Produktübersicht

# WithSecure™ Elements Endpoint Protection

**Risiken, Komplexität und Ineffizienz reduzieren - mit WithSecure™ Elements.**

# Inhalt



**Januar 2023**

HAFTUNGSAUSSCHLUSS: Dieses Dokument bietet einen umfassenden Überblick über die wichtigsten Sicherheitskomponenten von WithSecure™ Elements Endpoint Protection. Auf Details wurde bewusst verzichtet, um gezielte Angriffe auf unsere Lösungen zu verhindern. WithSecure™ verbessert seine Dienste fortlaufend. WithSecure™ behält sich das Recht vor, Merkmale oder Funktionen der Software in Übereinstimmung mit seinen Produktlebenszyklus-Praktiken zu ändern.

# Kurzbeschreibung

WithSecure™ Elements Endpoint Protection hilft Unternehmen, Bedrohungen wie Ransomware zu stoppen und Datenpannen auf ihren Arbeitsstationen, Laptops, Mobiltelefonen und Servern proaktiv zu verhindern. Die Lösung bietet alles, was Unternehmen für den Endpunktschutz benötigen, einschließlich vollständig integrierter Patchverwaltung, um wirksam Angriffe zu verhindern, die Schwachstellen in installierter Software ausnutzen.

## Flexible, widerstandsfähige Cybersicherheit mit WithSecure™ Elements

In der heutigen agilen Geschäftsumgebung ist die einzige Konstante die Veränderung. WithSecure™ Elements bietet Unternehmen eine Sicherheitskomplettlösung, die sich an Veränderungen sowohl im Unternehmen als auch mit Blick auf die Bedrohungslage anpasst und die mit der Organisation mitwächst. Die Lösung bietet flexible Lizenzmodelle und Sicherheitstechnologien, die Sie bedarfsgerecht zusammenstellen können. WithSecure™ Elements integriert die gesamte Palette von Cybersicherheitskomponenten, einschließlich Schwachstellen-Management, Patchverwaltung, Endpunktschutz sowie Erkennung und Reaktion, in einem einziges ressourcenschonendes Softwarepaket, das über eine einheitliche, cloudbasierte Verwaltungskonsole bedient wird. Über dieselbe Konsole können Unternehmen die Sicherheit ihrer Microsoft 365 Collaboration-Dienste verwalten. Mit einer flexiblen nutzungsbasierten SaaS-Option lässt sich Elements ganz einfach intern verwalten. Sie können es aber auch als vollständig verwalteten Abonnementdienst von einem unserer zertifizierten Partner erwerben. Der Wechsel von einer auf die andere Variante ist ebenfalls problemos möglich. So bleiben auch Unternehmen, die zunehmend Schwierigkeiten haben, Mitarbeiter mit entsprechenden Cybersicherheitskenntnissen zu finden, trotz der sich ständig weiterentwickelnden Angriffslage jederzeit geschützt.

WithSecure™ Elements besteht aus vier Lösungskomponenten, die alle über dieselbe Konsole, das WithSecure™ Elements Security Center, verwaltet werden.

**WithSecure™ Elements Endpoint Protection:** Der Endpunktschutz von WithSecure™ wurde mehrfach mit dem Best Protection Award von AV-TEST ausgezeichnet und ermöglicht als cloudnative, KI-gestützte Lösung eine einfache und flexible Bereitstellung und verwaltet die Sicherheit all Ihrer Endpunkte. So ist Ihre Organisation vor Angriffen geschützt. WithSecure™ Elements Endpoint Protection schützt Handys, Desktops, Laptops und Server.

**WithSecure™ Elements Endpoint Detection and Response:** WithSecure™ Elements Endpoint Detection and Response bietet einen sofortigen Überblick über IT-Umgebungen und ihren Sicherheitsstatus aus einem einzigen Blickwinkel. Es schützt Unternehmen und seine Daten, indem es Angriffe schnell erkennt und unter fachkundiger Anleitung reagiert. Schwierige Fälle können an unsere Elite-Cybersicherheitsspezialisten weitergeleitet werden. Mit der automatischen Reaktion können Sie Sicherheitsverletzungen rund um die Uhr effektiv beheben. WithSecure™ Elements Endpoint Detection and Response schützt Desktops, Laptops und Server.

**WithSecure™ Elements Vulnerability Management:** Entdecken und verwalten Sie kritische Schwachstellen in Ihrem Netzwerk und an Ihren Ressourcen. Indem Sie Schwachstellen aufdecken, priorisieren und patchen, verkleinern Sie Ihre Angriffsfläche und verringern die Einstiegspunkte für Angreifer.

**WithSecure™ Elements Collaboration Protection:** Ergänzen Sie die nativen E-Mail-Sicherheitsfunktionen von Microsoft 365 durch fortgeschrittene Sicherheitsfunktionen, um Angriffe per E-Mails und URLs zu vereiteln. Dank der Cloud-to-Cloud-Integration lässt sich die Lösung leicht bereitstellen und verwalten.

WithSecure™ Elements Endpoint Protection, Elements Endpoint Detection and Response und Vulnerability Management sind in einem einzigen Software-Paket gebündelt, das automatisch aktualisiert wird. So sparen Sie bei der Bereitstellung und Verwaltung der Software Zeit und Geld.

## Vorteile der integrierten Lösungen

Als modulare Lösung passt sich WithSecure™ Elements den wechselnden Anforderungen Ihres Unternehmens an. Einheitliche Cybersicherheit bedeutet einfachere Lizenzierung, weniger Aufwand zur Sicherheitsverwaltung und größere Produktivität ohne Einbußen für die Cybersicherheit Ihres Unternehmens. Die cloudbasierte Konsole – das WithSecure™ Elements Security Center – bietet einen zentralisierten Überblick über, Erkenntnisse zu und Verwaltungsmöglichkeiten für alle Endpunkte und Clouddienste. Es wird vollständig von einem unserer zertifizierten Managed Service Provider verwaltet oder auch von Ihnen selbst – mit On-Demand-Support von WithSecure™. Das Sicherheitscenter bietet eine Übersicht über den Schutzstatus an einem Ort, der Endpoint Protection, Endpoint Protection and Response, Vulnerability Management und Schutz für Microsoft 365 kombiniert.

Zusätzlich zu den Vorteilen bei der Bereitstellung und Verwaltung sind die WithSecure™ Elements-Lösungen so konzipiert, dass sie im Zusammenspiel die Sicherheitsvorteile für das Unternehmen maximieren. Durch die Kombination von Sicherheitsereignissen und Sicherheitsalarmen können die XDR-Funktionen von WithSecure™ Elements vollumfassende Sicherheit bieten und die Silos aus verstreuten Einzellösungen effektiv ersetzen.

WithSecure™ Elements Endpoint Protection richtet sich an Unternehmen mit folgenden Erfordernissen:

- Breitere Abdeckung von Endpunkten und Diensten als herkömmliche, marktübliche Lösungen zu wesentlich attraktiveren Gesamtbetriebskosten (TCO)
- Umsetzung eines hervorragenden Schutzniveaus mit minimalen Ressourcenanforderungen und der Option, die Verwaltung der Lösung vollständig an einen zertifizierten Dienstanbieter auszulagern
- Einsatz einer unkomplizierten, skalierbaren Lösung, die von einer Stelle aus Überblick und Schutz für mehrere, geografisch verteilte Standorte bietet
- Vermeidung von Investitionen in Zeit und Ressourcen zur Pflege lokaler Serverumgebungen

Durch die Bündelung des Schutzes verschiedener Endpunkte und zusätzlicher Sicherheitstools in einer einzigen Lösung bietet Elements Endpoint Protection:

- größere Sicherheitsabdeckung und -funktionen als die meisten anderen Sicherheitslösungen für Endpunkte,
- eine vereinheitlichte, straffe Verwaltung auf Cloudbasis, die Zeit und Ressourcen zum Verwalten und Warten der Sicherheitsumgebung einspart und die Gesamtbetriebskosten weiter reduziert.

Die Bereitstellung der Lösung erfolgt als cloudbasierter Dienst: entweder selbst verwaltet oder durch einen zertifizierten Dienstanbieter, mit der Option, die Lösung in Drittanbietersysteme zu integrieren.

Dass wir einen besseren und konsistenteren Schutz bieten als unsere Wettbewerber, bestätigen Jahr um Jahr Tests von unabhängigen Branchenexperten und Analysten.

WithSecure™ hat seine Beständigkeit in unabhängigen Tests unter Beweis gestellt. So haben wir als einziger Anbieter in den 6 Jahren seit seiner Einrichtung den prestigeträchtigen jährlichen „Best Protection Award“ von AV-TEST für Unternehmensprodukte erhalten. AV-Test führt das ganze Jahr über Vergleichstests durch. Um diese wertvolle Auszeichnung zu erhalten, müssen also durchgängig gute Ergebnisse in den Schutztests vorgewiesen werden.

Um diese anspruchsvollen Standards zu erfüllen, verwendet die Lösung einen mehrschichtigen Ansatz für die Sicherheit und nutzt verschiedene moderne Technologien wie heuristische und verhaltensbasierte Bedrohungsanalysen sowie Informationen über Bedrohungen in Echtzeit, die über die WithSecure™ Security Cloud bereitgestellt werden.

So ist gewährleistet, dass Sie in Sachen Sicherheit ganz vorne mit dabei sind.

# 1. Übersicht über die Lösung

Unternehmen stehen vor der Herausforderung, das Geschäftsrisiko zu minimieren, das Cyberbedrohungen wie Ransomware darstellen. Das zugrunde liegende Konzept von WithSecure™ Elements Endpoint Protection beruht darauf, anspruchsvolle Sicherheitsanforderungen von Unternehmen mit einem Minimum an Wartungs- und Verwaltungsaufwand zu erfüllen. Es bietet preisgekrönten Bestschutz für Windows- und Mac-Computer, iOS- und Android-Geräte und eine Vielzahl von Server-Plattformen. Mit integrierter Patchverwaltung, mehrschichtigem Schutz sowie fortgeschrittener verhaltensbasierter und heuristischer Analyse beugt Elements Endpoint Protection schon heute den Cyber-Bedrohungen von morgen vor.

## WithSecure™ Elements Endpoint Protection bietet:

- **Den besten Schutz** der Branche und damit die Unternehmenssicherheit sowie rasche Wiederherstellung nach einem Vorfall,
- **Proaktive Minimierung des Geschäftsrisikos** durch Datenpannen dank vollständig integrierter Patchverwaltung,
- **Eine cloudnative Lösung**, die Zeit spart beim Bereitstellen, Verwalten und Überwachen der Sicherheit.


WithSecure™ Elements Endpoint Protection Lösung ist auch als vollständig verwalteter Dienst verfügbar. WithSecure™-zertifizierte Dienstanbieter können die durch Partner verwaltete Version oder die SaaS-Version der Lösung nutzen, um viele einzigartige Funktionen für Dienstanbieter auszuschöpfen, wie z. B. das Dashboard für mehrere Unternehmen, die Berichterstattung und die Verwaltung von Abonnements. Die SaaS-Version der Lösung ermöglicht es Dienstanbietern, flexible Geschäftsmodelle zu nutzen, z. B. verbrauchsbasierte Abrechnung für alle Produkte von WithSecure™ Elements.

## 1.1 Pakete im Umfang der Lösung

Elements Endpoint Protection bietet Schutz für Windows und Mac, für Computer und Server und ist als Standardpaket und Premiumpaket erhältlich. Die Funktionen des Standardpakets umfassen erweiterte Anti-Malware-Funktionen, Patchverwaltung sowie zahlreiche weitere Sicherheitsfunktionen für Endpunkte. Die Funktionen des Premiumpakets bieten besseren Schutz vor Ransomware sowie eine Anwendungssteuerung. Beide Pakete für Endpunkte können um die Lösungen Elements Endpoint Detection and Response und Elements Vulnerability Management ergänzt werden. Die Funktionen von Detection and Response für Erkennung und Reaktion verbessern Transparenz, Erkennungen und automatisierte Reaktionen auf komplexe Bedrohungen sowie Datenpannen. Das Schwachstellenmanagement hilft dabei, kritische Schwachstellen auf den Endpunkten zu entdecken und zu verwalten. Darüber hinaus kann WithSecure™ Elements Collaboration Protection per Cloud-to-Cloud-Integration bereitgestellt werden, ohne dass Middleware oder Software auf den Endpunkten installiert werden muss.

## WithSecure™ Elements

| | Endpoint Protection Standard | Endpoint Protection Premium | Detection and Response | Vulnerability Management | Collaboration Protection |
|---|---|---|---|---|---|
| Hochentwickelte Anti-Malware und Patchverwaltung | ✓ | ✓ | | | |
| Zusätzlicher Schutz vor Ransomware mit DataGuard und Anwendungssteuerung | | ✓ | | | |
| Schutz vor komplexen Bedrohungen | | | ✓ | | |
| Schwachstellenmanagement und Priorisierung | | | | ✓ | |
| Zukunftsweisende cloudbasierte Sicherheit für E-Mails und die Zusammenarbeit mit Microsoft 365 | | | | | ✓ |

Die Pakete mit ihren jeweiligen Schutzfunktionen können ohne Neuinstallation der Client-Software installiert werden.
Weitere Information unter WithSecure™ Elements.

**Software Updater**
Automatisierte Patchverwaltung zur Aktualisierung von Softwareanwendungen von Microsoft und über 2500 Drittanbietern.

**DeepGuard**
Intelligente, heuristische Anti-Malware-Engine mit 0-Day-Erkennung.
Whitepaper zu WithSecure™ DeepGuard lesen.

**Webinhaltssteuerung**
Verbessern Sie Sicherheit und Produktivität durch kontrollierten Zugriff auf Websites. Verhindern Sie anhand von festgelegten Kategorien den Zugriff auf Websites, und setzen Sie Ihre Unternehmensrichtlinie durch.

**Verbindungssteuerung**
Aktivieren Sie zusätzliche Sicherheit für sensible Transaktionen wie Online-Banking.

**Echtzeit-Schutz**
WithSecure™ Security Cloud schützt vor neuer Malware, da es die Bedrohungsdetails anderer geschützter Rechner nutzt und so wesentlich effizienter reagieren kann.

**Anti-Malware-Schutz mit mehren Engines**
Bietet unübertroffenen Schutz mit hochentwickelter Multi-Engine-Anti-Malware.

**Firewall**
Zusätzliche Regeln und Verwaltungsfunktionen, die in die Windows Firewall integriert sind.

**Browser-Schutz**
Verhindert proaktiv, dass Mitarbeiter auf schädliche Websites mit bösartigen Links oder Inhalten zugreifen.

**Gerätesteuerung**
Die Gerätesteuerung verhindert, dass Bedrohungen über Hardware-Geräte wie USB-Sticks, CD-ROM-Laufwerke oder Webkameras auf Ihr System gelangen. Dies verhindert auch Datenlecks, indem z. B. nur Lesezugriff erlaubt wird.

**DataGuard**
Bietet zusätzlichen Schutz vor Ransomware und verhindert die Zerstörung und Manipulation von Daten.

**Anwendungssteuerung**
Verhindert die Ausführung von Anwendungen und Skripten anhand der von unseren Penetrationstestern erstellten oder vom Administrator festgelegten Regeln. Darüber hinaus kann die Anwendungssteuerung das Laden von DLLs oder anderen Dateien blockieren, um die Sicherheit zu erhöhen.

**XFENCE**
Einzigartige Sicherheitsfunktion zum Schutz von Macs vor Malware, Trojanern, Hintertüren, fehlerhaften Programmen und anderen Bedrohungen, die verhindert, dass Programme ohne ausdrückliche Berechtigung auf Dateien und Systemressourcen zugreifen.

**Endpunktverschlüsselung**
Überwachen und verwalten Sie den Status der Festplattenverschlüsselung Ihrer Windows-Computer. Sie können die Bitlocker-Verschlüsselung ein- und ausschalten und Wiederherstellungsschlüssel direkt vom WithSecure™ Elements Sicherheitscenter abrufen.

## 1.2 Komponenten der Lösung

Die Lösung besteht aus vier Hauptkomponenten, die in diesem Dokument einzeln beschrieben werden:

1. **Elements Security Center** als cloudbasiertes Management-Portal
2. **Computer Protection** als dedizierte Sicherheits-Clients für Arbeitstationen (Windows, Mac)
3. **Mobile Protection für Mobilgeräte** (iOS, Android)
4. **Server Protection** eine Vielzahl von Serverplattformen (Windows, Citrix, Linux)

## 1.3 Bereitstellung der Lösung

Clients für die Endpoint-Sicherheit können per E-Mail, lokaler Installation, Batch-Skript, Unternehmensverwaltungssystem (SolarWinds, Kaseya, Datto) oder mit einem MSI-Paket über domänenbasierte Tools für die Remoteinstallation bereitgestellt werden. Auf die gleiche Weise werden Mac-Clients als Pakete mit dem Installationsprogramm für macOS oder den Tools für Mobilgeräteverwaltung (Mobile Device Management - MDM) bereitgestellt und können mit zusätzlichen Bereitstellungsschritten zu individuell signierten Paketen zusammengestellt werden.

Im Normalfall kann die Verteilung der Endpoint Security Clients vom Portal aus über eine E-Mail initiiert werden. Der Abonnementschlüssel wird automatisch in den Link oder das Installationsprogramm integriert, sodass der Endbenutzer lediglich auf den Link klicken muss, um den Installationsvorgang automatisch zu starten.

Für größere Umgebungen können Sie ein MSI-Paket erstellen, das entweder mit Ihren eigenen oder mit unseren Tools für die Remoteinstallation bereitgestellt werden kann. Der Windows-Client enthält außerdem integrierte Programm-Flags, mit denen Sie die Bereitstellung des Clients per Batch-Skript automatisieren können.

Wenn der Windows-Client auf Systemen mit einer Sicherheitslösung bereitgestellt wird, die einen Konflikt verursacht, erkennt unsere Sidegrade-Funktion diese und deinstalliert sie automatisch. Erst dann wird die Installation der WithSecure™-Software fortgesetzt. Das gewährleistet einen reibungslosen und schnelleren  Wechsel von einem Lösungsanbieter zum anderen.

Wenn ein neuer Computer zu Elements Endpoint Protection hinzugefügt wird, kann ihm gemäß seiner Stellung in einer Active Directory-Hierarchie automatisch eine Standardkonfiguration (Profil) zugewiesen werden. Dadurch wird der Bereitstellungsprozess gestrafft und das Risiko einer Fehlkonfiguration verringert.

Die Funktionen von Mobile Protection werden in der Regel über die Mobilgeräteverwaltung (MDM) eines Drittanbieters bereitgestellt, die im Rahmen eines Abonnements erhältlich ist und die Verwendung externer MDM-Lösungen unterstützt.

Die Funktionen für die Patchverwaltung sind vollständig in die Clients von Windows-Servern und Arbeitsstationen integriert und können über das Management-Portal gesteuert werden. Da es sich um eine gehostete Lösung handelt, müssen im Gegensatz zu herkömmlichen Lösungen für die Patchverwaltung keine separaten Agenten, Verwaltungsserver oder Konsolen installiert werden.

WithSecure™ Endpoint Proxy, auch als Policy Manager Proxy bezeichnet, wird von WithSecure™ bereitgestellt, um die Bandbreitenauslastung beim Herunterladen von Updates auf Computer Protection-Clients zu minimieren. Dieser Proxy speichert Updates der Malware-Signatur-Datenbank sowie auch Software-Updates des Computer Protection-Clients selbst und Updates der Patchverwaltung in einem Cache.

Die Client-Software für den Endpunktschutz aktualisiert die Datenbanken mit Malware-Signaturen und die Client-Software selbst automatisch, ohne dass sich der Administrator manuell um die Updates oder Upgrades kümmern muss.

WithSecure™-Partner können sowohl die Client-Software für den Endpunktschutz als auch das Elements Security Center mit einem eigenen Logo und Support-Link versehen.

# 2. Elements-Sicherheitscenter

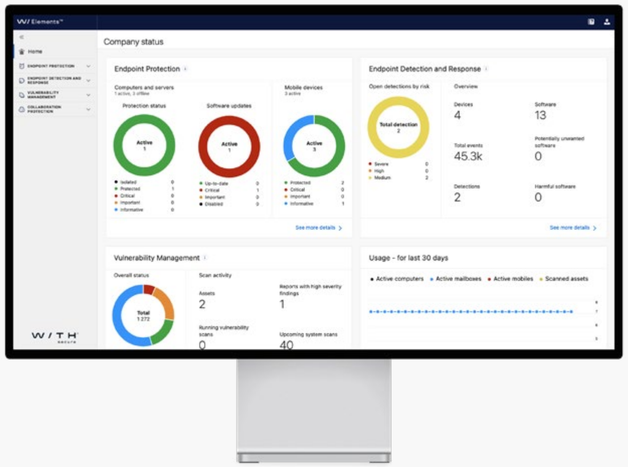
Mit WithSecure™ Elements Endpoint Protection können Sie die Sicherheit Ihrer Endpunkte über eine einzige, intuitive Konsole einfach bereitstellen, verwalten und überwachen. So haben Sie einen umfassenden Überblick über alle Ihre Geräte.

Bei der Entwicklung des Sicherheitscenters wurde von Grund auf darauf geachtet, das Sicherheitsmanagement in anspruchsvollen, geräte- und standortübergreifenden Umgebungen zu vereinfachen und zu beschleunigen. Nachfolgend finden Sie einige Beispiele dafür, wie die Lösung den Zeit- und Ressourcenaufwand für die Wartung und Verwaltung der Sicherheitslösung erheblich reduziert:

- Endpunkt-Clients erhalten automatisch Client-, Sicherheits- und Datenbank-Updates. Das minimiert den Zeitaufwand für Updates und Wartung.
- Durch die Bündelung der Sicherheitsverwaltung verschiedener Endpunkte und Tools in einem Portal wird die gesamte Verwaltung erheblich gestrafft und Zeit eingespart.
- Die Patchverwaltung kann so eingerichtet werden, dass fehlende Sicherheitspatches automatisch bereitgestellt werden, sobald sie verfügbar sind. So wird Zeit für manuelle Software-Updates gespart.
- Da es sich um einen gehosteten Dienst handelt, müssen Sie auf dem Server weder Hardware noch Software installieren oder Wartungsaufgaben übernehmen – ein Browser genügt.
- Das Portal wurde von einem eigens dafür eingesetzten User-Experience-Team entwickelt, um eine optimale Benutzerführung zu gewährleisten und die Effizienz der Bedienung zu steigern.

Die Kommunikation zwischen Konsole und Endpunkt erfolgt in Echtzeit. So können IT-Administratoren die Sicherheit der Umgebung ohne durch Abrufintervalle entstehende Unterbrechungen oder Verzögerungen verwalten und überwachen.

Im Wesentlichen ermöglicht dies IT-Administratoren, Änderungen in einem Arbeitsgang zu konfigurieren, bereitzustellen und zu validieren. Und falls sich ein Sicherheitsvorfall ereignet, der „sofort“ behoben werden muss, können Sie direkt eingreifen und Korrekturmaßnahmen einleiten.



Sie können individuelle Sicherheitsrichtlinien (Profile) erstellen und anpassen und diese Computern und Servern mittels Bezeichnungen entweder einzeln oder in Gruppen zuweisen. Sämtliche Einstellungen und Richtlinien können bei Bedarf bis auf die individuelle Ebene hinab durchgesetzt werden, sodass Endbenutzer keine Änderungen daran vornehmen können. Richtlinien können z. B. bezogen auf einzelne Active Directory-Gruppen erstellt werden. So werden die Richtlinien automatisch den Geräten der Gruppe zugewiesen.

Das Management-Portal bietet einen vollständigen Überblick über den Sicherheitsstatus Ihrer gesamten Umgebung. Dabei berücksichtigt werden potenzielle Schwachstellen in der Software, fehlende Sicherheits-Updates und der Status von Sicherheitsfunktionen wie Echtzeit-Scans und Firewall. Mit Security Events haben IT-Administratoren alle Alarme ganz einfach an einer zentralen Stelle im Blick.

Sie können z. B. die Anzahl der blockierten Infektionen verfolgen und sich stärker auf die am häufigsten angegriffenen Geräte konzentrieren. Sie können automatische E-Mail-Benachrichtigungen einrichten, sodass Sie bestimmten Infektionsparametern Ihre Aufmerksamkeit zuerst widmen können. Wenn Sie weitere Informationen über eine bestimmte Infektion benötigen, können Sie diese direkt in unserer Sicherheitsdatenbank abrufen.

Das Management-Portal liefert eine breite Palette von grafischen Berichten in einem intuitiven Format, sodass die Daten leichter und schneller zu erfassen und zu verstehen und damit für die Beteiligten besser nachvollziehbar sind. Die Sicherheitsdetails des Geräts können bei Bedarf auch als CSV-Dateien exportiert werden.

# 3. Schutz für Computer

Endpoint-Security ist der Eckpfeiler einer jeden sicheren Umgebung. Heute ist für die Sicherheit der Systeme von entscheidender Bedeutung, dass der Schutz den von herkömmlichen Anti-Malware-Lösungen weit übertrifft. Mit WithSecure™ Elements Endpoint Protection ist es einfach, leistungsstarke, ressourcenschonende Sicherheit für Windows-, Mac- und Linux-Computer bereitzustellen.

## 3.1 Der gesamte Endpunktschutz in einem Technologie-Stack

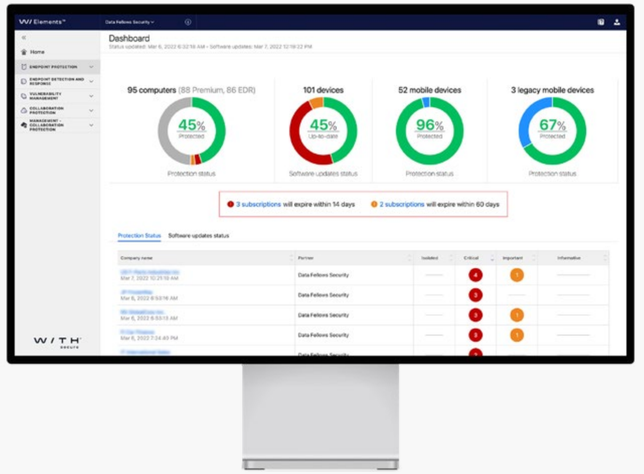
Moderne Softwarepakete für den Endpunktschutz verwenden einen mehrschichtigen Ansatz, um Sicherheit zu schaffen. Technologien wie Netzwerkfilter und Netzwerkscans, Verhaltensanalyse und URL-Filter ergänzen die traditionellen Komponenten für Dateiscans. Diese unterschiedlichen Schutzfunktionen werden in WithSecure™ Ultralight in einem mehrschichtigen System umgesetzt. Sollte eine Bedrohung eine Schicht umgehen, greift eine weitere Schicht, um die Bedrohung auszuschalten. Um sich Veränderungen der Bedrohungslage anzupassen, können Schichten entfernt oder neue Schichten hinzugefügt werden, sowohl auf den Endpunkten als auch in der Cloud.

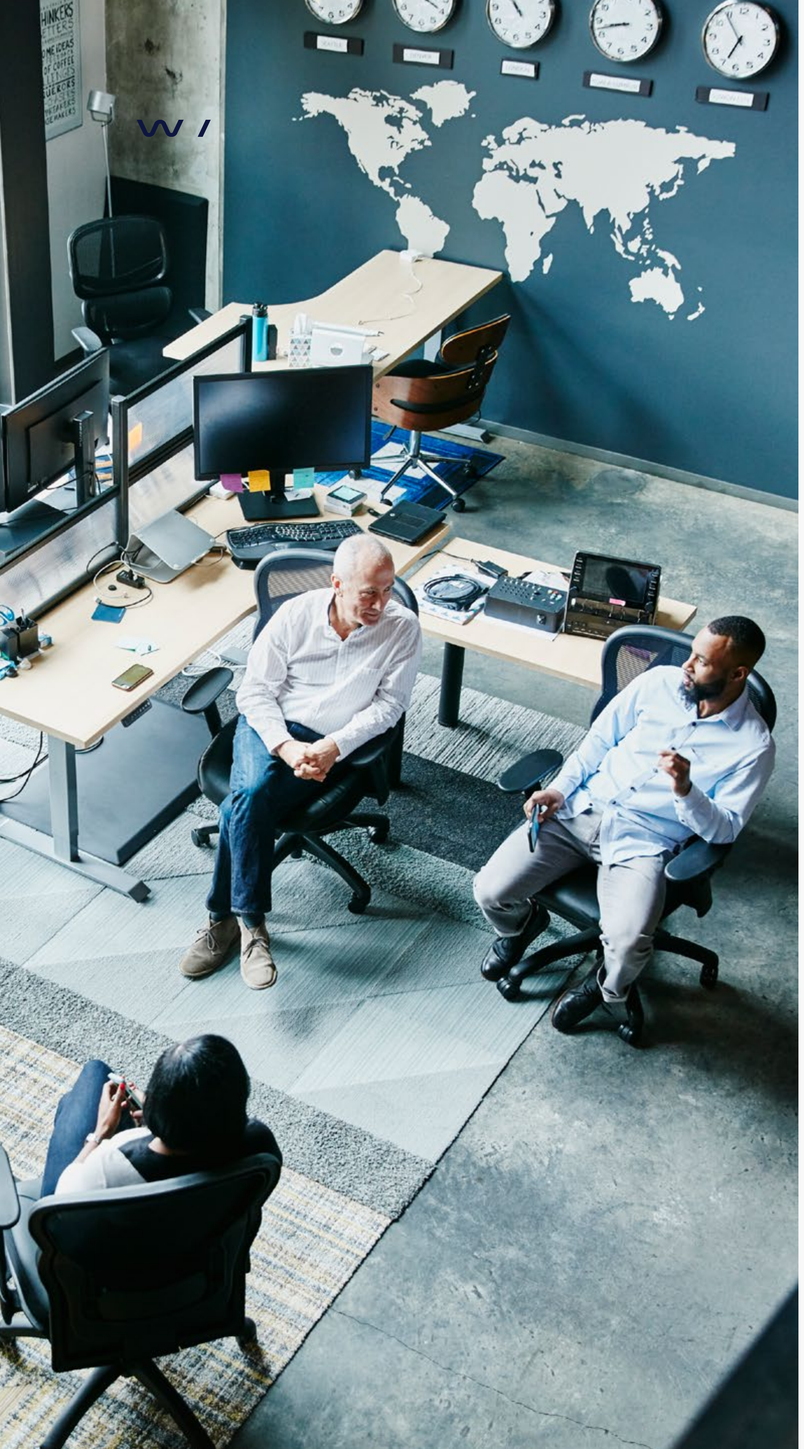
Ultralight vereint sämtliche Endpunktschutz-Technologien von WithSecure™ in einem einzigen Paket. Es umfasst eine Reihe von Treibern, Engines und Systemdiensten, die Mechanismen zum Schutz eines Geräts und seiner Benutzer bereitstellen. Ultralight bietet herkömmliche Antiviren-Funktionen wie Echtzeit-Scans von Dateien und Netzwerken. Darüber hinaus bietet es proaktive Schutztechnologien, die darauf abzielen, Zero-Day-Exploits zu stoppen und selbst neuartigen Angriffen zu entgehen. Die WithSecure™ Security Cloud versorgt Ultralight-Komponenten mit Echtzeitinformationen über jegliche Änderungen der Bedrohungslage.

Ausführlichere Informationen zu den integrierten Schutztechnologien von Ultralight finden Sie im einschlägigen technischen Whitepaper.

## 3.2 Heuristische und verhaltensbasierte Bedrohungsanalyse

Die heuristische und verhaltensbasierte Bedrohungsanalyse von DeepGuard ist für das Erkennen und Blockieren der heute verbreiteten, komplexen Malware-Bedrohungen von entscheidender Bedeutung. DeepGuard bietet sofortigen, proaktiven Schutz auf dem Host vor neuen und im Entstehen begriffenen Bedrohungen, indem es sich auf bösartige Verhaltensweisen von Anwendungen konzentriert und nicht auf das statische Identifizieren spezifischer, bereits bekannter Bedrohungen.







Durch diese Schwerpunktverlagerung lässt sich bisher unbekannte Malware allein aufgrund ihres Verhaltens identifizieren und blockieren. So bleiben Systeme geschützt, bis die Sicherheitsforscher in der Lage sind, diese spezielle Bedro-hung zu analysieren und eine Erkennung zu veröffentlichen.

Durch die Kommunikation mit der WithSecure™ Security Cloud kann DeepGuard zudem anhand der neuesten verfügbaren Informationen über Reputation und Prävalenz für jedes zuvor gefundene Objekt seine Sicherheitsbewertungen verfeinern. So werden das Risiko von Fehlalarmen oder redundanten Analysen und damit Störfaktoren für den Benutzer reduziert.

Die Verhaltensanalyse auf dem Host umfasst auch das Abfangen von Angriffen, die Schwachstellen in gängigen Programmen auszunutzen versuchen, um Malware auf den Rechner zu schleusen. DeepGuard kann Routinen erkennen und blockieren, die für Exploit-Versuche charakteristisch sind, um deren Ausnutzung – und damit Infektionen – zu verhindern. Das Abfangen von Exploits bewahrt Benutzer vor Schaden, selbst wenn anfällige Programme auf ihrem Rechner vorhanden sind.

Weitere Informationen über die von DeepGuard durchgeführte heuristische und verhaltensbasierte Bedrohungsanalyse finden Sie im einschlägigen technischen Whitepaper.

## 3.3 Informationen über Bedrohungen in Echtzeit

Der Sicherheits-Client nutzt Informationen über Bedrohungen in Echtzeit, die von der WithSecure™ Security Cloud bereitgestellt werden. So wird sichergestellt, dass alle neuen oder im Entstehen begriffenen Bedrohungen innerhalb von Minuten identifiziert, analysiert und abgewehrt werden.

Ein cloudbasierter Dienst zur Bedrohungsanalyse bietet viele Vorteile gegenüber herkömmlichen Ansätzen. WithSecure™ sammelt Informationen über Bedrohungen von vielen Millionen Client-Knotenpunkten und zeichnet so ein Echtzeitbild der globalen Bedrohungslage.

Wenn etwa eine heuristische und verhaltensbasierte Bedrohungsanalyse einen Zero-Day-Angriff auf einem anderen Endpunkt am gegenüberliegenden Ende der Welt identifiziert, werden die Informationen über die Security Cloud an alle geschützten Geräte übermittelt – und machen den komplexen Angriff bereits wenige Minuten nach der ersten Erkennung unschädlich.

Weitere Informationen zu den Funktionen und Vorteilen der WithSecure™ Security Cloud finden Sie in unserem technischen Whitepaper.

## 3.4 Speziell für macOS entwickelt

WithSecure™ Computer Protection für macOS beinhaltet XFENCE, eine einzigartige Sicherheitskomponente für den Mac. Das Produkt nutzt die modernen Sicherheitsfunktionen von macOS, um den Schutz vor Malware, Trojanern, Hintertüren, Anwendungen mit schädlichem Verhalten und anderen Bedrohungen zu verbessern, ohne die Benutzerfreundlichkeit oder Leistung zu beeinträchtigen. Der leistungsstarke XFENCE-Schutz verhindert, dass fehlerhafte Prozesse, Ransomware und andere Malware ohne ausdrückliche Zustimmung auf Ihre Dateien und Systemressourcen zugreifen.

WithSecure™ Computer Protection für macOS nutzt hochmoderne, regelbasierte Analysen, um Apps zu überwachen, die auf vertrauliche Dateien und Systemressourcen zurückgreifen versuchen. Zudem minimieren die über die Security Cloud bereitgestellten Informationen über Bedrohungen Fehlalarme, und Benutzer können sich über Eingabeaufforderungen leicht zum Zulassen oder Ablehnen entscheiden.

Darüber hinaus bietet WithSecure™ Computer Protection für macOS eine Firewall für die Anwendungsschicht, die den Netzwerkzugriff auf Anwendungsebene konfigurieren und kontrollieren kann. Es kann verwendet werden, um Hosts zu isolieren, den Zugriff auf das Netzwerk nur für vertrauenswürdige, signierte Anwendungen zuzulassen und Anwendungen anhand der Paket-ID auf eine Blockierliste bzw. Zulassliste zu setzen.

WithSecure™ Computer Protection für macOS wird mit Administrator-Tools für die einfache Bereitstellung und Verwaltung der Mac-Clients geliefert.

## 3.5 Schutz für Linux-Clients

WithSecure™ Elements Endpoint Protection umfasst Schutz für Linux mit WithSecure™ Server Protection. Das Produkt kann auch zum Schutz von Endgeräten verwendet werden.

## 3.6 Integrierte Patchverwaltung

Windows-Systeme verfügen über eine automatisierte, vollständig in die Clients integrierte Patchverwaltung. Eine Installation separater Agenten, Verwaltungsserver oder Konsolen ist nicht erforderlich.

Dazu wird nach fehlenden Updates gescannt, ein Schwachstellenbericht unter Berücksichtigung der fehlenden Patches erstellt, die anschließend automatisch heruntergeladen und bereitgestellt werden. Bei Bedarf können Sie Updates auch manuell installieren. Die Sicherheitspatches umfassen Microsoft-Updates und über 2500 Anwendungen von Drittanbietern wie Flash, Java, OpenOffice und weitere mehr, die aufgrund ihrer Popularität und der größeren Anzahl von Schwachstellen beliebte Angriffsvektoren darstellen.

Administratoren können detaillierte Ausschlüsse für den automatischen Modus basierend auf Software-Namen oder Bulletin-IDs definieren. Einige Updates sind definitionsgemäß ausgeschlossen, z. B. Service Packs. Administratoren können zudem flexibel festlegen, an welchem Tag und zu welcher Uhrzeit Installationen durchgeführt werden sollen, wie Neustarts erzwungen werden und welche Toleranzperiode vor dem Erzwingen eines Neustarts nach der Installation verstreichen soll.

Die Patchverwaltung ist eine wichtige Sicherheitskomponente. Sie stellt die erste Schutzschicht dar, wenn bösartige Inhalte auf die Endpunkte gelangen, und kann bis zu 80 % der Angriffe abwehren, indem es einfach Software-Sicherheitsupdates installiert, sobald diese zur Verfügung gestellt werden.

## 3.7 Anti-Malware-Schutz mit mehren Engines

Unsere Komponente für Computer nutzt eine proprietäre, Sicherheitsplattform mit mehreren Engines zur Erkennung und Abwehr von Malware. Sie bietet gegenüber herkömmlichen, signaturbasierten Technologien einen überlegenen Schutz:

- Sie erkennt ein breiteres Spektrum an bösartigen Charakteristika, Mustern und Trends und ermöglicht so eine zuverlässigere und präzisere Erkennung, selbst bei bisher unbekannten Malware-Varianten.
- Durch die Verwendung von Echtzeit-Überprüfungen mittels WithSecure™ Security Cloud kann das System schneller auf neue und im Entstehen begriffene Bedrohungen reagieren und schont gleichzeitig Ressourcen.
- Die Emulation ermöglicht die Erkennung von Malware, die Verschleierungstechniken einsetzt. Damit stellt sie eine zusätzliche Sicherheitsschicht dar, die eine Datei passieren muss, bevor sie ausgeführt werden kann.

## 3.8 Standortbezogene Profile

WithSecure™ Elements Endpoint Protection kann so konfiguriert werden, dass je nach Standort des Endpunkts unterschiedliche Konfigurationen zum Einsatz kommen. Der Administrator kann die Netzwerkstandorte und -regeln beispielsweise so einrichten, dass die Patchverwaltung und die Firewall bei einem Gerät eingeschaltet sind, wenn es zu Hause genutzt wird, im Büro jedoch sowohl Patchverwaltung als auch Firewall des Geräts ausgeschaltet sind.

## 3.9 Flexibilität durch Zuweisung automatisierter Tasks

WithSecure™ Elements Endpoint Protection kann so konfiguriert werden, dass bestimmte automatisierte Tasks sehr granular ausgeführt werden. Produkt-Updates können beispielsweise so konfiguriert werden, dass sie zu einem bestimmten Zeitpunkt ausgeführt werden, dass fehlende kritische und andere Sicherheits-Updates sofort installiert werden, dass an jedem Tag nach fehlenden Sicherheits-Updates gescannt wird und dass an jedem Wochentag ein vollständiger Systemscan auf Malware durchgeführt wird. Mit den automatisierten Tasks können Sie den Endpunktschutz so konfigurieren, dass er den Sicherheitsanforderungen Ihres Unternehmens entspricht, ohne die Leistung zu beeinträchtigen.

## 3.10 Umfassender und proaktiver Webschutz

Darüber hinaus bietet die Lösung umfassenden und proaktiven Webschutz, der sicherstellt, dass der meistgenutzte Angriffsvektor bestmöglich verteidigt wird.

- Die Lösung verhindert proaktiv den Zugriff auf bösartige Websites und Phishing-Websites, noch bevor diese aufgerufen werden (z. B. bei der Google-Suche und beim Klicken auf einen Weblink). Dies ist besonders effektiv, da ein frühzeitiges Eingreifen das Gefahrenpotenzial durch bösartige Inhalte und damit Angriffe erheblich reduziert.
- Sie verhindert die Ausnutzung aktiver Inhalte wie Java und Flash, die bei den allermeisten Online-Angriffe verwendet werden. Diese Komponenten werden automatisch auf unbekannten und verdächtigen Websites gemäß ihren Reputationsdaten blockiert. Dabei besteht die Möglichkeit, Ausschlüsse festzulegen.
- Die Lösung kann ebenfalls eingesetzt werden, um die unangemessene Nutzung des Internets einzuschränken, indem der Zugriff auf nicht arbeitsrelevante Ziele wie soziale Netzwerke und Websites mit nicht jugendfreien Inhalten granular verweigert oder zugelassen wird. So können die Effizienz maximiert und bösartige Websites vermieden werden.

- Nachdem der HTTP-Web-Datenverkehr die ersten Schichten des Webschutzes passiert hat, wird auch dessen Inhalt einer Analyse unterzogen, um zusätzlichen Schutz vor Malware zu bieten, bevor die Daten dem Endpunkt zugestellt werden.
- IT-Administratoren können außerdem festlegen, dass geschäftskritische Web-Aktivitäten, die HTTPS nutzen (wie Intranets oder sensible Clouddienste, z. B. CRMs), eine zusätzliche Sicherheitsschicht verwenden. Wenn er aktiv ist, beendet er alle nicht vertrauenswürdigen Netzwerkverbindungen und verhindert so Angriffe sowie das Abgreifen von Daten von den während der Sitzung genutzten Diensten.

Die Sicherheitsfunktionen hängen vom jeweiligen Betriebssystem ab. Nachfolgend finden Sie einen Vergleich der Funktionen unter Windows, macOS und Linux.

| | Windows | macOS | Linux |
|---|---|---|---|
| **Sicherheit** | | | |
| Anti-Malware | **Ja** | **Ja** | **Ja** |
| DeepGuard | **Ja** | Nein | Nein |
| DataGuard | **Ja** | **Ja*** | Nein |
| Sicherheitscloud | **Ja** | **Ja** | **Ja** |
| Patchverwaltung | **Ja** | Nein | Nein |
| Anwendungssteuerung | **Ja** | Nein | Nein |
| Browserschutz | **Ja** | **Ja** | Nein |

| | Windows | macOS | Linux |
|---|---|---|---|
| **Sicherheit** | | | |
| Webdatenverkehr-Scan | **Ja** | Nein | Nein |
| Webinhaltssteuerung | **Ja** | **Ja** | Nein |
| Inhaltstypfilterung | **Ja** | Nein | Nein |
| Verbindungssteuerung | **Ja** | **Ja** | Nein |
| Firewall | **Ja** | **Ja** | Nein |
| Integritätsprüfung | Nein | Nein | **Ja** |
| Endpunktverschlüsselung | **Ja** | Nein | Nein |

* Teil der von XFENCE bereitgestellten Funktionalität

# 4. Schutz für Mobilgeräte

Jederzeit die Kontrolle über Mobilgeräte zu haben ist ein grundlegender Aspekt moderner Cybersicherheit. Elements Mobile Protection bietet IT-Administratoren eine einfache Möglichkeit, Mobilgeräte, sowohl unter Android als auch unter iOS, zu sichern und zu kontrollieren.

Die Komponente WithSecure™ Elements Mobile Protection bietet alles, was herausragenden Schutz für Mobilgeräte ausmacht – in einem Paket: persönliches VPN, WLAN-Sicherheit und proaktiven App-Schutz (Android) sowie Webschutz.

Der Client für Mobilgeräte ist dabei so konzipiert, dass er MDM-Lösungen von Drittanbietern ergänzen und von diesen bereitgestellt werden kann.

## 4.1 VPN für Mobilgeräte

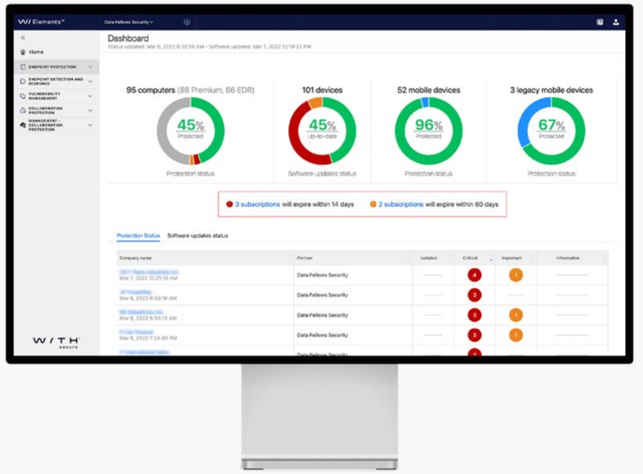
Das mobile VPN verschlüsselt automatisch den Datenverkehr zwischen Ihrem Mobilgerät und einem ausgewählten WithSecure™-Serviceknoten, sodass Ihre Mitarbeiter öffentliche WLANs und mobile Netzwerke sicher nutzen können.

Es verhindert das Abfangen von E-Mails, Browser-Sitzungen, die Nutzung von Onlinediensten und es legt eine zusätzliche Sicherheitsschicht über HTTPS-Verbindungen. Außerdem können Sie damit Ihren virtuellen Standort ändern, Ihre IP-Adresse verbergen und im Ausland auf Dienste zu Hause zugreifen.

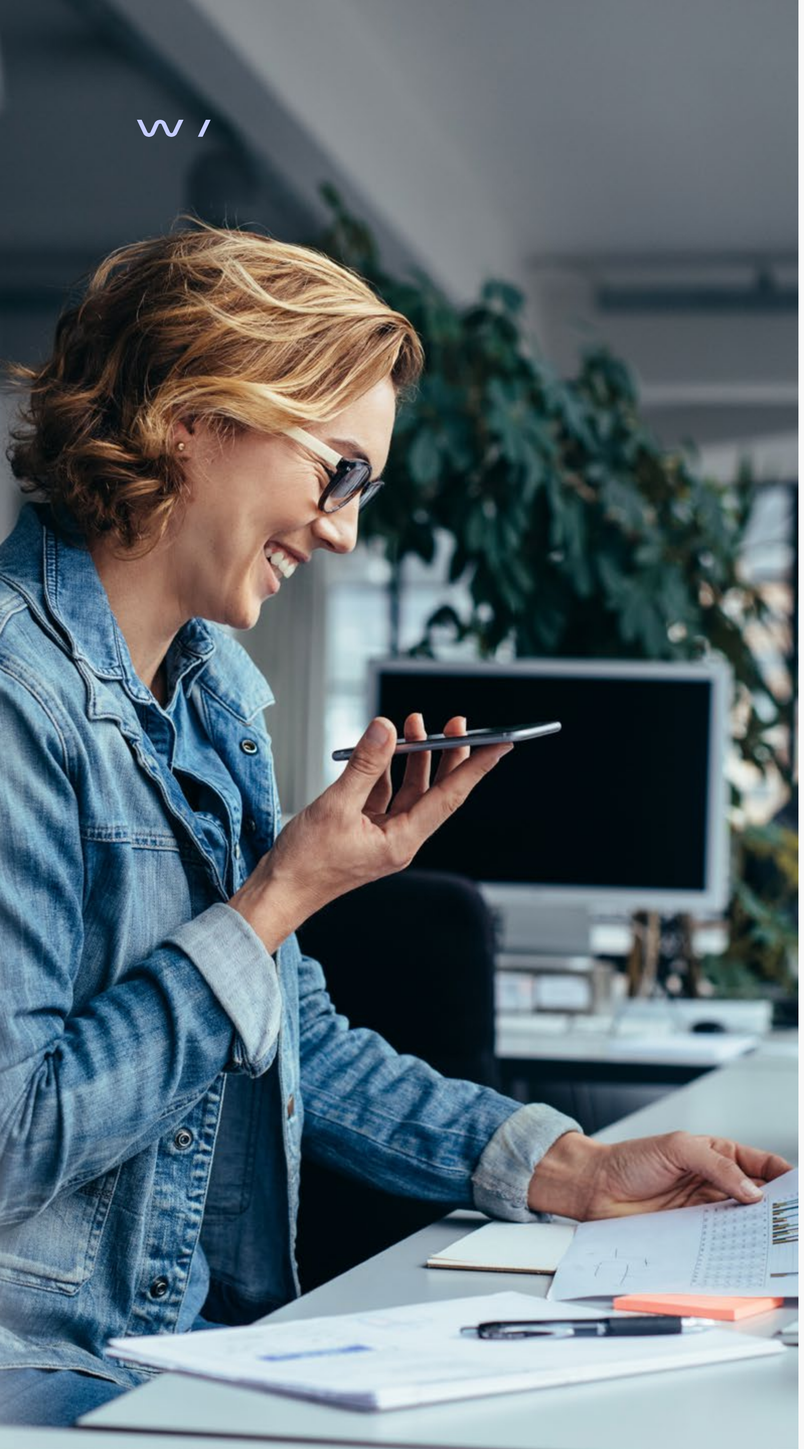
## 4.2 Security Cloud

Der Sicherheits-Client nutzt Informationen über Bedrohungen in Echtzeit, die von der WithSecure™ Security Cloud bereitgestellt werden. So wird sichergestellt, dass alle neuen oder im Entstehen begriffenen Bedrohungen innerhalb von Minuten identifiziert, analysiert und abgewehrt werden.

Ein cloudbasierter Dienst zur Bedrohungsanalyse bietet viele Vorteile gegenüber herkömmlichen Ansätzen. Wir sammeln Informationen über Bedrohungen von vielen Millionen Devices und zeichnen so ein Echtzeitbild der globalen Bedrohungslage. Wenn z. B. eine APK oder Datei heruntergeladen wird, wird sie gescannt und ihre Reputation in der Sicherheitscloud überprüft. Bösartige Dateien werden an der Ausführung gehindert und unbekannte Dateien oder Anwendungen werden zu einer eingehenderen Analyse hochgeladen. Die Scanergebnisse kommen allen Benutzern zugute, indem z. B. Fehlalarme minimiert und neue Angriffe innerhalb von Minuten vereitelt werden.




Weitere Informationen zu den Funktionen und Vorteilen der WithSecure™ Security Cloud finden Sie in unserem technischen Whitepaper.





## 4.3 Schutz für Anwendungen

Bei aktiver VPN-Verbindung werden Mobilgeräte automatisch vor Malware und bösartigen Inhalten geschützt. Die WithSecure™-Serviceknoten scannen den Datenverkehr auf Netzwerkebene und schöpfen dabei die Sicherheitsanalyse in vollem Umfang aus. Dadurch können wir eine bessere Sicherheit bieten als herkömmliche Lösungen für die Sicherheit von Mobilgeräten:

- Die Sicherheit wird nicht durch die begrenzten Ressourcen von Mobilgeräten eingeschränkt.
- Ressourcenlastige Prozesse beeinträchtigen die Leistung des Geräts und die Lebensdauer des Akkus nicht.
- Scanvorgänge auf Netzwerkebene verhindern von vornherein den Kontakt mit bösartigen Inhalten.

Bei Android-Geräten wird die Sicherheit durch lokale Scanvorgänge, einschließlich Echtzeit-Reputationsprüfungen über die WithSecure™ Security Cloud, weiter erhöht – selbst wenn das VPN nicht verbunden ist.

## 4.4 Browser-Schutz

Der Browserschutz stellt eine elementare Sicherheitsschicht dar, die proaktiv verhindert, dass Endbenutzer bösartige Websites aufrufen. Dies ist besonders effektiv, da ein frühzeitiges Eingreifen das Gefahrenpotenzial durch bösartige Inhalte – und damit Angriffe erheblich reduziert.

Der Browser-Schutz verhindert beispielsweise, dass Endbenutzer dazu verleitet zu werden, scheinbar legitime Phishing-Websites aufzurufen, über einen E-Mail-Link auf bösartige Websites zu gelangen oder sich über bösartige Werbung von Drittanbietern auf eigentlich legitimen Websites zu infizieren.

## 4.5 Schnelleres Surfen und geringerer Datenverbrauch

Diese Komponente ist auf eine minimale Beeinträchtigung der mobilen Leistung und der Akkulaufzeit hin ausgelegt. Durch die Komprimierung des Datenverkehrs über VPN und die Verhinderung von Online-Tracking und Werbung durch Anti-Tracking wird die Surfgeschwindigkeit sogar noch erhöht.

## 4.6 Bereitstellung mit Drittanbieter-MDM

Der Client für Mobilgeräte ist dabei so konzipiert, dass er von Lösungen zur Mobilgeräteverwaltung (MDM) von Drittanbietern wie AirWatch, MobileIron, Intune und MaaS360 ergänzt und bereitgestellt werden kann.

Durch den zusätzlichen Einsatz einer speziellen Sicherheitskomponente zur Ergänzung der grundlegenden Funktionen der MDM-Lösung können IT-Administratoren die Sicherheit in Bezug auf Malware, Datendiebstahl und Phishing-Versuche, die auf Mobilgeräte abzielen, deutlich steigern.

# 5. Schutz für Server

Server sind für die Kommunikation, die Zusammenarbeit und die Datenspeicherung in einem Unternehmen von entscheidender Bedeutung. Elements Endpoint Protection sorgt für die Sicherheit von Servern und ermöglicht es ihnen, mit maximaler Leistung zu arbeiten. Die Lösung bietet Sicherheit für Windows-, Citrix- und Linux-Server.

Im Folgenden finden Sie einen Überblick über die grundlegenden Funktionen für verschiedene Plattformen:

| | Windows | Citrix | Linux |
|---|---|---|---|
| **Grundlegende Sicherheit** | | | |
| Anti-Malware | **Ja** | **Ja** | **Ja** |
| DeepGuard | **Ja** | **Ja** | Nein |
| Sicherheitscloud | **Ja** | **Ja** | **Ja** |
| Patchverwaltung | **Ja** | **Ja*** | Nein |
| Browserschutz | **Ja** | **Ja** | Nein |
| Webdatenverkehr-Scan | **Ja** | **Ja** | Nein |
| Firewall | **Ja** | Nein | Nein |
| Integritätsprüfung | Nein | Nein | **Ja** |
| **Remoteverwaltung über das Portal** | | | |
| Sicherheitsverwaltung | **Ja** | **Ja** | **Ja** |
| Sicherheitsüberwachung | **Ja** | **Ja** | **Ja** |

## 5.1 Heuristische und verhaltensbasierte Bedrohungsanalyse

Die heuristische und verhaltensbasierte Bedrohungsanalyse von DeepGuard ist für das Erkennen und Blockieren der heute verbreiteten, komplexen Malware-Bedrohungen von entscheidender Bedeutung. Der DeepGuard schützt die Systeme proaktiv vor aktuellen und zukünftigen Bedrohungen. Dabei analysiert er das Verhalten der Anwendungen und ist nicht auf eine signaturbasierte Erkennung angewiesen. Durch diese Schwerpunktverlagerung lässt sich bisher unbekannte Malware allein aufgrund ihres Verhaltens identifizieren und blockieren. So bleiben Systeme geschützt, bis die Sicherheitsforscher in der Lage sind, diese spezielle Bedrohung zu analysieren und eine Erkennung zu veröffentlichen.

Durch die Kommunikation mit der WithSecure™ Security Cloud kann DeepGuard zudem anhand der neuesten verfügbaren Informationen über Reputation und Prävalenz für jedes zuvor gefundene Objekt seine Sicherheitsbewertungen verfeinern. So werden das Risiko von Fehlalarmen oder redundanten Analysen und damit Störfaktoren für den Benutzer reduziert. Die Verhaltensanalyse auf dem Host umfasst auch das Abfangen von Angriffen, die Schwachstellen in gängigen Programmen auszunutzen versuchen, um Malware auf den Rechner zu schleusen. DeepGuard kann Routinen erkennen und blockieren, die für Exploit-Versuche charakteristisch sind, um deren Ausnutzung – und damit Infektionen – zu verhindern.

Das Abfangen von Exploits bewahrt Benutzer vor Schaden, selbst wenn anfällige Programme auf ihrem Rechner vorhanden sind.

Weitere Informationen über die von DeepGuard durchgeführte heuristische und verhaltensbasierte Bedrohungsanalyse finden Sie im einschlägigen technischen Whitepaper.

## 5.2 Informationen über Bedrohungen in Echtzeit

Der Sicherheits-Client nutzt Informationen über Bedrohungen in Echtzeit, die von der WithSecure™ Security Cloud bereitgestellt werden. So wird sichergestellt, dass alle neuen oder im Entstehen begriffenen Bedrohungen innerhalb von Minuten identifiziert, analysiert und abgewehrt werden.

Ein cloudbasierter Dienst zur Bedrohungsanalyse bietet viele Vorteile gegenüber herkömmlichen Ansätzen. WithSecure™ sammelt Informationen über Bedrohungen von vielen Millionen Devices und zeichnet so ein Echtzeitbild der globalen Bedrohungslage. Wenn etwa eine heuristische und verhaltensbasierte Bedrohungsanalyse einen Zero-Day-Angriff auf einem anderen Endpunkt am gegenüberliegenden Ende der Welt identifiziert, werden die Informationen über die Security Cloud an alle geschützten Geräte übermittelt – und machen den komplexen Angriff bereits wenige Minuten nach der ersten Erkennung unschädlich.

Weitere Informationen zu den Funktionen und Vorteilen der WithSecure™ Security Cloud finden Sie in unserem technischen Whitepaper.

## 5.3 Integrierte Patchverwaltung

Die Komponente verfügt über eine automatisierte und vollständig in Windows Server-Clients integrierte Patchverwaltung. Eine Installation separater Agenten, Verwaltungsserver oder Konsolen ist nicht erforderlich.

Dazu wird nach fehlenden Updates gescannt, ein Schwachstellenbericht unter Berücksichtigung der fehlenden Patches erstellt, die anschließend automatisch heruntergeladen und bereitgestellt werden. Bei Bedarf können Sie Updates auch manuell installieren. Die Sicherheitspatches umfassen Microsoft-Updates und über 2500 Anwendungen von Drittanbietern wie Flash, OpenOffice und weitere mehr, die aufgrund ihrer Popularität und der größeren Anzahl von Schwachstellen beliebte Angriffsvektoren darstellen.

## 5.4 Anti-Malware-Schutz mit mehren Engines

Unsere Komponente für Computer nutzt eine proprietäre, Sicherheitsplattform mit mehreren Engines zur Erkennung und Abwehr von Malware. Sie bietet gegenüber herkömmlichen signaturbasierten Technologien einen überlegenen Schutz:

- Sie erkennt ein breiteres Spektrum an bösartigen Charakteristika, Mustern und Trends und ermöglicht so eine zuverlässigere und präzisere Erkennung, selbst bei bisher unbekannten Malware-Varianten.
- Durch die Verwendung von Echtzeit-Überprüfungen mittels WithSecure™ Security Cloud kann das System schneller auf neue und im Entstehen begriffene Bedrohungen reagieren und schont gleichzeitig Ressourcen.
- Die Emulation ermöglicht die Erkennung von Malware, die Verschleierungstechniken einsetzt. Damit stellt sie eine zusätzliche Sicherheitsschicht dar, die eine Datei passieren muss, bevor sie ausgeführt werden kann.

## 5.5 Proaktiver Webschutz

Darüber hinaus bietet die Lösung umfassenden und proaktiven Webschutz für Terminals, der sicherstellt, dass dieser meistgenutzte Angriffsvektor bestmöglich verteidigt wird.

- Die Lösung verhindert proaktiv den Zugriff auf bösartige Websites und Phishing-Websites, noch bevor diese aufgerufen werden. Dies ist besonders effektiv, da ein frühzeitiges Eingreifen das Gefahrenpotenzial durch bösartige Inhalte und damit Angriffe erheblich reduziert.
- Nachdem der Web-Datenverkehr (HTTP) die erste Schicht des Webschutzes passiert hat, wird auch dessen Inhalt einer Analyse unterzogen, um zusätzlichen Schutz vor Malware zu bieten, bevor die Daten dem Endpunkt zugestellt werden.

## 5.6 Schutz für Serverfreigaben

Die gemeinsame Nutzung von Dateien auf lokalen Dateiservern bedeutet für Organisationen das Risiko von Ransomware-Angriffen, insbesondere dann, wenn Geräte, die nicht unter der vollständigen Kontrolle der Organisation stehen, auf die Serverfreigaben zugreifen, um große Mengen wichtiger Dateien zu verschlüsseln und unbrauchbar zu machen.

Sie können Windows-Dateifreigaben weiter sicher nutzen, indem Sie den Serverfreigabe-Schutz als zusätzlichen Schutz gegen Ransomware einsetzen. Dieser ist darauf ausgelegt, jegliche Verschlüsselung oder anderweitige, auch unbeabsichtigte, Zerstörung von Dateien sofort zu erkennen, rückgängig zu machen und Ihre Organisation vor einem Ausbreiten der Ransomware zu schützen.

## 5.7 Citrix und Terminalserver

Ergänzend zu denselben grundlegenden Sicherheitsfunktionen wie für Windows-Server bietet die Citrix-Komponente zusätzlichen Schutz für Citrix-Umgebungen, indem sie die integrierten Funktionen zur Patchverwaltung für veröffentlichte Anwendungen erweitert. Da der Client Citrix Ready-zertifiziert ist, läuft er in Citrix-Umgebungen einwandfrei. In gleicher Weise bietet Server Protection Schutz für Windows Terminalserver. Beachten Sie, dass Kunden, die Server Protection in Remotedesktopumgebungen einsetzen, auch eine Lizenz für WithSecure™ Remote Desktop Protection benötigen.

## 5.8 Linux

Linux Protection bietet grundlegende Sicherheitsfunktionen für Linux-Clients: Echtzeit-Scans bei Dateizugriff mit mehreren Engines, nach Zeitplan und manuell ausgeführte Scanvorgänge sowie Integritätsprüfungen. Es ist darauf ausgelegt, sowohl Windows- als auch Linux-basierte Angriffe zu erkennen und zu verhindern. Das macht es besonders wertvoll in gemischten Umgebungen, in denen ein ungeschützter Linux-Rechner als einfacher Angriffsvektor genutzt werden kann.

## 5.9 Anti-Malware-Schutz mit mehren Engines

Die Clients nutzen eine proprietäre, Sicherheitsplattform mit mehreren Engines zur Erkennung und Verhinderung von Malware. Sie bietet gegenüber herkömmlichen signaturbasierten Technologien einen überlegenen Schutz mit dem zusätzlichen Vorteil technologischer Unabhängigkeit. Die Plattform erkennt ein breiteres Spektrum an bösartigen Charakteristika, Mustern und Trends und ermöglicht so eine zuverlässigere und präzisere Erkennung, selbst bei bisher unbekannten Malware-Varianten.

## 5.10 Integritätsprüfung

Die Komponente verfügt über eine interne Integritätsprüfung, die Erkennungen vornimmt und Angreifer daran hindert, den Kernel, Systemdateien oder Konfigurationen zu manipulieren. Dies ist eine elementare Sicherheitsfunktion, da sie das System vor unbefugten Änderungen schützt, die anderweitig unbemerkt bleiben könnten.

Die Integritätsprüfung kann so konfiguriert werden, dass der Administrator bei jedem Versuch, die überwachten Dateien zu ändern, benachrichtigt wird. Unerlaubte Änderungen können dadurch leicht erkannt werden, sodass bei einem Vorfall sofort reagiert werden kann. Wenn Änderungen an der Baseline erforderlich sind, z. B. aufgrund von Updates an dem Betriebssystem, den Sicherheitskomponenten oder der Software, können Administratoren ein geschütztes Installationstool verwenden, um die erforderlichen Updates problemlos durchzuführen. Vorteil technologischer Unabhängigkeit. Die Plattform erkennt ein breiteres Spektrum an bösartigen Charakteristika, Mustern und Trends und ermöglicht so eine zuverlässigere und präzisere Erkennung, selbst bei bisher unbekannten Malware-Varianten.

# 6. Integration mit SIEM/RMM

WithSecure™ Elements Endpoint Protection kann mit WithSecure™ Elements Connector vollständig in ein SIEM-, ein RMM-System oder ein anderes Tool zur Berichterstellung oder Verwaltung integriert werden. Unter anderem in Tools von Kaseya, Tableau, N-Able, Splunk und viele weitere.

Die Integration trägt dazu bei, die vorhandenen Investitionen einer Organisation zu nutzen und von den Vorteilen zentraler Tools zu profitieren, z. B. durch die Optimierung der Tätigkeiten des Administrators im Zusammenhang mit der Sicherheit und der Reaktion auf Vorfälle.

Die Nutzung der Fähigkeiten von SIEM/RMM-Systemen ermöglicht die Integration z. B. die Erstellung zusätzlicher automatisierter, benutzerdefinierter Arbeitsabläufe und Berichte, wodurch der Arbeitsaufwand weiter reduziert und die Lösung für die spezifischen Bedürfnisse Ihrer Organisation optimiert wird. Der Umfang der Integration kann flexibel an Ihren tatsächlichen Bedarf angepasst werden, da jeder Vorgang einzeln über die API-Aufrufe abgerufen werden kann. IT-Administratoren können sich z. B. dafür entscheiden, nur relevante Daten an ein Berichterstellungs-, Protokollierungs- oder Auditsystem zu übermitteln, anstatt auch die Verwaltungsfunktionen zu integrieren.

Die Integration erfolgt über eine REST-API, die WithSecure™ Management API. Sie ermöglicht den Zugriff auf alle im Management-Portal verfügbaren Vorgänge und Daten.

Weitere Informationen über die Management-API sowie die SIEM/RMM-Integration finden Sie in der Beschreibung der Management-API unter connect.withsecure.com.

# 7. Professionelle Dienstleistungen

Die zusätzlichen Support-Pakete von WithSecure™ stellen ein Dienstleistungsangebot für flexiblere und umfassendere Unterstützung durch den Support dar. Unser Support steht Ihnen während der Geschäftszeiten oder sogar rund um die Uhr zur Verfügung. Wir bieten Ihnen erweiterten Support oder Premium-Support verschiedener Dienstleistungsstufen gemäß Ihren Bedürfnissen.

| Erweitert | Premium |
|---|---|
| **Ortsübliche Geschäftszeiten** (Deutsch, Finnisch, Französisch, Deutsch, Japanisch und Schwedisch) | **Rund um die Uhr** (Englisch) |
| Vorrangiger Zugang zu technischem Support | Reaktion auf kritische Vorfälle innerhalb einer Stunde |
| Online-Tools für Tickets und Nachverfolgung | Eskalation auf Managementebene |
| Anruf und Rückruf | Beratung zu Upgrades |
| Chat und Fernzugriff | Ratschläge zur Entfernung von Malware |

# 8. Datensicherheit

Die WithSecure™ Elements Endpoint Protection-Plattform nutzt Amazon Web Services (AWS). Dadurch können wir eine hohe Verfügbarkeit und Fehlertoleranz gewährleisten, die Reaktionszeiten verbessern und die Skalierbarkeit steigern. Die derzeit verfügbaren geografischen Regionen sind Europa, Nordamerika und Asien-Pazifik.

AWS gibt an, dass jedes seiner Rechenzentren den Tier 3+ Richtlinien entspricht. Weitere Informationen zu den AWS-Rechenzentren finden Sie unter:
https://aws.amazon.com/de/compliance/

WithSecure™ erfüllt die Datenschutzbestimmungen und -verordnungen in allen Ländern, in denen es tätig ist.

Wir nehmen die Sicherheit unserer Rechenzentren sehr ernst und schützen sie durch zahlreiche Sicherheitsvorkehrungen, wie z. B.:

- **Security by Design:** Unsere Systeme sind von Grund auf auf Sicherheit ausgelegt. Wir berücksichtigen Datenschutz und Sicherheit schon bei der Entwicklung unserer Technologien und Systeme, von den frühen Phasen der Konzeption und des Designs an bis hin zur Implementierung und zum Betrieb.
- **Strenge Zugriffssteuerungen:** Nur eine kleine, streng überprüfte Gruppe von WithSecure™-Mitarbeitern hat Zugang zu den Kundendaten. Zugriffsberechtigungen und -ebenen werden in strenger Abstimmung auf Tätigkeiten und Rollen vergeben, wobei das Prinzip der geringsten Rechte auf die definierten Verantwortlichkeiten angewandt wird.
- **Starke operative Sicherheit:** Die operative Sicherheit ist ein fester Bestandteil unseres Tagesgeschäfts, einschließlich des Schwachstellenmanagements, der Verhinderung von Malware und zuverlässigen Prozessen zur Verwaltung von Vorfällen für Sicherheitsereignisse, die die Vertraulichkeit, Integrität oder Verfügbarkeit von Systemen oder Daten beeinträchtigen können.

# Über das Unternehmen

WithSecure™, ehemals F-Secure Business, ist der zuverlässige Partner für Cybersicherheit. IT-Dienstleister, Managed Security Service Provider und Unternehmen, darunter die größten Finanzinstitute, Fertigungsunternehmen sowie Tausende der führenden Kommunikations- und Technologieanbieter weltweit, vertrauen auf uns in Bezug auf ergebnisorientierte Cybersicherheit, die ihren Geschäftsbetrieb schützt und verbessert. Unser KI-gesteuerter Schutzansatz sichert Endpunkte und die Zusammenarbeit in der Cloud. Unsere Lösung für intelligente Erkennung und Reaktion wird von Experten betreut, die Geschäftsrisiken identifizieren, indem sie proaktiv nach Bedrohungen suchen und sich aktuelle Angriffe abwehren. Unsere Berater arbeiten mit Unternehmen und anerkannten Technologie-Fachleuten zusammen, um die Widerstandsfähigkeit durch evidenzbasierte Sicherheitsberatung zu stärken. Mit über 30 Jahren Erfahrung in der Entwicklung von Technologien, mit denen Geschäftsziele erfüllt werden, haben wir unser Portfolio so gestaltet, dass wir mit unseren Partnern durch flexible Geschäftsmodelle wachsen können.

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

W / T H
secure