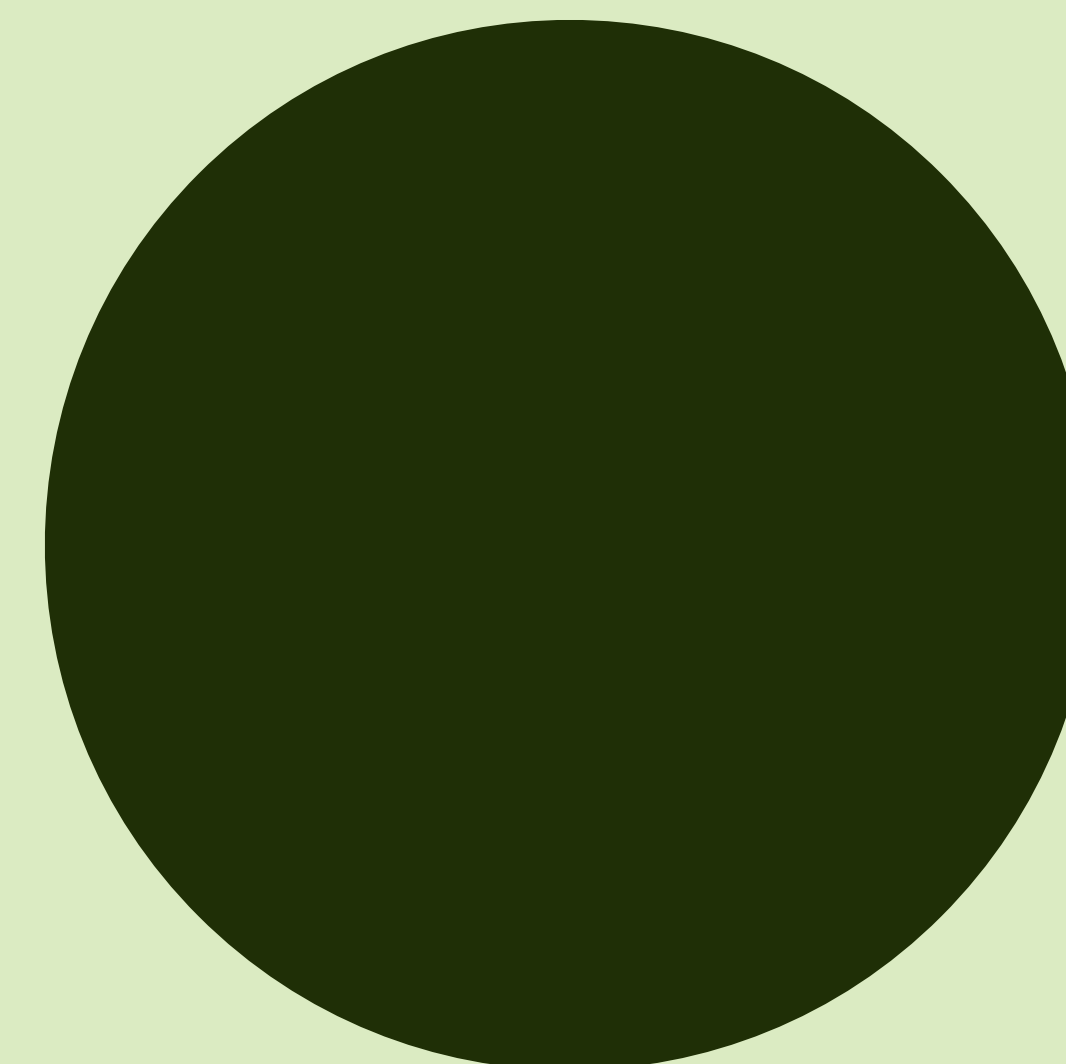


Broschüre

**W / T H**<sup>®</sup>  
secure

# Gezielte Angriffe stoppen

**WithSecure™ Elements Endpoint Detection and Response**



# Unternehmen und Daten vor komplexen Cyberangriffen schützen

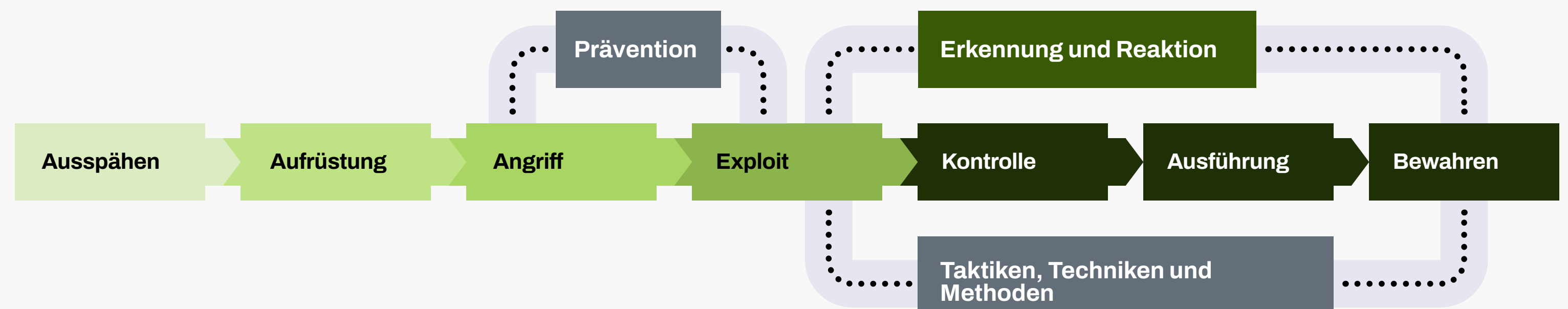
Eine effektive, vorbeugende Bedrohungsabwehr ist der Eckpfeiler aller Cybersicherheit. Auf Präventivmaßnahmen allein dürfen sich Unternehmen, die sich und ihre Daten vor den Taktiken, Techniken und Methoden der Angreifer schützen wollen, aber nicht verlassen.

Die sich ständig verändernde Bedrohungslage und regulatorische Bestimmungen wie die DSGVO erfordern, dass Unternehmen auch auf die Erkennung von Sicherheitsverletzungen nach einem Schadensfall vorbereitet sind. Konkret muss sichergestellt sein, dass Sie schnell auf komplexe Angriffe reagieren können.

WithSecure™ Elements Endpoint Detection and Response ist eine Lösung, die von einem erfahrenen Team von Threat Huntern trainiert wird.

Damit kann Ihre IT-Abteilung oder ein zertifizierter Dienstleister Ihr Unternehmen vor komplexen Bedrohungen schützen. Mit der Unterstützung der erstklassigen Cybersicherheitsexperten von WithSecure™ können Ihre IT-Fachleute schnell

und effektiv auf Vorfälle reagieren. Wenn Sie sich ganz auf das Kerngeschäft konzentrieren wollen, überlassen Sie Erkennung und Reaktion getrost einem Dienstleister, und greifen im Angriffsfall auf die Hilfestellung von Experten zurück.



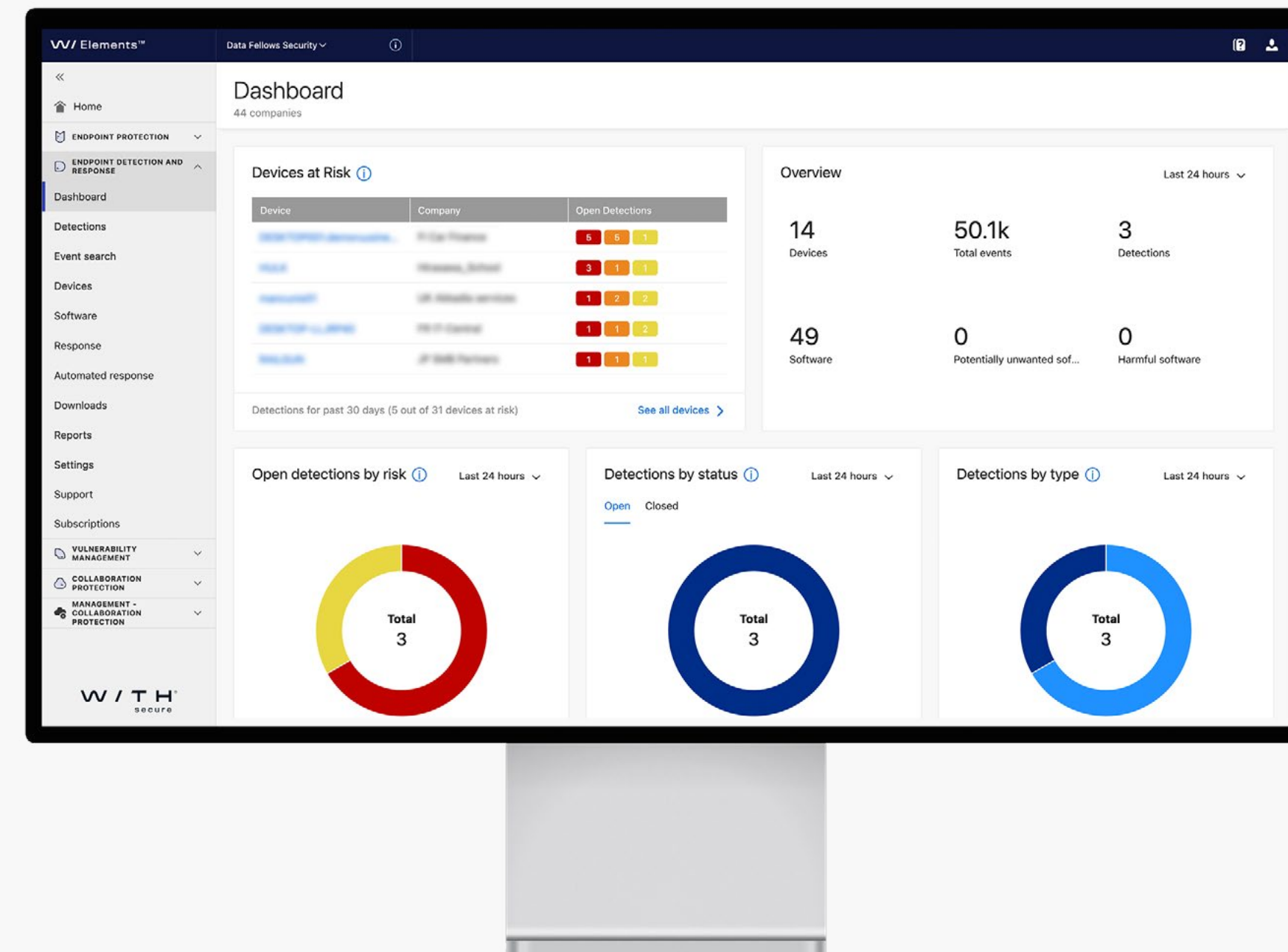
## Übersicht

# Gezielte Angriffe rasch stoppen mit Automatisierung und Hilfestellung

Wie können Sie komplexe Angriffe erkennen? Indem Sie die fortschrittlichsten Analysetechniken und maschinellen Lernverfahren einsetzen, die Ihr Unternehmen vor komplexen Cyberbedrohungen und Sicherheitsverletzungen schützen.

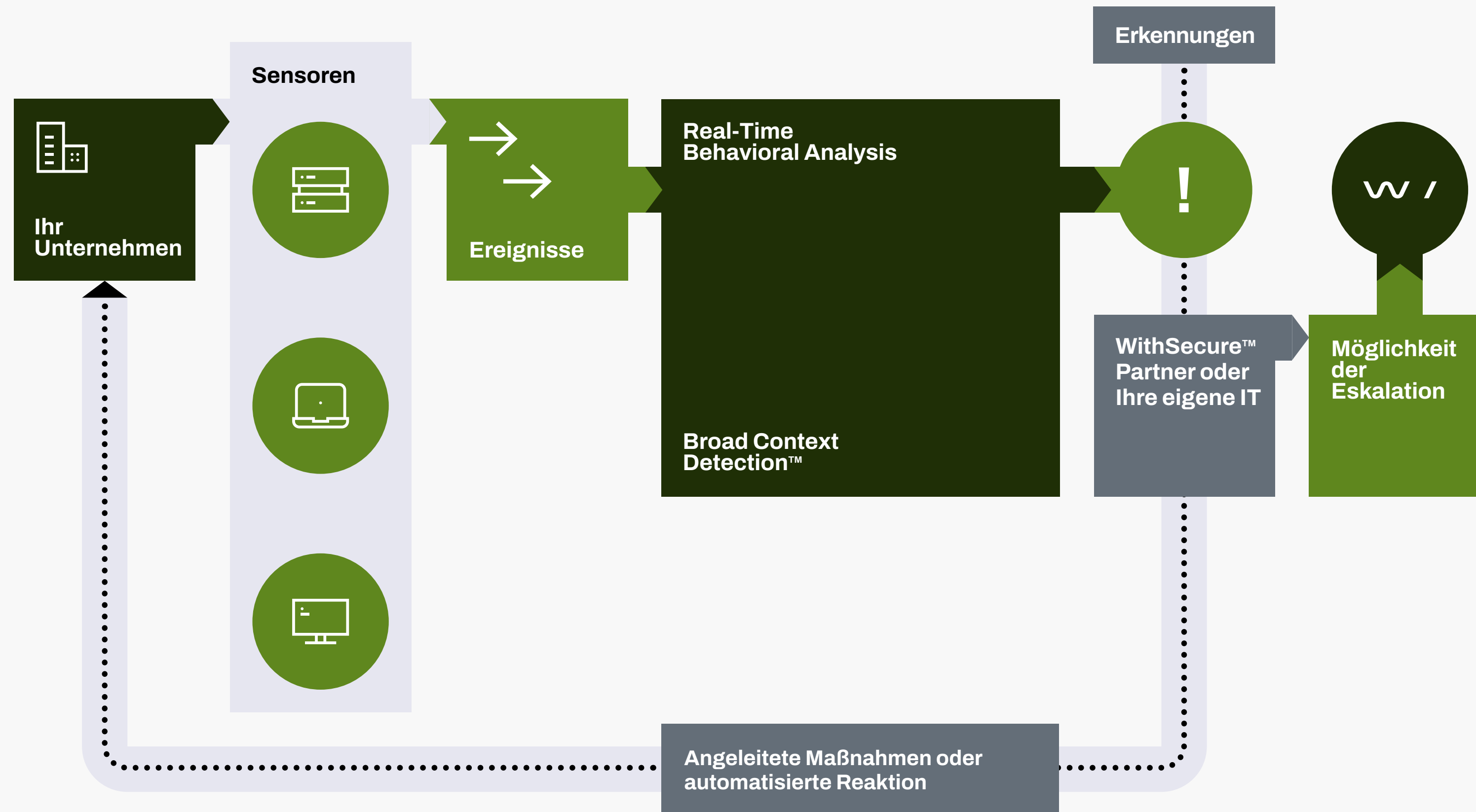
Die branchenführende Lösung Endpoint Detection und Response (EDR) von WithSecure™ verschafft Ihnen einen kontextbezogenen Einblick in komplexe Bedrohungen und versetzt Sie in die Lage, darauf automatisiert und mit Hilfestellung zu reagieren.

Wenn eine Sicherheitsverletzung eintritt, brauchen Sie mehr als nur einen Alarm. Damit Sie optimal reagieren können, müssen Sie die Struktur des Angriffs durchschauen. Mit unserer Broad Context Detection™, zertifizierten Dienstleistern und integrierter Automatisierung wehren Sie Angriffe schnell ab und erhalten konkrete, leicht umsetzbare Anleitungen zur weiteren Problemlösung.





## How it works



Stets zu Diensten: die branchenführende Technologie und Sicherheitsexperten von WithSecure™

1. Ressourcenschonende Sensoren auf allen Endpunkten überwachen Verhaltensereignisse auf Anwenderseite und geben sie zur Echtzeitdatenanalyse sowie an unsere Broad Context Detection™ weiter, um böswilliges Verhalten von normalem Benutzerverhalten zu unterscheiden.
2. Alarme mit Risikoeinstufung und einer Visualisierung des umfassenden Kontexts über alle betroffenen Hosts hinweg erleichtern die Bestätigung einer Erkennung, ob durch den WithSecure™ Partner oder die interne IT. Optional sind automatisierte Reaktionsmaßnahmen und die Eskalation an WithSecure™ möglich.
3. Nach einer bestätigten Erkennung bietet die Lösung Ratschläge und Handlungsempfehlungen für die erforderlichen Schritte, mit denen Sie die Bedrohung rasch eindämmen und beheben können.

## Funktionsweise

# Die Nadel im Heuhaufen - ein Beispiel aus der Praxis

Die Erkennung komplexer Bedrohungen anhand von 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 durch unsere Backend-Systeme reduzierte sich diese Zahl auf 225.000.

Nach einer 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 bestätigt.

IT- und Sicherheitsteams können sich somit auf weniger, aber präzisere Erkennungsergebnisse konzentrieren und dadurch bei tatsächlichen. ??? Bedrohungen entsprechend eingreifen.

# 500 millionen

Datenergebnisse im Monat

Erfasst mit 325 Endpunktsensoren

# 225 000

Verdächtige Ereignisse nach der Echtzeit-Verhaltensanalyse der Ereignisse

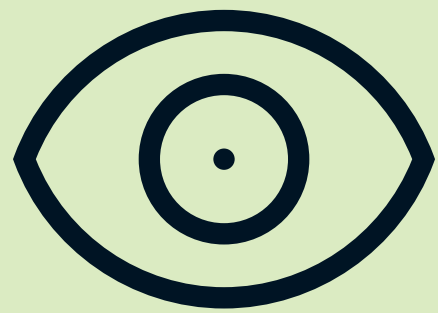
# 24

Erkennungen nach der Berücksichtigung des breiteren Kontextes der verdächtigen Ereignisse

# 7

Echte Bedrohungen nach der Bestätigung der Erkennungen als tatsächliche Bedrohungen

## Vorteile



### Transparenz

Unmittelbarer Einblick in IT-Umgebung und Sicherheitsstatus

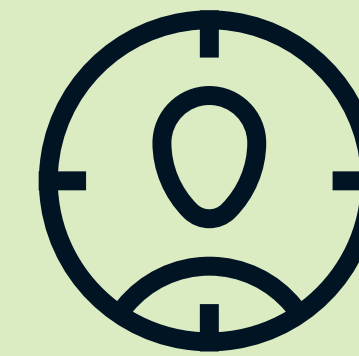
- Klarerer Überblick über die IT-Umgebung und den Sicherheitsstatus durch Inventarisierung der Anwendungen und Endpunkte
- Identifizierung verdächtiger Aktivitäten durch Erfassung von Verhaltensereignissen und Herstellung von Zusammenhängen, die über übliche Malware hinausgehen
- Erleichterte Reaktion auf Vorfälle durch Alarme mit Informationen zum umfassenden Kontext und zur Kritikalität



### Erkennung

Schutz des Unternehmens und seiner sensiblen Daten durch die rasche Erkennung von Sicherheitsvorfällen

- Minimierung von Ausfallzeiten und negativen Auswirkungen auf die Markenreputation durch schnelle Erkennung und Abwehr gezielter Angriffe
- Implementierung innerhalb weniger Stunden zu Ihrem Sofortschutz vor Sicherheitsverletzungen
- Compliance mit Standards (PCI, HIPAA und DSGVO), die die Meldung von Sicherheitsvorfällen innerhalb von 72 Stunden vorschreiben



### Reaktion

Umgehende Reaktion mit Hilfestellung und Automatisierung im Angriffsfall

- Fokus auf relevante Bedrohungen dank Automatisierung und Analyseintelligenz
- Alarme mit Hilfestellung zu Reaktionsmaßnahmen und deren Automatisierung rund um die Uhr
- Mangelnde Expertise und Ressourcen kompensieren durch zertifizierte und von WithSecure™ unterstützte Dienstleister

## Funktionen

### Endpunktsensoren

Ressourcenschonende, diskrete Überwachungstools, die mit allen Schutzlösungen für Endpunkte zusammenarbeiten

- Bereitstellung von ressourcenschonenden Sensoren auf allen relevanten Computern in Ihrem Unternehmen
- Single-Client- und Management-Infrastruktur mit Endpunktsicherheitslösungen von WithSecure™
- Datenschutzgerechte Erfassung von Verhaltensdaten auf Windows-, Mac- und Linux-Geräten durch die Sensoren compromising users' privacy.

### Angeleitete Reaktion

Abwehr selbst komplexester Cyberangriffe mit dem vorhandenen Team

- Integrierte Schritt-für-Schritt-Hilfestellung und Remote-Maßnahmen zur Unterbindung von Angriffen
- Reaktionsmaßnahmen mit Anleitung und Unterstützung durch zertifizierte Dienstleister
- An WithSecure™ eskalieren: unser einzigartiger Service für Bedrohungsanalyse und Expertenunterstützung

### Broad Context Detection™

Die proprietäre Erkennungstechnologie von WithSecure™, die es einfach macht, das Ausmaß eines zielgerichteten Angriffs zu verstehen

- Verhaltens-, Reputations- und Big-Data-Analyse in Echtzeit mit maschinellen Lernalgorithmen
- Automatische Kontexteinordnung von Erkennungen, Visualisierung auf einer Zeitleiste
- Einbeziehung von Daten zu Risikostufen, zur Kritikalität des betroffenen Hosts und zur jeweiligen Bedrohungslage

### Automatisierte Reaktion

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

- Automatische Reaktionsmaßnahmen auf der Grundlage von Kritikalität, Risikostufe und festgelegtem Zeitplan
- Priorisierung von Reaktionsmaßnahmen auf der Basis von Kritikalität und Risikostufen
- Schnelle Abwehr von Angriffen auch außerhalb der Geschäftszeiten

### Anwendungstransparenz

Nie dagewesener Überblick über IT-Umgebung und Sicherheitsstatus

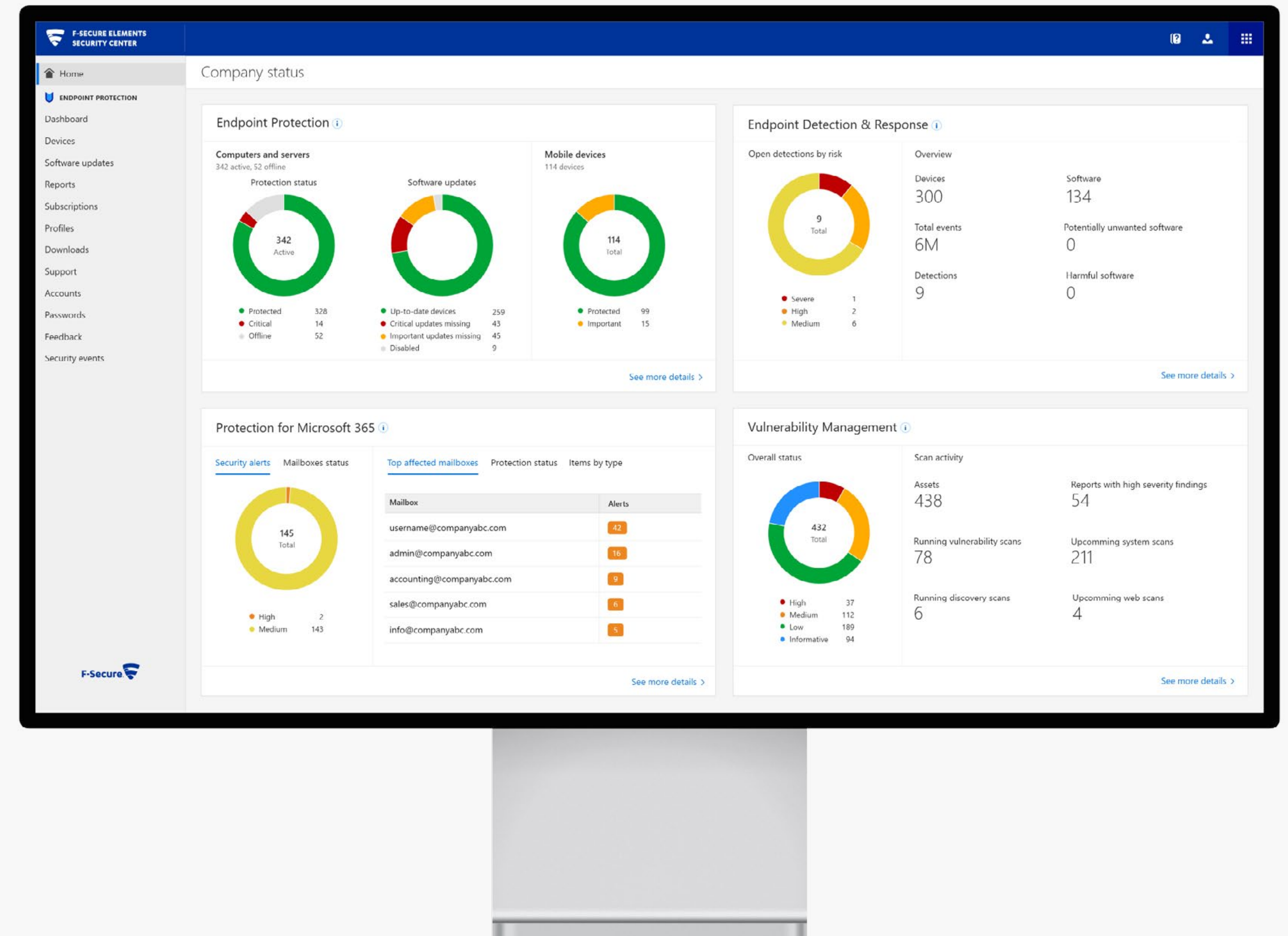
- Ermittlung von schädlichen und unerwünschten Anwendungen sowie der externen Adressen von Clouddiensten
- Nutzung der Reputationsdaten von WithSecure™ zur Identifizierung potenziell gefährlicher Anwendungen
- Einschränkung potenziell schädlicher Anwendungen und Clouddienste, bevor es zu Sicherheitsverletzungen kommt



# WithSecure™ Elements – mehr Flexibilität, weniger Komplexität. Die einzige Cybersicherheitsplattform, die Sie brauchen.

WithSecure™ Elements Endpoint Detection and Response ist als eigenständige Lösung oder als integrierte Funktionalität in der modularen Cybersicherheitsplattform WithSecure™ Elements erhältlich.

Probieren Sie es noch heute selber aus





# Über WithSecure

WithSecure™ 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™ ist Teil der 1988 gegründeten F-Secure Corporation, die an der NASDAQ OMX Helsinki Ltd. gelistet ist.

