

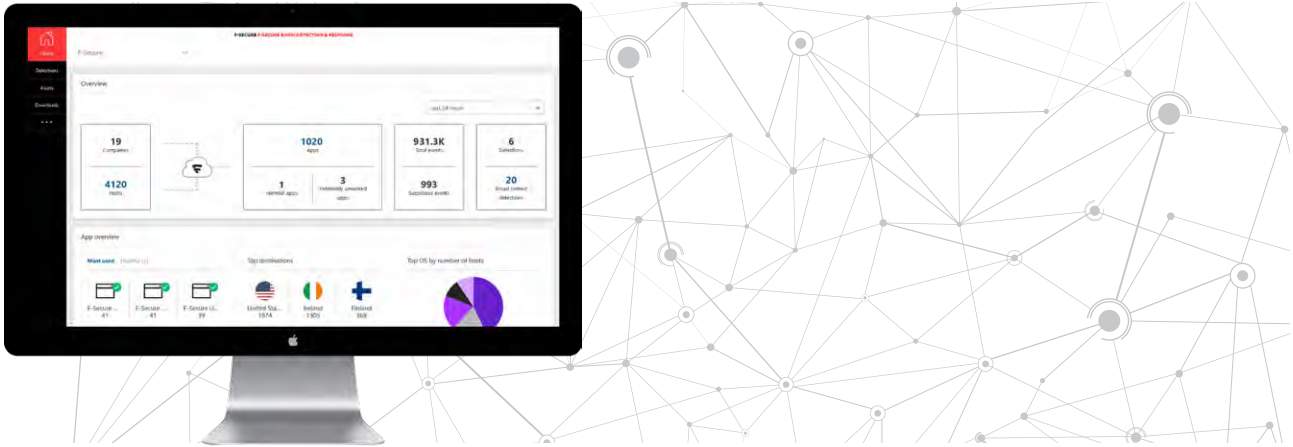
F-Secure

SCHÜTZEN SIE IHR UNTERNEHMEN VOR FORTSCHRITTLICHEN ANGRIFFEN

Effektiver Schutz, der Angriffe verhindert, ist der Kern aller Cybersicherheit. Unternehmen, die sich und ihre Daten gegen die Taktiken, Techniken und Methoden von Angreifern wappnen wollen, dürfen sich dennoch nicht allein auf Prävention verlassen.

Die sich ständig verändernde Bedrohungslandschaft und regulatorische Anforderungen wie die DSGVO machen es nötig, dass Unternehmen nach einem Angriff den getroffenen Punkt zuverlässig ermitteln können. Konkret muss dabei sichergestellt sein, dass das Unternehmen schnell auf Angriffe reagieren kann.

Die von einem erfahrenen Threat-Hunting-Team entwickelte und betreute Lösung F-Secure Rapid Detection & Response ermöglicht Ihrer eigenen IT-Abteilung oder einem zertifizierten Dienstleister den Schutz Ihrer Organisation vor komplexen Bedrohungen. Mit Unterstützung der erstklassigen Cybersecurity-Experten von F-Secure können Ihre IT-Spezialisten schnell und effektiv auf Sicherheitsvorfälle reagieren. Wenn Sie sich voll auf Ihr Kerngeschäft konzentrieren wollen, können Sie die Bedrohungssuche und -abwehr auch einem Dienstleister überlassen und dann im Angriffsfall auf die Unterstützung von Experten zurückgreifen.



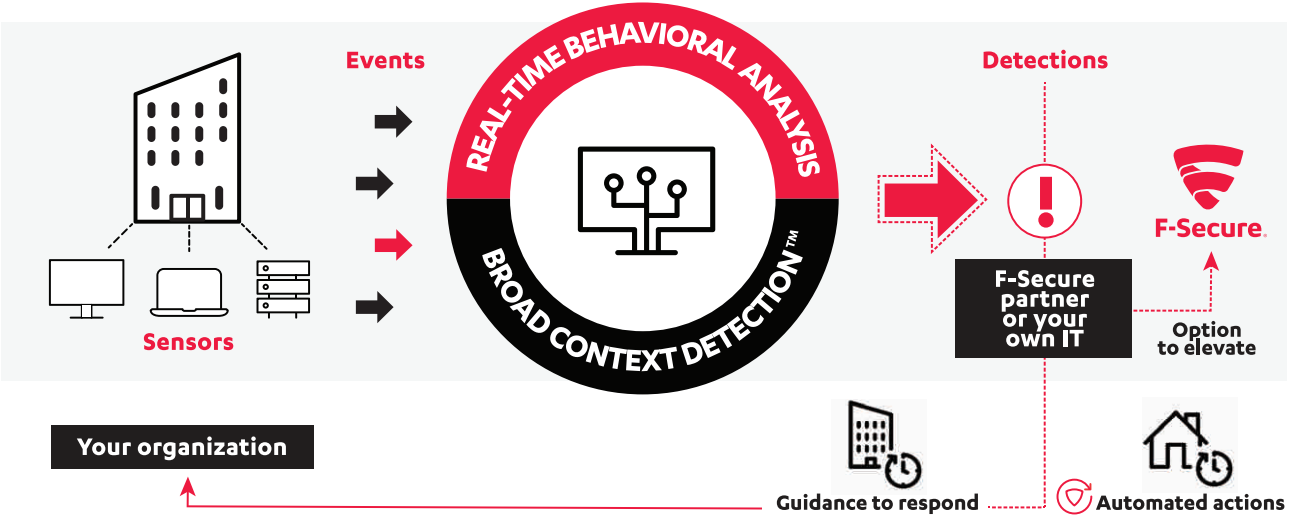
ATTACKEN MIT EXPERTENHILFE SCHNELL STOPPEN

Um Ihre Organisation vor komplexen Cyberbedrohungen zu schützen, brauchen Sie die beste Technologie sowie aktuelle und umfassende menschliche Expertise.

Die marktführende Lösung Endpoint Detection & Response (EDR) von F-Secure gibt Ihnen kontextuellen Einblick in komplexe Bedrohungen und ermöglicht Ihnen, automatisiert und mit Anleitung auf Angriffe zu reagieren.

Wenn sich ein Sicherheitsvorfall ereignet, brauchen Sie mehr als nur eine Warnung. Damit Sie bestmöglich reagieren können, müssen Sie die Struktur des Angriffs verstehen. Unsere Broad Context Detection™-Lösungen stoppen im Zusammenwirken mit zertifizierten Dienstleistern und integrierter Automatisierung Angriffe schnell und liefern konkrete Anleitungen zur Problemlösung.

FUNKTIONSWEISE



Führende F-Secure-Technologie für Ihre Sicherheit

1. Ressourcenschonende Sensoren überwachen die Endgeräte der Anwender und streamen auffällige Ereignis- und Verhaltensdaten in Echtzeit in unsere Cloud.

2. Unsere Datenanalysen und Broad Context Detection™-Verfahren grenzen die Daten ein und unterscheiden zuverlässig zwischen Schadverhalten und normalem Nutzerverhalten, um echte Angriffe schnell zu ermitteln.

3. Warnungen mit umfassender Kontextvisualisierung und Beschreibungen des Angriffs erleichtern die Erkennung durch den F-Secure-Partner oder Ihr eigenes IT-Team. Falls erforderlich, kann zusätzlich F-Secure den Vorfall umfassend analysieren.

4. Nach einer bestätigten Erkennung führt Sie die Lösung sicher durch die nötigen Schritte, mit denen Sie die Bedrohung eindämmen und beheben.

FUNKTIONSWEISE

DIE SUCHE NACH DER NADEL IM HEUHAUFEN – EIN REALBEISPIEL

Wollte man komplexe Bedrohungen aus der Unmenge von Einzelereignissen erkennen, die Angreifer auslösen, gliche das der Suche nach der Nadel im Heuhaufen.

In einer Kundeninstallation mit 325 Knoten meldeten unsere Sensoren in einem Monat etwa 500 Millionen Ereignisse. Durch die Rohdatenanalyse in unseren Backend-Systemen reduzierte sich diese Zahl auf 225.000.

Nach weiterer Analyse der verdächtigen Vorfälle durch unsere Broad Context Detection™-Lösung erfolgte eine Eingrenzung auf nur noch 24 Probleme. Diese wurden im Detail ausgewertet und nur 7 davon wurden letztendlich als echte Bedrohungen identifiziert.

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

500 MIO.
Sicherheitsvorfälle/Monat
Erfasst von 325 Sensoren auf Endgeräten

225.000
VERDÄCHTIGE VORFÄLLE
Nach Echtzeit-Verhaltensanalyse der Ereignisse

24
ERKENNUNGEN
Nach Analyse der Ereignisse in weiterem Kontext

7
ECHTE BEDROHUNGEN
Nach Bestätigung der Erkennungen als tatsächliche Bedrohungen

VORTEILE

TRANSPARENZ

Unmittelbare Transparenz bei IT-Umgebung und Sicherheitsstatus

- Die Inventarisierung von Anwendungen und Endgeräten sorgt für Transparenz bei IT-Umgebung und Sicherheitsstatus.
- Die Erfassung und Korrelierung von Verhaltensauffälligkeiten, die über übliche Malware hinausgehen, macht verdächtige Aktivitäten klar identifizierbar.
- Warnungen mit umfassendem Kontext und Informationen zur Asset-Gefährdung erleichtern die Vorfallreaktion

ERKENNUNG

Schutz Ihres Unternehmens und seiner Daten durch schnelle Erkennung

- Die schnelle Erkennung und Abwehr beschränkt Ausfallzeiten und Auswirkungen auf die Markenreputation auf ein Minimum.
- Die Lösung kann innerhalb von Stunden eingerichtet werden, sodass Sie sofort optimal vor Bedrohungen geschützt sind.
- Ihr Unternehmen erfüllt regulatorische Standards (PCI, HIPAA und DSGVO), die die Meldung von Sicherheitsvorfällen innerhalb von 72 Stunden erfordern.

REAKTION

Sofortreaktion auf Angriffe mit Anleitung und Automatisierung

- Automatisierung und Analyse ermöglichen es Ihrem Team, sich auf die tatsächlichen Bedrohungen zu konzentrieren.
- Warnmeldungen enthalten klare Anleitungen zur Vorfallreaktion, die Einrichtung rund um die Uhr aktiver automatisierter Reaktionen ist möglich.
- Ein zertifizierter und von F-Secure unterstützter Dienstleister bietet zusätzliche Expertise und erweiterte Ressourcen.

MERKMALE

Endgeräte-Sensoren

Ressourcenschonende und diskrete Monitoring-Tools, die mit jedem Endgeräteschutz funktionieren

- Sparsam arbeitende Sensoren für alle relevanten Computer in Ihrer Organisation
- Single-Client- und Management-Infrastruktur mit Endgeräteschutz von F-Secure
- Die Sensoren erfassen das Verhalten von Endgeräten, ohne die Privatsphäre der Nutzer zu verletzen

Broad Context Detection™

Die F-Secure-eigene Erkennungstechnologie erleichtert die Einschätzung gezielter Angriffe

- Verhaltens-, Reputations- und Big-Data-Analyse in Echtzeit mit maschinellem Lernen
- Automatische Einordnung von Erkennungen im Kontext auf einer Zeitleiste
- Einbeziehung von Risikoklassen, der Kritikalität des betroffenen Hosts und der relevanten Bedrohungslandschaft

Anwendungsanalyse

Transparenz bezüglich IT-Umgebung und Sicherheitsstatus ist damit einfacher denn je

- Ermittlung aller schädlichen und unerwünschten Anwendungen sowie der externen Adressen von Cloud-Services
- F-Secure-Reputationsdaten zur Identifizierung potenziell gefährlicher Anwendungen
- Blockierung von potenziell gefährlichem Code noch vor der Ausführung

Reaktion mit Anleitung

Ermöglicht die Abwehr selbst komplexester Cyberangriffe mit den verfügbaren Ressourcen

- Integrierte Schritt-für-Schritt-Anleitungen und Remote-Aktionen zur Abwehr von Angriffen
- Zertifizierte Dienstleister führen Sie durch die Maßnahmen bei der Reaktion auf Vorfälle
- Exklusive Bedrohungsanalyse (Elevate to F-Secure) und Expertenunterstützung

Automatisierte Reaktion

Reduzierung der Folgen von gezielten Cyberangriffen durch automatisierte Reaktion rund um die Uhr

- Automatische Gegenmaßnahmen auf Basis von Kritikalität, Risikoklasse und vordefiniertem Zeitplan
- Priorisierung der Abwehrmaßnahmen mit Einstufung nach Kritikalität und Risikoklasse
- Schnelle Abwehr, auch wenn Ihr Team nur während der Bürozeiten vor Ort ist

SEHEN SIE DAS VIDEO AUF
www.f-secure.com/RDR

ÜBER F-SECURE

DEM ANGREIFER IMMER EINEN SCHRITT VORAUS

Wie können Sie komplexe Angriffe erkennen? Indem Sie modernste Technologien und maschinelles Lernen nutzen. Aber das allein reicht noch nicht. Sie müssen darüber hinaus denken wie der Angreifer.

Die Experten von F-Secure waren an mehr Ermittlungen im Bereich Internetkriminalität in Europa beteiligt als jeder andere Anbieter von Sicherheitslösungen. Unsere Experten beobachten die Bedrohungslage genau und greifen auf aktuelle Informationen zu, um Ihre Sicherheit zu gewährleisten.

Niemand weiß mehr über Cybersicherheit als F-Secure. F-Secure sorgt seit drei Jahrzehnten für Innovationen im Bereich Cybersicherheit und schützt damit Zehntausende Unternehmen und Millionen Anwender. Mit unübertroffener Erfahrung in den Bereichen Endpoint Protection sowie Erkennung und Reaktion schützt F-Secure Unternehmen und Verbraucher vor Bedrohungen jeder Art – von fortschrittlichen Cyberangriffen und Datenschutzverletzungen bis hin zu umfassenden Ransomware-Infektionen. In der ausgefeilten Technologie von F-Secure vereinen sich die Stärken maschinellen Lernens mit den menschlichen Kompetenzen der weltweit anerkannten Sicherheitslabors zu einem einmaligen Ansatz: Live Security. Die Produkte von F-Secure werden von mehr als 200 Breitband- und Mobilfunkanbietern und Tausenden Vertriebspartnern weltweit verkauft. F-Secure wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd notiert.

F-Secure

www.f-secure.com
www.twitter.com/fsecure
www.facebook.com/f-secure