# ÜBERSICHT DER LÖSUNGEN

THREATLOCKER®

ZERO TRUST ENDPOINT PROTECTION PLATFORM

# Wie ThreatLocker®
# Ihr Unternehmen schützt

ThreatLocker® ist eine Zero-Trust-Plattform zum Schutz von Endpunkten, die Unternehmen weltweit Cybersicherheit auf Unternehmensebene bietet. Anstatt sich stark auf Erkennungsmethoden zu verlassen und Bedrohungen zu jagen, blockieren die ThreatLocker®-Lösungen alles, was nicht ausdrücklich vertrauenswürdig ist, und beschränken die Aktionen auf das Notwendige.

Zero-Trust-Sicherheit ist viel effektiver als Erkennungstools. Die Zero-Trust-Philosophie von ThreatLocker® geht über die Zulassungsliste hinaus und umfasst die Kontrolle darüber, was zulässige Anwendungen tun dürfen, auf welche Speicherbereiche wie zugegriffen werden kann und welche Netzwerkverbindungen hergestellt werden können. Verweigerungen und Zulassungen werden in Echtzeit in einem einheitlichen Audit aufgezeichnet, um die Einhaltung zu unterstützen, und ThreatLocker® Ops verwendet diese Echtzeitdaten, um Sie über blockierte böswillige Aktionen zu informieren.

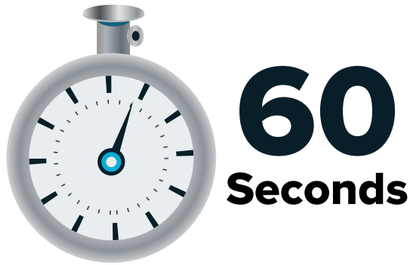
Die ThreatLocker®-Endpoint-Protection-Plattform ist so konzipiert, dass sie einfach zu bedienen ist und sich nahtlos in bestehende IT-Umgebungen integrieren lässt. Unser innovativer Lernmodus und die schnelle Reaktionszeit des 24/7 Cyber Hero Support-Teams machen das Onboarding und die Implementierung von ThreatLocker® zu einem optimierten Prozess.

# Allowlistingsseite

Die Anwendungs-Positivliste verweigert die Ausführung aller Anwendungen mit Ausnahme der ausdrücklich zugelassenen Anwendungen. Dies bedeutet, dass nicht vertrauenswürdige Software, einschließlich Ransomware und anderer Malware, standardmäßig abgelehnt wird.

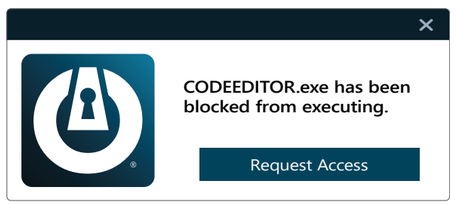
## WIE FUNKTIONIERT ES?

Wenn der Agent zum ersten Mal installiert wird, arbeitet er im Lernmodus. Während dieses Zeitraums werden alle Anwendungen und ihre Abhängigkeiten, die auf dem Computer gefunden werden oder ausgeführt werden, katalogisiert und Richtlinien erstellt, um sie zuzulassen. Nach der Lernphase kann der IT-Administrator die Liste der Anwendungen überprüfen, nicht benötigte Anwendungen entfernen und den Computer sichern. Sobald der Computer gesichert ist, wird jede Anwendung, jedes Skript oder jede Bibliothek, die versucht auszuführen, die nicht vertrauenswürdig ist, verweigert. Der Benutzer kann beim IT-Administrator neue Software anfordern, die in 60 Sekunden genehmigt werden kann.




## WARUM ZULASSUNGSLISTE (ALLOWLIST)?

Anwendungs-Positivlisten (Allowlist) sind seit langem der Goldstandard zum Schutz von Unternehmen vor bekannter und unbekannter Malware. Im Gegensatz zu Antivirus gibt Ihnen Application Allowlisting die Kontrolle darüber, welche Software, Skripte, ausführbare Dateien und Bibliotheken auf Ihren Endpunkten und Servern ausgeführt werden können. Dieser Ansatz stoppt nicht nur bösartige Software, sondern verhindert auch, dass andere nicht zugelassene Anwendungen ausgeführt werden. Dieser Prozess minimiert Cyber-Bedrohungen und andere bösartige Anwendungen in Ihrem Netzwerk.



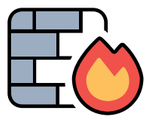

## BESEITIGEN SIE DAS RISIKO UND DAS RÄTSELRATEN

Neben der Positivliste (Allowlist) ist der Virtual Desktop Installer (VDI) von ThreatLocker® ein leistungsstarkes Tool, das risikobewertete Genehmigungen (Allows) ermöglicht, die das Rätselraten beseitigen. Der VDI ermöglicht es Administratoren, eine Anwendung schnell zu überprüfen, indem er die kritischen und zeitnahen Informationen bereitstellt, die erforderlich sind, um die beste Entscheidung für ihr Unternehmen zu treffen. Ohne Ihre Produktionsumgebung zu beeinträchtigen, erstellt der Virtual Desktop Installer von ThreatLocker® eine Testumgebung, um die angeforderte Anwendung automatisch zu installieren.


## MERKMALE

### Lernmodus

Mit der ThreatLocker® -Lösung können Sie die Ausführung jeder Anwendung auf Ihrem Gerät verweigern, die nicht auf der Positivliste (Allowlist) steht. Dies trägt dazu bei, Cyberangriffe auf Ihren Geräten oder in Ihrem Netzwerk abzuschwächen und zu verhindern.



### Firewall-ähnliche Richtlinien

Eine leistungsstarke Firewall-ähnliche Richtlinien-Engine, mit der Sie den Anwendungszugriff auf granularer Ebene zulassen, verweigern oder einschränken können.

### Zeitbasierte Richtlinien

Zugriff auf Anwendungen für einen bestimmten Zeitraum zulassen. Blockieren Sie die Anwendung automatisch, nachdem die Richtlinie abgelaufen ist.

### Integrierte Anwendungen

ThreatLocker® fügt automatisch neue Hashes hinzu, wenn Anwendungs- und Systemupdates veröffentlicht werden, sodass Ihre Anwendungen ohne Störungen aktualisiert werden können, während gleichzeitig verhindert wird, dass Updates blockiert werden.

# Ringfencing™-Seite

Ringfencing™ steuert, was Anwendungen tun können, sobald sie ausgeführt werden. Durch die Begrenzung dessen, was Software tun kann, kann ThreatLocker® die Wahrscheinlichkeit verringern, dass ein Exploit erfolgreich ist oder ein Angreifer legitime Tools wie PowerShell als Waffe nutzt.

Mit Ringfencing™ können Sie steuern, wie Anwendungen mit anderen Anwendungen interagieren können. Während beispielsweise sowohl Microsoft Word als auch PowerShell zulässig sein können, verhindert Ringfencing™, dass Microsoft Word PowerShell aufrufen kann, wodurch verhindert wird, dass eine versuchte Ausnutzung einer Schwachstelle wie der Follina-Schwachstelle erfolgreich ist.

## WARUM RINGFENCING™?

Im Normalbetrieb können alle auf einem Endpunkt oder Server zugelassenen Anwendungen auf alle Daten zugreifen, auf die der ausführende Benutzer zugreifen kann. Das bedeutet, wenn die Anwendung kompromittiert ist, kann der Angreifer die Anwendung verwenden, um Dateien zu stehlen oder zu verschlüsseln.
Mit Ringfencing™ können Sie Dateizugriffsberechtigungen für Anwendungen entfernen, die keinen Zugriff benötigen, und sogar Netzwerk- oder Registrierungsberechtigungen entfernen.

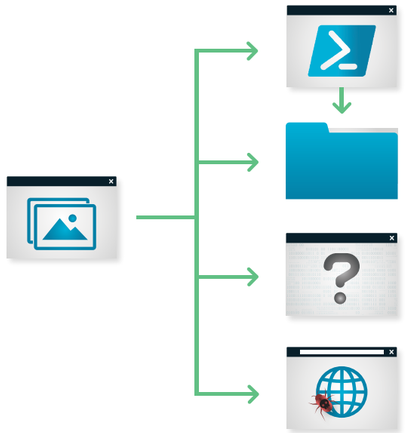


Fig. 2


Fig. 3

*Abbildung 2: Veranschaulicht die Seite Anwendungssteuerungsrichtlinien mit einer Liste von Anwendungsrichtlinien. Abbildung 3: Zeigt eine unvollständige Richtlinienliste. Die gelben Zaunsymbole werden neben Permit with Ringfence™-Richtlinien angezeigt.*

## WIE FUNKTIONIERT RINGFENCING™?

Wenn Sie Ringfencing™ zum ersten Mal bereitstellen, wird Ihr Gerät automatisch an den standardmäßigen ThreatLocker® -Richtlinien ausgerichtet. Diese Richtlinien werden dann automatisch auf eine Liste bekannter Anwendungen wie Microsoft Office, PowerShell oder Zoom angewendet. Das Ziel der Standardrichtlinien besteht darin, ein grundlegendes Schutzniveau für alle Endpunkte bereitzustellen. Jede dieser Richtlinien kann leicht verändert werden, um sie jederzeit an jede Umgebung anzupassen. Unser Team engagierter Cyber Heroes steht Ihnen rund um die Uhr zur Verfügung, um alle Anfragen zu unterstützen.

## MERKMALE

### Schutz vor dateiloser Malware

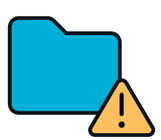
Stoppen Sie dateilose Malware, indem Sie einschränken, was Anwendungen tun dürfen.

### Granulare Anwendungsrichtlinien

Verhindern Sie, dass Anwendungen mit anderen Anwendungen, Netzwerkressourcen, Registrierungsschlüsseln, Dateien und mehr interagieren.

### Anwendungsangriffe begrenzen

Begrenzen Sie Angriffe auf Anwendungen wie Application Hopping, indem Sie einschränken, auf welche Anwendungen zugegriffen werden kann.



### Beschränken Sie den Zugriff auf Ihre Dateien

Der durchschnittliche Computer hat über 500 Anwendungen; Nur eine Handvoll muss auf Ihre Dateien zugreifen. Mit Ringfencing™ können Sie auswählen, welche Anwendungen welche Dateien verwenden können.

# Speicher Zugriff Kontroll Seite

Storage Control bietet eine richtliniengesteuerte Kontrolle über Speichergeräte, unabhängig davon, ob es sich bei dem Speichergerät um einen lokalen Ordner, eine Netzwerkfreigabe oder einen externen Speicher wie ein USB-Laufwerk handelt. ThreatLocker® Storage Control ermöglicht das Festlegen granularer Richtlinien, die so einfach wie das Blockieren von USB-Laufwerken oder so detailliert wie das Blockieren des Zugriffs auf Ihre Backup-Freigabe sein können, außer wenn darauf von Ihrer Backup-Anwendung zugegriffen wird.

## DIGITAL TRAIL MIT UNIFIED AUDIT (AUDIT LOGS)

Unified Audit bietet ein zentrales Protokoll aller Speicherzugriffe durch Benutzer im Netzwerk und Remote-Arbeiter, bis hin zu den kopierten Dateien und der Seriennummer des Geräts.

## WIE FUNKTIONIERT DIE SPEICHERKONTROLLE?

Wenn ein Speichergerät blockiert ist, kann einem Benutzer ein Popup angezeigt werden, in dem er den Zugriff auf ein Speichergerät anfordern kann. Der Administrator kann dann entscheiden, das Speichergerät in nur 60 Sekunden zuzulassen.

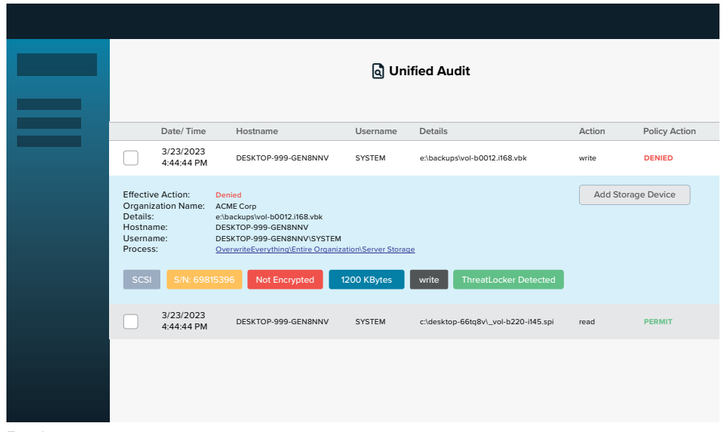


Fig. 4

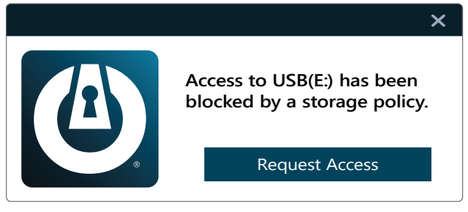



*Abbildung 4: Veranschaulicht die Unified Audit-Seite mit einem erweiterten Speichersteuerungseintrag, der zeigt, dass der Schreibzugriff verweigert wurde.*

## MERKMALE

### Audit-Zugriff auf Dateien

Eine vollständige und detaillierte Prüfung aller Dateizugriffe auf Netzlaufwerke, USB- und lokale Festplatten ist innerhalb von Minuten nach dem Öffnen einer Datei zentral zugänglich.

### Granulare Speicherrichtlinien

Diese Richtlinien erlauben oder verweigern den Zugriff auf Speicher basierend auf Benutzer, Zeit, Anwendungen und mehr.

### Einfache Zugriffsanfragen

Ein Popup mit der Option, den Zugriff auf das Speichergerät anzufordern.

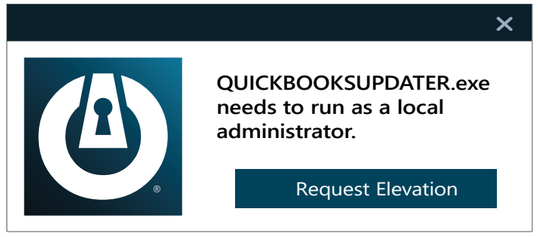
### Einfache USB-Blockierung

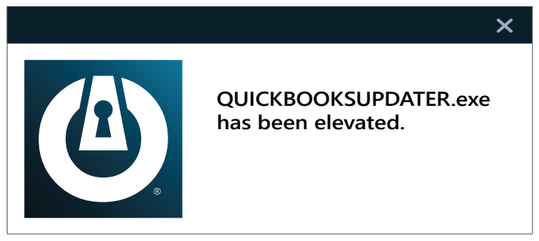
USB-Richtlinien ermöglichen den Zugriff basierend auf der Seriennummer des Geräts, dem Anbieter und/oder dem Dateityp.

# Erhöhte Benutzerrechte Kontroll Seite (UAC)

Elevation Control ermöglicht es Benutzern, bestimmte Anwendungen als lokaler Administrator auszuführen, selbst wenn sie keine lokalen Administratorrechte haben. Elevation Control versetzt IT-Administratoren in die Lage, genau zu steuern, welche Anwendungen als lokaler Administrator ausgeführt werden können, ohne Benutzern lokale Administratorrechte zu erteilen.

der erstmaligen Bereitstellung von ThreatLocker® werden alle vorhandenen Anwendungen erlernt. Administratoren können die Anwendungen überprüfen und auswählen, welche als lokaler Administrator ausgeführt werden können. Nach der Aktivierung kann ein Benutzer die Software als lokaler Administrator ausführen, ohne Anmeldeinformationen einzugeben.




## MERKMALE

### Vollständige Sichtbarkeit der Administratorrechte

Gibt Ihnen die Möglichkeit, bestimmte Anwendungen zur Ausführung als Administrator zu genehmigen, selbst wenn der Benutzer kein lokaler Administrator ist.

### Optimierte Berechtigungsanfragen

Benutzer können die Berechtigung zum Hochstufen von Anwendungen anfordern und Dateien und Notizen anhängen, um ihre Anforderungen zu unterstützen.

### Differenzierte Erhöhte BenutzerrechteKontrolle

Ermöglicht Ihnen, die Dauer festzulegen, wie lange ein Benutzer Zugriff auf bestimmte Anwendungen hat, indem Sie entweder temporären oder permanenten Zugriff gewähren.

### Sichere Anwendungsintegration

Ringfencing™ stellt sicher, dass Benutzer nicht springen können, um verbundene Anwendungen innerhalb des Netzwerks zu infiltrieren, sobald Anwendungen erhöht werden.

# Netzwerk Zugriffs Kontolle (NC)

ThreatLocker® NC ist eine Endpoint- und Server-Firewall, die Ihnen die vollständige Kontrolle über den Netzwerkverkehr gibt, was Ihnen letztendlich hilft, Ihre Geräte zu schützen. Mithilfe benutzerdefinierter Richtlinien können Sie granularen Zugriff basierend auf IP-Adresse, bestimmten Schlüsselwörtern oder sogar Agentenauthentifizierung oder dynamischen ACLs zulassen.

## WARUM NETZWERK ZUGRIFFS KONTROLLE?

Das lokale Netzwerk gibt es nicht mehr. Benutzer arbeiten vom Büro und aus der Ferne, was bedeutet, dass das Netzwerk, das wir alle nutzen, schnell zum Internet geworden ist. Diese Auflösung des Perimeters macht Geräte und Daten angreifbar und Cyber-Bedrohungen ausgesetzt. Aus diesem Grund müssen Sie den Netzwerkverkehr kontrollieren, um Ihr Gerät und damit auch Ihre Daten zu schützen. Sie können dies erreichen, indem Sie eine Network Control-Lösung (NC) implementieren.

Fig. 5

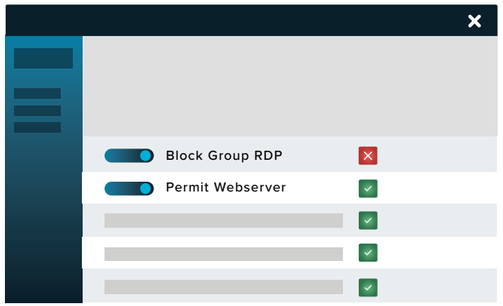
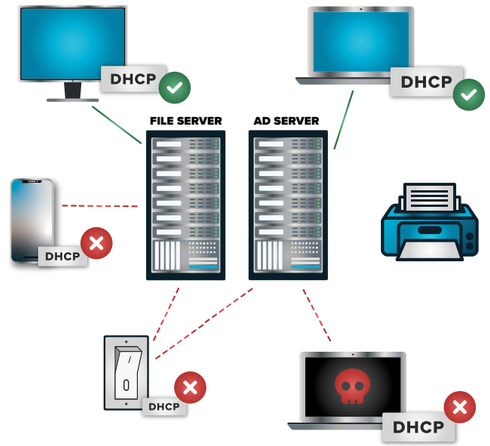



*Abbildung 5: Zeigt einen Teil einer NC-Richtlinienliste. Abbildung 6: Zeigt eine partielle NC-Richtlinie.*

## DYNAMISCHE ACLS

Mit dynamischen ACLs können Sie Ports basierend auf dem Standort eines Computers oder einer Gruppe von Computern zu einem bestimmten Zeitpunkt automatisch öffnen. Bei dynamischen ACLs ist die Verbindung zwischen Server und Client direkt, im Gegensatz zu einem VPN, das eine Verbindung über einen zentralen Punkt herstellen muss.

Fig. 6


## MERKMALE

### Konfigurierbar

Mithilfe globaler und granularer Richtlinien ermöglicht NC Benutzern, den Netzwerkzugriff auf Endpunkte zu konfigurieren.

### Cloudbasiert

Die Cloud-verwaltete Lösung bietet Kunden eine zentralisierte Ansicht der Endpunktrichtlinien und des Netzwerkverkehrs in Ihrer gesamten Organisation.

### Dynamisch

NC ermöglicht den gesamten Datenverkehr zu öffentlichen Servern zu verhindern, wohingegen einzelne Computer, nach IP-Adresse oder dynamisch mit einem Schlüsselwort, zugelassen werden können. Der Zugriff mit Schlüsselwort ist insbesondere für einen Benutzer, der oft unterwegs ist, hilfreich.

### Verbesserte Netzwerksicherheit

Stellen Sie mit dynamischen ACLs sicher, dass Rogue-Geräte in Ihrem Netzwerk nicht auf Ihre Server oder Endpunkte zugreifen können.

# THREATLOCKER®

ThreatLocker® verbessert die Server- und Endpunktsicherheit auf Unternehmensebene mit Zero-Trust-Kontrollen, einschließlich Allowlisting, Ringfencing™, Elevation, Storage, Network Control, Configuration Management und Operational Alert-Lösungen.