Elements EDR im Überblick

# WithSecure™ Elements **Endpoint Detection and Response**

**WithSecure™ Elements –**
**Weniger Cyberrisiko, Komplexität und Ineffizienz.**

# Inhalt





Stand: Mai 2021

# 1. Kurzfassung

Gezielte Angriffe auf die Cybersicherheit sind schwer zu analysieren und zu bekämpfen. Für Unternehmen stellen sie ein äußerst kostspieliges Problem dar, schon bevor sie sich zu tatsächlichen Datenpannen entwickeln. Allein die Abhilfemaßnahmen für einen Angriff können über zwei Monate dauern und fast zwei Millionen Euro kosten.[1] „Fileless Attacks" werden von herkömmlichen Virenschutzprogrammen kaum erkannt, und gezielte Angriffe bleiben oft über Monate oder gar Jahre unbemerkt.[2] Mit WithSecure™ Elements Endpoint Detection and Response gewinnen Sie einen kontextbezogenen Einblick zu Ihrer Sicherheit, automatisieren die Erkennung von Bedrohungen und stoppen Angriffe, bevor es zu Datenpannen kommt, bei denen sensible, vertrauliche oder anderweitig geschützte Daten in die Hände von Unbefugten, z. B. Cyberkriminellen, gelangen.

## Flexibilität beim Aufbau resilienter Cybersicherheit mit WithSecure™ Elements

In unserer agilen Geschäftswelt ist Wandel die einzige Konstante. WithSecure™ Elements bietet Unternehmen All-in-One-Sicherheit, die sich an Veränderungen im Unternehmen und in der Bedrohungslandschaft anpasst und mit dem Unternehmen mitwächst. Es bietet Flexibilität bei Lizenzierungsmodellen wie bei der Auswahl von Sicherheitstechnologien. WithSecure™ Elements integriert eine Reihe von Cybersicherheitskomponenten wie Schwachstellenmanagement, Patch-Management, Endgerätesicherheit sowie Detection and Response in einem einzigen, schlanken Softwarepaket, verwaltet über eine einheitliche, Cloud-basierte Managementkonsole, mit der sich auch die Sicherheit der Microsoft 365 Collaboration Services verwalten lässt. Die Lösung ist als komplett verwalteter Abonnement-Service über unsere zertifizierten Partner oder als selbstverwaltete Cloud-Service-Lösung erhältlich. Kunden können leicht von selbstverwalteten zu komplett verwalteten Services wechseln. Wenn also Unternehmen nur schwer Personal mit Cybersicherheitskenntnissen finden, bleiben sie trotz ständig wechselnder Angriffsmethoden geschützt.

WithSecure™ Elements umfasst vier Lösungen, die alle über eine Konsole, das WithSecure™ Elements Security Center, verwaltet werden.

### WithSecure™ Elements Endpoint Protection:

Der Cloud-native, KI-gestützte Endgeräteschutz von WithSecure™ ist mehrfacher AV-TEST Best Protection-Gewinner. Er lässt sich sofort vom Browser aus einsetzen und verwaltet die Sicherheit all Ihrer Endgeräte, so dass Ihr Unternehmen vor Angriffen geschützt ist. WithSecure™ Elements Endpoint Protection schützt Handys, Desktops, Laptops und Server.

### WithSecure™ Elements Endpoint Detection and Response:

Gewinnen Sie vollen Einblick in neuartige Bedrohungen mit unserer Endpoint Detection and Response. Die einzigartige Broad Context Detection reduziert Alarmrauschen auf ein Minimum – Sie fokussieren sich auf echte Zwischenfälle. Mit der automatisierten Reaktion stoppen Sie effektiv rund um die Uhr Angriffe. WithSecure™ Elements Endpoint Detection and Response schützt Desktops, Laptops und Server.

### WithSecure™ Elements Vulnerability Management:

Erkennen und behandeln Sie kritische Schwachstellen in Ihren Netzen und Anlagen. Durch das Aufdecken, Priorisieren und automatische Patchen von Schwachstellen reduzieren Sie Ihre Angriffsflächen und Einfallspunkte für Angreifer.

### WithSecure™ Elements Collaboration Protection:

Ergänzen Sie die nativen E-Mail-Sicherheitsfunktionen von Microsoft 365 durch hochentwickelte Sicherheitfunktionen gegen Angriffe über E-Mails und URLs. Durch die Cloud-to-Cloud-Integration lässt sich die Lösung einfach bereitstellen und verwalten.

WithSecure™ Elements Endpoint Protection, Endpoint Detection and Response und Vulnerability Management kommen in einem einzigen, automatisch aktualisierten Softwarepaket. Das spart Ihnen Zeit und Geld bei Softwarebereitstellung und -verwaltung.

## Die Vorteile der integrierten Lösungen

Die modulare Lösung WithSecure™ Elements lässt sich an veränderte Bedarfe Ihres Unternehmens anpassen. Einheitliche Cybersicherheit heißt einfachere Lizenzierung, weniger Sicherheitsverwaltung und mehr Produktivität – ohne Beeinträchtigung Ihrer Cybersicherheitslage. Die Cloud-basierte Konsole - WithSecure™ Elements Security Center - bietet zentrale Transparenz, Einblicke sowie Verwaltung für alle Endgeräte und Cloud-Services. Sie wird komplett von einem unserer zertifizierten Managed Service Provider verwaltet oder kann bei Bedarf mit Unterstützung von WithSecure™ selbst verwaltet werden.

[1] Der Ponemon Institute Cost of a Data Breach Report von 2018 gibt an, dass die Zeit bis zur Feststellung von Datenpannen je nach Branche zwischen 150 und 287 Tagen liegt und allein für die Maßnahmen nach der Datenpanne im Schnitt 1,76 Millionen Dollar Kosten in 69 Tagen entstand.
[2] Dem Ponemon Institute Cost of a Data Breach Report von 2020 zufolge dauert es im Schnitt 280 Tage, bis eine Datenpanne erkannt und behoben ist.

Alle Endgeräte-Lösungen (Elements Endpoint Protection, Endpoint Detection and Response und Vulnerability Management) verwenden einen einzigen Software-Agenten, den Sie nur einmal zu installieren brauchen. Die Add-on-Lösungen können Sie dann auch später noch aktivieren, ohne zusätzliche Lösungen installieren zu müssen. WithSecure™ Elements Collaboration Protection ist eine Cloud-basierte Lösung, die keine Installation auf den Endgeräten Ihres Unternehmens erfordert.

Zusätzlich zu den Vorteilen bei der Bereitstellung und Verwaltung sind die WithSecure™ Elements-Lösungen auf Zusammenarbeit ausgelegt, um die sicherheitsbezogenen Verbesserungen für das Unternehmen zu maximieren. Durch die Verbindung von Sicherheitsereignissen und -warnungen bieten die XDR-Funktionen von WithSecure™ Elements eine ganzheitliche Sicherheit, die die Silos isolierter Lösungen aufbricht.

## WithSecure™ Elements

| | Endpoint Protection Standard | Endpoint Protection Premium | Detection and Response | Vulnerability Management | Microsoft 365 Protection |
|---|---|---|---|---|---|
| **Erweitertes Anti-Malware- und Patch-Management** | ✓ | ✓ | | | |
| **Anti-Ransomware mit Dataguard- und Anwendungskontrolle** | | ✓ | | | |
| **Erweiterter Bedrohungsschutz** | | | ✓ | | |
| **Schwachstellen-Management und Priorisierung** | | | | ✓ | |
| **Erweiterte E-Mail-Sicherheit für Microsoft 365** | | | | | ✓ |

Hinweis: Die verfügbaren Funktionen können je nach Betriebsplattform variieren.

## Zur Einführung: WithSecure™ Elements Endpoint Detection and Response

WithSecure™ Elements Endpoint Detection and Response ist eine marktführende kontextbasierte Lösung für Endpoint Detection and Response (EDR). Sie hilft Unternehmen, sofortige Transparenz über ihre IT-Umgebung und ihren Sicherheitsstatus zu erlangen sowie das Unternehmen und seine sensiblen Daten zu schützen, da sie Angriffe schnell erkennt und mit fachkundiger Betreuung schnell darauf reagiert.
Die WithSecure-Lösung verfügt über tiefgehende bidirektionale Intelligenz und einen hohen Automatisierungsgrad und schützt vor neuartigen Bedrohungen, noch bevor es zu Sicherheitsverletzungen kommt. Sie erkennt Zwischenfälle mit kompakten Clients, die auf überwachten Hosts im gesamten Unternehmensnetzwerk installiert werden. Diese sammeln Daten über verhaltensbezogene Ereignisse wie Dateizugriffe, gestartete Prozesse, neue Netzwerkverbindungen oder Einträge in der Registry bzw. den Systemprotokollen. Diese Ereignisse werden dann von der Lösung weiter analysiert. Zusätzlich zu den Echtzeit-Erkennungen führt die Lösung auch Erkennungen auf der Grundlage historischer Daten durch.

Die Lösung wird speziell durch WithSecure™ unterstützt, d. h. eine Erkennung kann zur weiteren Bedrohungsanalyse durch erfahrene Cybersicherheitsexperten an WithSecure™ weitergeleitet werden.

Die Lösung gibt es auch als von Partnern verwalteten EDR-Service, der Technologie, Bedrohungsdaten und Partner-Services kombiniert, um einen All-in-One-Service für die Detection and Response bei Sicherheitsverletzungen anzubieten. Die verwalteten EDR-Services entlasten die eigenen Ressourcen eines Unternehmens von der Überwachung neuartiger Bedrohungen sowie vom Management von Zwischenfällen und alarmieren das Unternehmen nur bei echten Bedrohungen.

Der Einsatz von Spitzentechnologie ist aber nur eine Seite der Medaille, denn die Technologie ist nur so gut wie die Menschen dahinter. Unsere Threat Hunters und Forscher gehören zu den führenden Experten der Branche. Sie engagieren sich unermüdlich dafür, das Beste auf dem Markt für Cybersicherheit zu bieten. Bei WithSecure™ kombinieren wir diese Technologie mit dem unübertroffenen Fachwissen unserer Mitarbeiter, um eine erstklassige Lösung für Endpoint Detection and Response bereitzustellen.

### Prävention macht Angreifern das Leben schwer

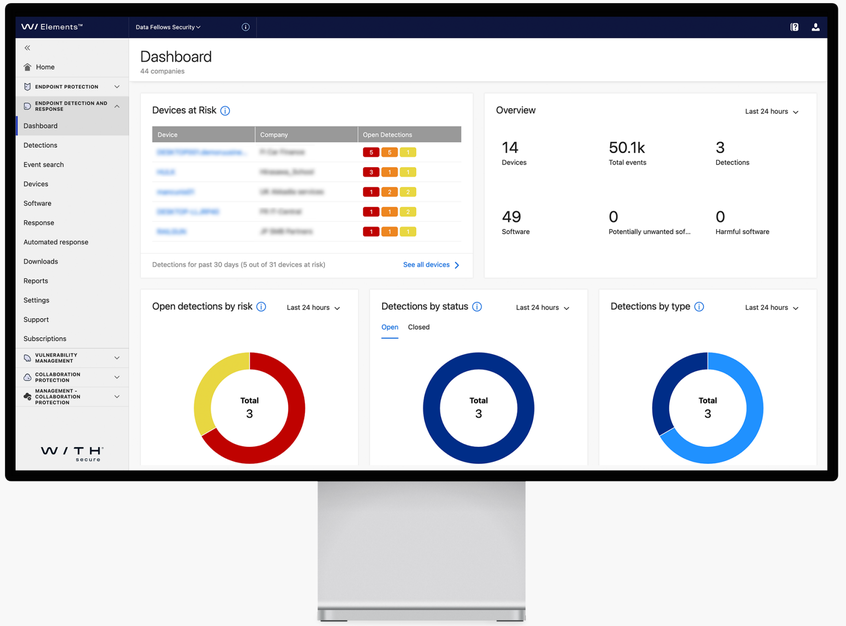
Geschickte Angreifer haben zwar die nötigen Fähigkeiten, um in Ihr Netzwerk einzudringen, aber man muss ihnen ja nicht auch noch einen roten Teppich ausrollen. Wenn Sie in die Prävention von Schwachstellen investieren, machen Sie diesen Angreifern ihr Geschäft immerhin etwas schwerer, denn ein Mehraufwand bei Angriffen wirkt durchaus abschreckend.

WithSecure™ Elements Endpoint Detection and Response als Post-Compromise-Lösung zur Erkennung neuartiger Angriffe benötigt zum Schutz von Endgeräten aber immer noch eine starke Lösung, die Standardbedrohungen wie Ransomware blockiert.

# 2. Die entscheidenden Vorteile

Mit WithSecure™ Elements Endpoint Detection and Response erkennen Sie neuartige Bedrohungen und gezielte Angriffe mit Fileless-Techniken, bevor es zu Datenverletzungen kommt, und mithilfe der hochmodernen Technologie von WithSecure™ können Sie diese immer schnell analysieren und darauf re-agieren.

Einige der zentralen Vorteile der Lösung für Transparenz, Erkennung und Reaktion findes Sie im Folgenden:




## Sofortiger kontextbezogener Einblick in Ihre IT-Umgebung und Ihren Sicherheitsstatus

- Verbessern Sie Ihren Überblick über Status und Sicherheit der IT-Umgebung mit Anwendungs- und Endgeräte-Inventaren.
- Unterscheiden Sie leicht Missbrauch und korrekte Nutzung, indem Sie über Malware hinausgehendes Verhalten sammeln und abgleichen.
- Reagieren Sie schneller auf identifizierte gezielte Angriffe mithilfe von Warn-meldungen mit breitem Kontext und Hostkritikalität.

## Schützen Sie Ihr Unternehmen und seine sensiblen Daten durch schnelle Erkennung von Sicherheitsverletzungen

- Erkennen und stoppen Sie gezielte Angriffe schnell, um Betriebsunterbrechungen und Rufschädigungen Ihres Unternehmens zu vermeiden.
- Bereiten Sie sich frühzeitig auf Angriffe vor, indem Sie binnen weniger Tage modernisierte Funktionen zur Detection and Response einrichten.
- Identifizieren Sie Bedrohungen oder Anzeichen von Angriffen, die auf einem Endgerät durchgeführt wurden und noch im Speicher aktiv sind, wenn die EDR-Funktionalität aktiviert wird.
- Erfüllen Sie die regulatorischen Anforderungen von PCI, HIPAA und der DSGVO der EU, wonach Sie Datenschutzverletzungen binnen 72 Stunden melden müssen.

## Reagieren Sie bei Angriffen schnell mit Automatisierung und Unterstützung, oder nutzen Sie die vollständigen Daten von Zwischenfällen für Ihre eigenen SOC-Untersuchungen.

- Optimieren Sie die Arbeit Ihres Teams durch integrierte Automatisierung und Erkenntnisse, die eine rasche Reaktion auf neuartige Bedrohungen und gezielte Angriffe ermöglichen.
- Sie erhalten bei Warnmeldungen eine Handlungsanleitung, können rund um die Uhr Reaktionsmaßnahmen automatisieren (Automatisierungsfunktionen werden in einem Update eingeführt).
- Überwinden Sie Defizite bei Know-how und Ressourcen Ihres Teams, indem Sie die hochentwickelte Überwachung von Bedrohungen an einen WithSecure™-zertifizierten Managed Service Provider auslagern, der von WithSecure™-Experten unterstützt wird. Alternativ können Kunden oder Partner mit Threat-Hunting-Fähigkeiten über WithSecure™ Elements for Endpoint Detection and Response die gesamten Rohdaten der Zwischenfälle mit dem zusätzlichen Service Event Search for Threat Hunting bereitstellen.

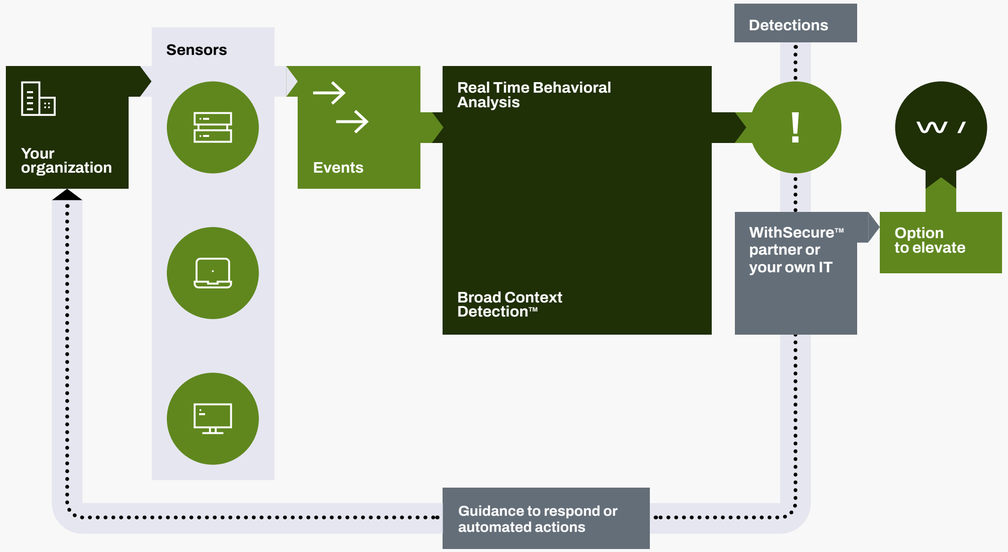
## Die passende Lösung für Ihre Fähigkeiten und Ressourcen bei der Cybersicherheit

WithSecure™ Elements Endpoint Detection and Response steht Ihnen in verschiedenen Varianten je nach Ihren Fähigkeiten und Ressourcen im Bereich Cybersicherheit zur Verfügung:

1. **Vollständig verwalteter Dienst durch Partner von WithSecure™:** Diese Option empfiehlt sich für Unternehmen, die gegen neuartige gezielte Bedrohungen geschützt sein wollen, aber die Strategie verfolgen, ihre Cybersicherheit auszulagern.
2. **Interne Verwaltung mit Hilfe von WithSecure™ bei Zwischenfällen:** Diese Option ist ideal für Unternehmen mit begrenzten Cybersicherheitskenntnissen, die komplexe Zwischenfälle über die integrierte WithSecureTM Elevate-Funktion an WithSecure™ weiterleiten können.
3. **Intern verwaltet:** Diese Option passt zu Unternehmen, deren IT-Abteilung über gute Kenntnisse im Bereich Cybersicherheit verfügt. Der normale Ablauf der Incident Response umfasst die Erkennung von Zwischenfällen mit Hilfe von Broad Context Detection und die Reaktion auf diese Bedrohungen.
4. **Intern verwaltet bei professionellen Threat-Hunting-Fähigkeiten:** Diese Option eignet sich für Unternehmen mit eigenem Security Operations Center (SOC), die im Rahmen ihrer Untersuchungen selbst modernstes Threat Hunting durchführen können.

# 3. Die Lösung im Überblick

Elements Endpoint Detection and Response von WithSecure™ besteht aus einer Kombination einfach zu implementierender Clients auf Hosts, einem Cloud-basierten Elements Security Center und optionalen zertifizierten verwalteten Diensten für Partner. Die Lösung bietet Funktionen zur Erkennung neuartiger Bedrohungen und gezielter Angriffe sowie Broad Context Detection zur Abschätzung des Gesamtrisikos und entsprechender Maßnahmen. Der lokale Teil der Bereitstellung umfasst einen Client zur Überwachung und Reaktion an Endgeräten, der auf den Endgeräten des Unternehmens installiert wird.




Die Abbildung beschreibt in Grundzügen, wie WithSecure™ Elements Endpoint Detection and Response funktioniert:

1. **Einfache Clients** überwachen diverse Aktivitäten von Angreifern auf Endgeräten und streamen Verhaltensereignisse in Echtzeit an unsere Cloud.
2. **Echtzeit-Verhaltensdatenanalysen** markieren und verfolgen Prozesse und anderes Verhalten, das die Ereignisse ausgelöst hat.
3. **Broad Context Detection™-Verfahren** grenzen die Daten weiter ein, indem sie verknüpfte Ereignisse in einen Kontext stellen, echte Angriffe schnell identifizieren und sie nach Risikostufe, Kritikalität des Hosts und der vorherrschenden Bedrohungslage priorisieren.
4. **Nach einer bestätigten Entdeckung leitet die Lösung** IT- und Sicherheitsteams durch die nötigen Schritte zur Eindämmung und Beseitigung der Bedrohung.

## 3.1 Das Elements Security Center: Ihr Management Portal

Elements Endpoint Detection and Response (EDR) erleichtert die Bereitstellung, Verwaltung und Überwachung neuartiger Bedrohungen auf Ihren Endgeräten über eine einzige, intuitive, webbasierte Konsole. Die Lösung vermittelt Ihnen unmittelbare kontextbezogene Einblicke in die IT-Umgebung und den Sicherheitsstatus in Ihrem gesamten Netzwerk – selbst dann, wenn Ihr Personal nicht im Haus ist.

Das Management Portal wurde entwickelt, um die Sicherheitsverwaltung in anspruchsvollen und standortübergreifenden Umgebungen einfacher und schneller zu gestalten.

Im Folgenden finden Sie einige Beispiele für die deutliche Reduzierung des Zeit- und Ressourcenaufwands bei der hochentwickelten Überwachung und Verwaltung von Bedrohungen durch die Lösung:

- Die Elements EDR ist so konzipiert, dass sie mit jeder Lösung zum Schutz von Endgeräten zusammenarbeitet und mit den WithSecure™-Lösungen für Endgerätesicherheit in einer einzigen Client- und Management-Infrastruktur funktioniert.
- In Kombination mit WithSecure™ Elements EDR werden Malware und neuartige Bedrohungen sichtbar und kontrollierbar.
- Die Erkennungen erhalten Sie mit einer anschaulichen Visualisierung, die einen weiten Überblick zu gezielten Angriffen auf einer Zeitachse bietet – mit allen betroffenen Hosts, relevanten Ereignissen und empfohlenen Maßnahmen.
- Durch die Konsolidierung des hochentwickelten Bedrohungsmanagements von Endgeräten und Systemtools in einem einzigen Sicherheitsportal für Endgeräte wird die gesamte Verwaltung erheblich rationalisiert, und der Zeitaufwand sinkt.
- Sie brauchen hier keine Server-Hardware oder -Software zu installieren oder zu warten. Da es sich um einen Cloud-basierten Dienst handelt, der von WithSecure™ verwaltet wird, ist alles, was Sie benötigen, ein Browser und eine Internetverbindung.

Das Management Portal unterstützt die neuesten Versionen der gängigen Browser: Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome und Safari.

Das Management Portal ist auf Deutsch, Englisch, Finnisch, Französisch, Italienisch, Japanisch, Polnisch, Portugiesisch, Schwedisch und Spanisch (Lateinamerika) verfügbar.

**Die Partner Managed-Version** des Management Portals enthält speziell entwickelte Funktionen zur Unterstützung von Service Providern, z. B. Endkunden-Reporting, ein Dashboard mit komfortablem Überblick zu allen verwalteten Unternehmen und außerdem Zugriff auf das eigene Dashboard jedes verwalteten Unternehmens.

## 3.2 Endpoint Clients

Endpoint Clients sind einfache und diskrete Überwachungstools. Sie dienen der Erkennung von Anomalien, einschließlich neuer, bisher nicht identifizierter Ereignisse oder einer Abfolge von Ereignissen, die sehr wahrscheinlich auf schädliche Aktivitäten zurückzuführen sind.

Die Clients lassen sich auf allen relevanten Windows- und MacOS-Computern im Unternehmen einsetzen und sammeln von dort verhaltensbezogene Ereignisdaten. Sie sind für den Einsatz mit jeder Endgerätesicherheitslösung konzipiert und funktionieren nahtlos mit den Sicherheitslösungen für Endgeräte von WithSecure in einer Mandanten- und Cloud-basierten Verwaltungsinfrastruktur.

Die Tabelle zeigt die unterstützten Betriebssysteme und deren einzelne Funktionen.

### WithSecure™ Elements

| | Windows Workstations | Windows Server | MacOS | Linux |
|---|---|---|---|---|
| **Betriebssysteme** | 7 / 8 / 10 | 2019 / 2016 / 2012 /2011 / 2008 R2 | 10.12 oder neuer | |
| **Single-Client bei WithSecure™** | Ja | Ja | Ja | Ja |
| **Verhaltensbezogene Ereignisse** | Ja | Ja | Ja | Ja |
| **Application Visibility** | Ja | Ja | Nein* | Nein* |
| **Remote Host Isolation** | Ja | Ja | Ja | Ja |

*** Bereitstellung später: Die Funktion ist noch nicht verfügbar.**

**Weitere Informationen** über die Systemanforderungen und die Client-Bereitstellung im Benutzerhandbuch unter https://help.f-secure.com/product.html#business/edr/latest/de/deployment-latest-de

## 3.3 Application Visibility

Ein umfassender Einblick in Ihre IT-Umgebung und die Cloud-Services reduziert die Anfälligkeit für neuartige Bedrohungen und Datenlecks. Mit der Application Visibility unserer Lösung erhalten Sie eine Liste aller aktiven Anwendungen, die auf Endgeräten im gesamten Netzwerk Ihres Unternehmens ausgeführt werden. So können Sie unerwünschte, unbekannte und schädliche Anwendungen leicht auffinden.

Mit der Application Visibility können Sie potenziell unerwünschte Anwendungen (PUA) und unerwünschte Anwendungen (UA) identifizieren. "Potentially Unwanted Applications" weisen Verhaltensweisen oder Eigenschaften auf, die Sie als störend oder unerwünscht einstufen könnten. "Unwanted Applications" weisen Verhaltensweisen oder Eigenschaften mit gravierenderen Auswirkungen auf Ihr Gerät oder Ihre Daten auf.

### Als "Potentially Unwanted" (PUA) identifizierte Anwendungen können ...

- Ihre Privatsphäre oder Produktivität beeinträchtigen - zum Beispiel durch die Preisgabe persönlicher Daten oder durch unbefugte Handlungen;
- die Ressourcen Ihres Geräts übermäßig belasten, z. B. durch übermäßigen Gebrauch von Speicherplatz oder Arbeitsspeicher;
- die Sicherheit Ihres Geräts oder der dort gespeicherten Informationen gefährden, z. B. durch unerwartete Inhalte oder Anwendungen.

Die Auswirkungen dieser Verhaltensweisen und Merkmale auf Ihr Gerät oder Ihre Daten können geringfügig bis gravierend sein. Sie sind jedoch nicht so schädlich, dass die Anwendung als Malware eingestuft werden müsste.

### Sammlung von Ereignisdaten zur Erkennung und Eindämmung von Bedrohungen

WithSecure™ Elements Endpoint Detection and Response sammelt Daten von zahlreichen Endgeräten, um Bedrohungen in Ihrer Umgebung zu erkennen und einzudämmen. Diese Daten werden über drei verschiedene Kanäle bereitgestellt:

1. **Broad Context Detection™.** Diese automatisierte Methode zur Identifizierung von Bedrohungen wurde entwickelt, um in der riesigen Menge von Verhaltensdaten, aus Endgeräten des Unternehmens die echten Bedrohungen zu identifizieren. Darüber hinaus können Sie mit der integrierten WithSecure™ Elevate-Funktion professionelle Unterstützung von unseren spezialisierten Experten für Cybersicherheit anfordern, um hartnäckige Fälle zu lösen.
2. **Event Search**. Mit dieser integrierten Funktion können Sie die aus den Endgeräten Ihres Unternehmens gesammelten Ereignisdaten, die mit Broad Context Detection in Zusammenhang stehen, anzeigen, durchsuchen und untersuchen.
3. **Event Search for Threat Hunting**. Mit dieser hochentwickelten Funktion können Sie alle von den Endgeräten gesammelten Ereignis-Rohdaten untersuchen und mit ihnen interagieren. Dank ausgefeilter Filterfunktionen können Ihre Cyber-Sicherheitsexperten im SOC ein proaktives Threat Hunting durchführen, um auch die raffiniertesten versteckten Bedrohungen zu erkennen und zu stoppen. Event Search for Threat Hunting ist eine optionale Komponente von WithSecure™ Elements Endpoint Detection and Response.

## 3.4 Analyse von Verhaltensdaten

Diese Kernfunktion dient zur Identifikation neuartiger Bedrohungen in sehr großen Mengen von Verhaltensdaten, um verdächtige Ereignisse oder eine Abfolge von Ereignissen zu erkennen, die zuvor noch nicht beobachtet wurden und sehr wahrscheinlich schädlich sind.

WithSecure™ nutzt Echtzeit-Verhaltens-, Reputations- und Big-Data-Analysen mit maschinellem Lernen, um mehrere verdächtige Ereignisse zu sammeln, die – z. B. anhand von Aktivitäten – miteinander verknüpft werden können. Die Verhaltensanalyse nutzt KI, um schädliche, versteckte Aktivitäten auf Basis kleiner Einzelereignisse zu erkennen, die als Teil der Taktiken, Techniken und Verfahren des Angreifers ausgeführt werden. Die Verhaltensanalyse wird bei der automatischen Identifizierung von Host-Profilen verwendet, die sich auf die Risikoeinstufung von Erkennungen in Bezug auf das überwachte Unternehmen und den Host sowie auf die gesamte IT-Umgebung auswirken.

Die KI umfasst maschinelle Lernfunktionen, die zur kontinuierlichen Verbesserung der Erkennung und zur Verringerung von Fehlalarmen eingesetzt werden. Die Verhaltensanalyse ist ein Musterbeispiel für die Kombination von Datenwissenschaft und Cybersicherheitsexpertise. Diesen Ansatz bezeichnet WithSecure™ als "Mensch und Maschine".

## 3.5 Broad Context Detection™

Die von WithSecure entwickelten Broad Context Detection™-Methoden grenzen die Anzahl der Erkennungen systematisch auf nur wenige signifikante Zwischenfälle ein, die auf System- oder Datenmissbrauch hindeuten könnten.

Broad Context Detection™ markiert Hinweise auf mögliche Verstöße durch Warnung der Administratoren vor Taktiken, Techniken und Verfahren (TTPs bei gezielten Angriffen, z. B. bei folgenden potentiell verdächtigen Aktionen:

- auffällige Aktivität von Standardprogrammen
- Aufrufe laufender Prozesse aus nicht standardisierten ausführbaren Dateien
- Ausführung unerwarteter Skripte
- unerwartetes Ausführen von Systemtools aus Standardprozessen

Broad Context Detection™ meldet nur relevante Erkennungen und ordnet ihnen eine Kritikalität anhand der Risikostufe, der Information über die Kritikalität der betroffenen Hosts und der aktuellen Bedrohungslage zu. Ein Einzelereignis muss noch kein Angriff sein, doch wenn in kurzer Zeit mehrere Erkennungen auftreten, kann dies zu einem höheren Risikograd und damit einer Broad Context Detection™ als Warnung vor einem möglichen Zwischenfall führen.

**Durch diesen Ansatz erhalten IT-Teams eine relativ kurze Liste von Erkennungen mit klaren Prioritätsstufen und empfohlenen Maßnahmen. So wissen die Teams, worauf sie sich zuerst konzentrieren und wie sie reagieren müssen und können dies schnell und gezielt tun.**

## 3.6 Incident Management

Die Lösung verfügt über eine integrierte Funktion zum Incident Management für die Anzeige und Verwaltung von Broad Context Detections. Neue Erkennungen erzeugen eine E-Mail-Warnung mit direktem Zugriff auf das Management Portal, um Details anzuzeigen und Maßnahmen zu ergreifen..

Das benutzerfreundliche Dashboard listet die Broad Context Detections auf und hilft, Zwischenfälle auf Basis ihrer Risikobewertung zu priorisieren, die automatisch über Kritikalität und Konfidenzniveau berechnet wird. Auch unkritische Broad Context Detections mit niedrigen Risikowerten werden aufgelistet, da langsam laufende Angriffe sich letztlich zu ernsteren Zwischenfällen mit hohen Risikowerten entwickeln können.

Beim Incident Management werden Broad Context Detections bestätigt oder als in Bearbeitung, überwacht, bestätigt abgeschlossen, falsch positiv oder unbestätigt abgeschlossen markiert. Wenn Sie eine Broad Context Detection als falsch positiv markieren, werden zukünftige Erkennungen desselben Typs automatisch geschlossen, Prozessparameter lauten dann "Auto false positive".

## 3.7 Response-Anleitung

Nach einer bestätigten Erkennung hilft die integrierte Anleitungsfunktion der Lösung Ihnen dabei, die nötigen Schritte zur Eindämmung und Beseitigung der Bedrohung zu ergreifen. Dazu gehören unter anderem empfohlene Maßnahmen wie eine Information der Benutzer und die Isolierung von Hosts.

Die Experten für Cybersicherheit von WithSecure™ haben anhand eigener Erfahrungen eine Reihe von verbreiteten Bedrohungen analysiert, um die Lösung zu trainieren. Dadurch kann das Tool leicht verständliche Response-Anleitungen für eine Vielzahl neuartiger Bedrohungen und entsprechende Hinweise zur Vorgehensweise liefern. Die Response-Anleitungen erleichtern es auch weniger erfahrenen Mitgliedern von IT- und Sicherheitsteams, die richtigen Maßnahmen zur Eindämmung und Behebung der Bedrohung zu ergreifen.

### Die folgende Liste zeigt Beispiele für Aktivitäten, die eine Erkennung auslösen.

Die Liste enthält nicht bloß bekannte Angriffsarten, da die Erkennungsdaten kontinuierlich analysiert werden und laufend weitere Angriffsarten durch die Methoden der Broad Context Detection™ und durch die Threat Hunter von WithSecure identifiziert werden.

- **Gezielter Angriff,** der sich auf einen Host richtet
- **Lateral movement** – schließt Bewegungen zwischen Hosts ein
- **Spoofing** schließt Informationen als Teil des Angriffs ein
- **Persistenz** – z. B. durch Verwendung eines Prozesses auf demselben Host
- **Privilege Escalation** - z. B. durch Erzwingen von Administratorrechten
- **Zugang zu Anmeldedaten:** Zugang und Kontrolle über bestimmte Geräte/Netzwerke
- **Exfiltration** hilft dem Angreifer, Informationen aus dem Zielgerät/Netzwerk zu exfiltrieren
- **Anormale Prozessausführung,** z. B. mit verdächtigen Parametern
- **Anormaler Dateizugriff,** z. B. auf mehrere Dateitypen oder auf Systemdateien ohne Root-Zugriff
- **Client-Manipulation:** z. B. Versuche, Client-Einstellungen zu ändern oder den Client zu deaktivieren
- **Injektionsversuche** an anderen Prozessen, z. B. dem Kernel-Modus oder einer anderen Anwendung
- **Verbindung zum Befehls- und Kontrollnetz,** für einen remote Host geöffnet
- **PowerShell-Skript vom Standort des Angreifers,** als untypischer Ort zum Laden eines Skripts markiert
- **PowerShell hat ein PowerShell-Skript geändert:** typischerweise Teil des Erreichens von Persistenz
- **Anormale DLL-Nutzung mit PowerShell,** von einem Prozess aus genutzt, der das Modul geladen hat
- **Remote-Verbindung und -Ausführung,** potenziell für die laterale Bewegung verwendet

## 3.8 Elevate to WithSecure™

WithSecure™ bietet einen optionalen Service zur Bedrohungsanalyse für den Fall, dass eine Erkennung weitere Bedrohungsanalysen und Beratung durch die Cybersicherheitsexperten von WithSecure erfordert. "Elevate to WithSecure™" ist ein Premium-Service, bei dem Eskalationen im Voraus für eine Reihe von zu analysierenden Fällen bestellt werden müssen.

Die Anfragen seitens Elevate to WithSecure™ über die Lösung gewähren den Bedrohungsanalysten von WithSecure™ die Erlaubnis, auf sämtliche Metadaten zuzugreifen, die von den installierten Clients rund um eine bestimmte Erkennung gesammelt wurden.

Die Bedrohungsanalysten von WithSecure sind im Schichtdienst tätig und nehmen die Anfrage innerhalb des 2-Stunden-Ziel-SLA auf. Sie beginnen mit der Identifizierung der Art des potenziellen Zwischenfalls, indem sie zusätzliche Belege sammeln und mithilfe der Lösung weitere fachkundige Anleitungen zur Validierung der Bedrohung bereitstellen.Optional kann auch eine Untersuchung der Bedrohung durchgeführt werden.

- Die Bedrohungsvalidierung liefert zusätzliche Informationen über eine Broad Context Detection™ aus den letzten 7 Tagen. Dazu gehören eine von Experten erstellte Zusammenfassung und Beschreibung der Erkennung sowie weitere relevante Daten, anhand derer Sie feststellen können, ob Response-Maßnahmen erforderlich sind.

- Threat Investigation bietet eine sehr detaillierte Untersuchung zu einer speziellen Broad Context Detection™, wobei alle aktuellen und historischen Daten genutzt werden. Diese Option umfasst auch eine Response-Anleitung für Zwischenfälle von unseren Cybersicherheitsexperten und einen detaillierten Bericht zum erkannten Angriffstyp.

Elevate to WithSecure™ dient speziell der Analyse technischer Belege für potenzielle Zwischenfälle, z. B. Methoden und Technologien, Netzwerkrouten, Herkunft des Datenverkehrs und zeitliche Abläufe. Das WithSecure™-Team bietet jedoch nur eine Anleitung zur Lösung selbst; weitere professionelle Services zur Unterstützung der Incident Response sind gesondert zu vereinbaren. Wenn der Kunde eine Straftat vermutet, empfehlen wir, die zuständigen Behörden zu kontaktieren und den Bericht zur Bedrohungsermittlung vorzulegen.

## 3.9 Automatisierung von Maßnahmen

Automatisierte Response-Maßnahmen sind verfügbar, um die Auswirkungen gezielter Cyberangriffe zu verringern, indem sie außerhalb der Geschäftszeiten automatisch eingedämmt werden, wenn das Risiko hinreichend hoch ist. Die Automatisierung wurde speziell entwickelt, um in der Nacht oder am Wochenende erste Maßnahmen zu ergreifen, wenn Teams die Erkennungen überwachen, die nur während der Geschäftszeiten auf Zwischenfälle reagieren können, .

## 3.10 Hochentwickelte Response-Maßnahmen

Mit hochentwickelten Response-Maßnahmen lassen sich die Auswirkungen gezielter Cyberangriffe reduzieren und mehr Informationen über die Zwischenfälle und die IT-Umgebung sammeln. Die Maßnahmen können für mehrere Endgeräte gleichzeitig festgelegt werden. Das erhöht die Effizienz bei der Reaktion auf Zwischenfälle. Darüber hinaus führen Endgeräte, die derzeit nicht online sind, die Aktionen sofort aus, sobald sie online sind.

Zu den für WithSecure™ Endpoint Detection and Response verfügbaren Response-Maßnahmen gehören:

- Durchführung der Netzwerkisolierung für das Endgerät (diese Reaktion kann automatisiert werden)
- Scannen des Endgeräts auf Malware und andere schädliche Inhalte
- Abfrage verschiedener Daten, Protokolle, Prozess- und Aufgabenlisten
- Löschen und Isolieren von Dateien, Ordnern, Registry-Daten, Prozessen und Diensten

Mit diesen Maßnahmen kann ein Netzwerkadministrator Datenpannen effizient stoppen, bevor sie größeren Schaden im Unternehmen anrichten. Bitte beachten Sie, dass hochentwickelte Response-Maßnahmen nicht in Kombination mit WithSecure™ Business Suite-Produkten verfügbar sind.

## 3.11 Event Search

Mit dieser integrierten Funktion können Sie die von den Endgeräten Ihres Unternehmens gesammelten Ereignisdaten, die mit Broad Context Detection in Zusammenhang stehen, anzeigen, durchsuchen und untersuchen. Event Search ermöglicht das Filtern und Suchen nach Ereignissen basierend auf der Zeit, zu der sie aufgetreten sind, sowie auf dem Gerät und der Organisation, wo das Ereignis stattgefunden hat.

## 3.12 Event Search for Threat Hunting

Diese hochentwickelte Funktion dient zur Untersuchung und Interaktion mit allen von den Endgeräten gesammelten Ereignisrohdaten. Dank ausgefeilter Filterfunktionen können Ihre Cybersicherheitsexperten im SOC ein proaktives Threat Hunting durchführen, um die raffiniertesten versteckten Bedrohungen zu erkennen und zu stoppen. Da die Funktion eine viel umfangreichere Reihe von Ereignissen umfasst (außer denen, die mit den Broad Context Detections zusammenhängen), ist auch die Datenmenge viel größer. Aus diesem Grund ist Event Search for Threat Hunting eine optionale Komponente von WithSecure Elements Endpoint Detection and Response.

# 4. Der Datenschutz

## 4.1 Datenschutz und Vertraulichkeit

Die gesammelten verhaltensbezogenen Ereignisdaten von Endgeräten werden innerhalb der Europäischen Union (in Irland) für ein Jahr rollierend während der Geschäftsbeziehung gespeichert und innerhalb von zwei Monaten nach Beendigung der Zusammenarbeit gelöscht.

Die Lösung ist nicht für die Überwachung von nicht sicherheitsrelevanten Aktivitäten vorgesehen, wie z. B. die Erstellung von Profilen der Aktivitäten, Interessen oder Interaktionen von Mitarbeitern. Der Schwerpunkt der Datenerfassung liegt nicht auf einzelnen Mitarbeitern, Geschäftsdokumenten oder E-Mail-Inhalten. Weitere Einzelheiten entnehmen Sie bitte der lösungsspezifischen Datenschutzrichtlinie.

Da WithSecure™ seinen Sitz in Finnland hat, halten wir uns an die strengen Datenschutz- und Sicherheitsvorschriften Finnlands und der Europäischen Union. Wir erfüllen die Datenschutzrichtlinien der EU und berücksichtigen die Datenschutzbedürfnisse unserer Kunden. WithSecure™ folgt der finnischen Umsetzung der EU-Datenschutzrichtlinie. Die Lösung WithSecure™ Elements Endpoint Detection and Response wurde in Übereinstimmung mit der Datenschutzgrundverordnung (DSGVO) der EU entwickelt. Weitere Informationen über die Einhaltung der DSGVO durch WithSecure finden Sie unter https://www.WithSecure.com/GDPR.

## 4.2 Maßnahmen zur Datensicherheit

Als Security-Unternehmen nehmen wir die Sicherheit unserer Rechenzentren sehr ernst und setzen Dutzende von Sicherheitsmaßnahmen ein, um sie zu gewährleisten, z. B:

- Security by Design: Unsere Systeme sind von Anfang an auf Sicherheit ausgelegt. Wir integrieren Datenschutz und Sicherheit in die Entwicklung unserer Technologien und Systeme, von den frühen Phasen von Konzeption und Design bis hin zu Implementierung und Betrieb.
- Strenge Zugangskontrollen: Nur eine kleine, verifizierte Gruppe von WithSecure™-Mitarbeitern hat Zugang zu Kundendaten. Die Zugriffsrechte und -ebenen richten sich entsprechend dem Least-Privilege-Konzept nach ihrer Funktion und Rolle, abgestimmt auf die definierten Verantwortlichkeiten.
- Starke operative Sicherheit: Operative Sicherheit ist ein alltäglicher Bestandteil unserer Arbeit, einschließlich Schwachstellenmanagement, Malware-Prävention und robuster Prozesse für das Management von Zwischenfällen, die die Vertraulichkeit, Integrität oder Verfügbarkeit von Systemen oder Daten beeinträchtigen können.

## 4.3 Rechenzentren

Unsere Endpoint Detection and Response nutzt die Rechenzentren von Amazon Web Services (AWS), um die höchstmögliche Verfügbarkeit und Fehlertoleranz sowie bessere Reaktionszeiten und die Fähigkeit zur bedarfsgerechten Skalierung zu gewährleisten. AWS erklärt, dass jedes seiner Rechenzentren den Tier 3+ Richtlinien entspricht. Weitere Informationen über die AWS-Rechenzentren finden Sie unter https://aws.amazon.com/compliance/.

Die gesammelten verhaltensbezogenen Ereignisdaten von Endgeräten werden auf AWS in Europa (Irland) gespeichert. Die Datenspeicherung für ein Jahr ist im Elements Endpoint Detection and Response-Abonnement enthalten. Es fallen keine zusätzlichen Gebühren für eine mengenbezogene Datenspeicherung an.

# Über WithSecure™

WithSecure™, ehemals F-Secure Business, ist der zuverlässige Partner für Cybersicherheit. IT-Dienstleister, Managed Security Services Provider und andere Unternehmen vertrauen WithSecure™ – wie auch große Finanzinstitute, Industrieunternehmen und führende Kommunikations- und Technologieanbieter. Mit seinem ergebnisorientierten Ansatz der Cybersicherheit hilft der finnische Sicherheitsanbieter Unternehmen dabei, die Sicherheit in Relation zu den Betriebsabläufen zu setzen und Prozesse zu sichern sowie Betriebsunterbrechungen vorzubeugen. WithSecure™ nennt diesen Ansatz „Outcome-based Cyber Security“. KI-gesteuerte Sicherheitsmaßnahmen sichern Endpoints und die Zusammenarbeit in der Cloud mit intelligenten Erkennungs- und Reaktionsmechanismen. Die Detection & Response-Experten von WithSecure™ identifizieren Geschäftsrisiken, indem sie proaktiv nach Bedrohungen suchen und bereits laufende Angriffe abwehren – dabei arbeiten sie eng mit Instituten, großen Unternehmen und innovativen Tech-Firmen zusammen. Sie haben mehr als 30 Jahre Erfahrung in der Entwicklung von Technologien, die sich an den Bedürfnissen der Unternehmen orientieren. Das Portfolio von WithSecure™ eröffnet durch flexible Vertriebsmodelle die Möglichkeit, gemeinsam mit Partnern zu wachsen.

WithSecure™ Corporation wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd. gelistet.

WITH secure