DriveLock

Application Control

Ein Teil der HYPERSECURE Platform

Einleitung

Die **Applikationskontrolle** spielt eine entscheidende Rolle bei Ihrer Sicherheitsstrategie.

Sie bietet die Kontrolle darüber, welche Software, Software-Bibliotheken und Skripte genehmigt werden, um effektiv arbeiten zu können. Gleichzeitig können auch eingebaute Werkzeuge, die von Angreifern missbraucht werden könnten, auf eine Block-List gesetzt werden oder ihre Nutzung auf bestimmte administrative Gruppen beschränkt werden. So können Sie sicherstellen, dass Ihre IT-Umgebung geschützt ist und nur die erforderlichen Tools und Programme verwendet werden.

Die Konfiguration für Applikationskontrolle wird zentral in den DriveLock Richtlinien verwaltet und kann gezielt auf alle Computer zugewiesen oder auch auf Personengruppen eingeschränkt werden. Sie behalten stets die Kontrolle.

Das DriveLock „predictive" Allow-Listing minimiert den Pflegeaufwand von Allow-Lists und gewährleistet durch das automatisierte Lernen der Allow-List Sicherheitsstandards, indem Implementierung und Ausführung von unbekannten Anwendungen verhindert werden.

Dies vermeidet Cyberangriffe durch jede Art von dateibasierter und dateiloser Malware, einschließlich Ransomware und hochentwickelter hartnäckiger

Applicaton Control

Ein Teil der HYPERSECURE Platform

DriveLock

1

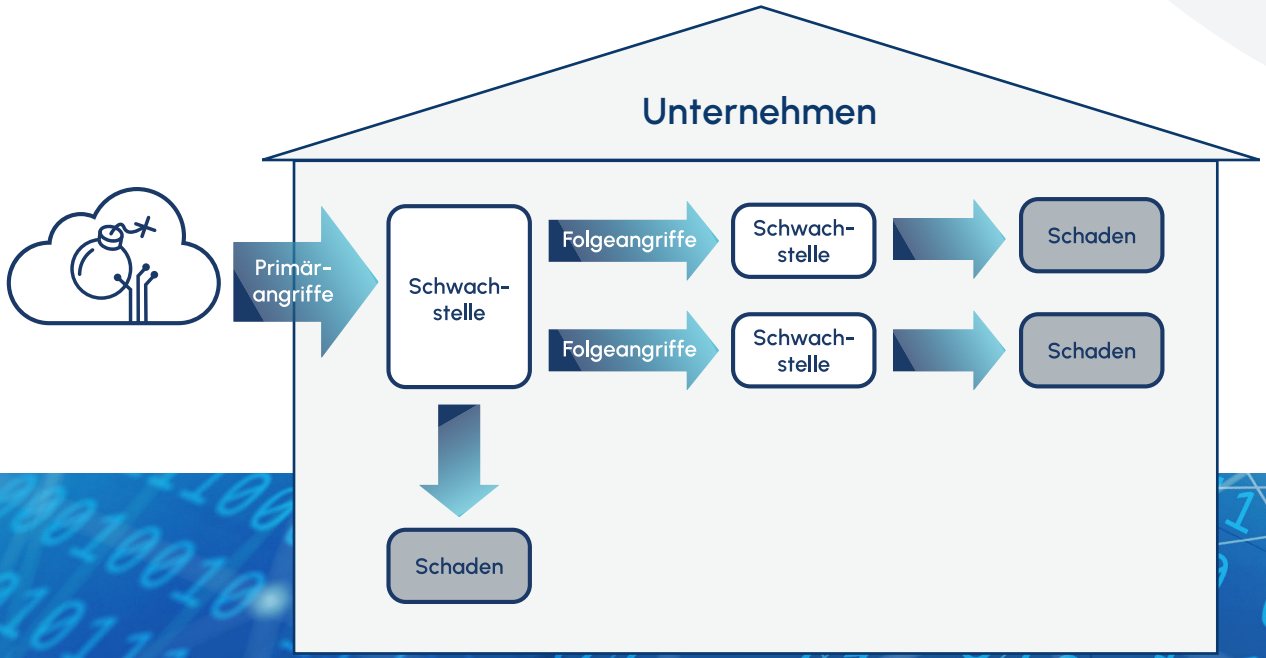
Der Schutz vor dem Unbekannten

Die Bedrohungslandschaft

Wir sehen eine zunehmende Abhängigkeit von digitalen Technologien. Allerdings erhöht diese auch das Risiko großangelegter Cyberangriffe auf kritische Infrastrukturen. Die Digitalisierung bringt nicht nur Segen.

Viele Einrichtungen haben das bereits bitter erfahren müssen. Sie wurden Opfer von Ransomware-Angriffen und anderen Techniken und kämpfen auch Monate später noch mit den Nachwirkungen. Gerade kritische Infrastrukturen bieten viele Angriffsvektoren, über die beispielsweise die Verfügbarkeit der Infrastruktur beeinträchtigt oder sensible Daten gestohlen bzw. manipuliert werden.

Hinter diesen Angriffen können größere Organisationen bis hin zu Regierungen stecken, die umfangreiche Ressourcen für die Entwicklung von Schadcodes besitzen. Hinzu kommen die steigende Komplexität der IT-Umgebungen und IT-Sicherheitskräfte. Ist „Stress der IT-Sicherheitskräfte" der Hauptgrund, warum es solche Organisationen leicht haben, sich in Firmennetzwerke zu hacken? Sind diese vielleicht auch überfordert bzw. nicht gut genug geschult/qualifiziert/trainiert? Besonders im öffentlichen Sektor mangelt es häufig an ausreichenden Fachkräften. Und es geht nicht nur um die Sicherheit im eigenen Unternehmen, sondern auch um die Sicherheitsstandards von externen Partnern, Lieferketten und die der Kunden. Neue gesetzliche Vorschriften wie die DSGVO (GDPR) sowie NIS2 erhöhen den Handlungsdruck.



Applikationskontrolle zur Abwehr von Cyberbedrohungen

Die Anzahl der Angriffe nimmt kontinuierlich zu und Angreifer gehen immer gezielter und trickreicher vor. Sie nutzen gezielt den Faktor Mensch aus, indem sie Phishing E-Mails als täuschend echt verpacken. USB-Sticks und Wechseldatenträger sind nach wie vor eine der häufigsten Quellen für Malware-Infektionen.

Bei „traditionellen" Angriffsarten wird primär externe Malware auf dem Zielsystem installiert oder ausgeführt.

Darüber hinaus gibt es die „Living off the Land"-Methoden (LotL), die auch als „Fileless Malware" bekannt sind. Angreifer nutzen bereits auf dem Zielsystem vorhandene Administrations- bzw. System-Tools wie PowerShell oder MS-Office (Skripte und Software-Makros), um einen Angriff zu initiieren.

Bei hochentwickelten, hartnäckigen Bedrohungen (Advanced Persistent Threat – kurz APT) gehen Angreifer sehr zielgerichtet und behutsam vor und nehmen u.U. viel Aufwand auf sich, um nach dem ersten Einfallen in einen Rechner weiter in die lokale IT-Infrastruktur des Angegriffenen vorzudringen. Deshalb ist es wichtig, „Einbrüche" zu stoppen oder zumindest die negativen Auswirkungen, wie Diebstahl sensibler Daten, zu begrenzen.

Der **Bericht des Bundesamtes für Sicherheit in der Informationstechnik** (BSI) identifiziert verschiedene Bedrohungen, die insbesondere aus Schwachstellen resultieren. Zu den Hauptgefahren zählen das Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme, die Infektion über Internet und Intranet, menschliches Fehlverhalten sowie Sabotage.

Einmal im Unternehmensnetzwerk eingedrungen, haben Angreifer die Möglichkeit zur lateralen Ausbreitung und zur Initiierung von Folgeangriffen. Diese können verschiedene Formen annehmen, darunter Rechteerweiterungen und der Einsatz von Schadsoftware. Die potenziellen Auswirkungen reichen von Daten- und Know-How-Diebstahl bis hin zu einer Qualitätsminderung der erzeugten Produkte, die beispielsweise im Bereich der Trinkwasserversorgung weitreichende Konsequenzen haben können.

Um nicht nur primäre Angriffe zu verhindern, sondern auch wirksam gegen Folgeangriffe vorzugehen, ist der Einsatz von kritischen Sicherheitskontrollen (CSC) von entscheidender Bedeutung. Applikationskontrolle spielt hierbei eine zentrale Rolle. Durch die gezielte Kontrolle und Überwachung wird eine präventive Schicht geschaffen, die die Verbreitung von Schadsoftware und die Ausführung schädlicher Prozesse effektiv unterbindet.

Rechteerweiterungen, die oft im Rahmen von Angriffen zur Eskalation von Berechtigungen eingesetzt werden, können durch Applikationskontrolle-Maßnahmen gezielt blockiert werden. Gleichzeitig wird auch der Einsatz von Schadsoftware durch eine genaue Überwachung und Kontrolle der Anwendungen eingeschränkt, was eine zusätzliche Schutzschicht gegen Folgeangriffe darstellt.

Applikationskontrolle trägt nicht nur zur Abwehr von Angriffen bei, sondern schützt auch vor dem Diebstahl sensibler Daten und geistigem Eigentum. Durch gezielte Kontrollen können unberechtigte Zugriffe und Datentransfers verhindert werden, wodurch das Unternehmen seine wertvollen Informationen effektiv schützt.

2

Der effektivste Schutz vor Schadsoftware

Bedrohungslage

Wir benötigen einen ganzheitlichen und mehrschichtigen Schutz. Eine Firewall und eine Antiviren-Software per se sind nur ein Teil des Ganzen, da es mehr Sicherheitskontrollen braucht, um effektiven Schutz zu gewährleisten. Eine Antivirus-Software erkennt hauptsächlich bekannte Schadsoftware, weswegen keine getarnte oder zum Zeitpunkt des Angriffs noch unbekannte Malware oder AV erkannt werden kann. Zudem bietet sie keinen Schutz vor Zero Day Exploits und LotL Attacken.

Applikationskontrolle erklärt

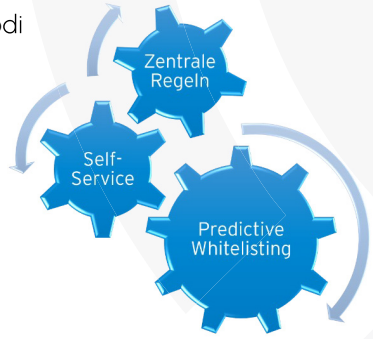
Mit der Standard-Applikationskontrolle sind Administratoren in der Lage, die Ausführung jeder beliebigen Anwendung auf Computern zu kontrollieren. Es können verschiedene Regeln oder Strategien verwendet werden, um festzulegen, welche Anwendungen ausgeführt und welche gesperrt werden. Diese Freigabe oder Sperre kann anhand verschiedener Kriterien und Regeltypen definiert werden:
Die Flexibilität, sowohl Block-List- und Allow-List-Regeln zu kombinieren, macht die Applikationskontrolle sowohl einfach in der Verwendung als auch leistungsstark in der Absicherung.

Allow-List und Block-List erklärt

Beim Application Allow-Listing erstellen Sie eine Liste von vertrauenswürdigen Entitäten (Anwendungen, Software-Bibliotheken, Skripte), die auf ein System oder Netzwerk zugreifen dürfen, und blockieren alles andere. Sie basiert auf dem „Zero Trust"-Prinzip, das im Wesentlichen alles verweigert und nur das zulässt, was notwendig ist. Angesichts der Tatsache, dass Block-Lists auf bekannte Muster (dokumentierte Malware usw.) beschränkt sind und dass Malware-Varianten ständig die verhaltens- oder signaturbasierten Erkennungsmodi umgehen, herrscht in vielen Kreisen die Meinung, dass Allow-Listing der vernünftigere und sicherere Ansatz für Informationssicherheit ist. Aus Sicherheitssicht ist es sinnvoller, zunächst alles pauschal zu verbieten und dann gezielt Applikationen und Skripte zuzulassen. Wenn nur zugelassene Software ausgeführt werden darf, werden die Chancen, dass Malware das System übernimmt, minimiert.

Applikationskontrolle mit verschiedenen Betriebsmodi

Bevor Sie mit der Sperrung von Programmen beginnen, bieten sich Simulationsmodi an, um die Auswirkungen Ihrer Regeln vorab zu testen. Während einer Simulation erzeugt DriveLock entsprechend den Regeln Ereignismeldungen für gestartete oder blockierte Anwendungen, die Ausführung selbst wird dabei aber noch nicht verhindert. Der Simulationsmodus kann sehr hilfreich sein, um zu ermitteln, welche Anwendungen gesperrt worden wären. Anschließend analysieren Sie die Daten mit Hilfe des DriveLock Operations Centers, um entsprechende Ereignisse schnell zu finden. Dieser Modus führt Sie schrittweise durch die Produktionsumgebung.



Applikationskontrolle mit intelligentem Allow-Listing

Applikationskontrolle spielt eine entscheidende Rolle bei der Sicherheitsstrategie. Der herkömmliche Ansatz mit statischen Block-Lists oder Allow-Lists funktioniert in der sich schnell ändernden Lage nur bedingt und oftmals klagen Administratoren über den überproportionalen Pflegeaufwand. Das von DriveLock angebotene „predictive" Allow-Listing hält dagegen den Aufwand für die Pflege von Allow-Lists auf einem Minimum und verhindert durch das automatisierte Lernen der Allow-List Sicherheitsstandards die Implementierung und Ausführung von unbekannten Anwendungen. Dies vermeidet Cyberangriffe durch jede Art von dateibasierter und dateiloser Malware, einschließlich Ransomware oder APTs. Um den administrativen Aufwand zu minimieren, ist es möglich, alle bestehenden Anwendungen zu genehmigen. Zu diesem Zweck muss die „lokale" Allow-List aktiviert werden. Sie können den Lernprozess auf bestimmte Verzeichnisse beschränken, wenn Sie dies wünschen. Das DriveLock Operations Center gewährt jederzeit einen Überblick und somit Kontrolle über die neuesten Ergänzungen zur lokalen Allow-List.

Integrieren Sie Ihren Software Deployment Agent mit DriveLock Applikationskontrolle

Um die Anwendungssteuerung zu vereinfachen, können Software-Verteilungssysteme, Patch-Management-Systeme und eigenständige Updater in die DriveLock Anwendungssteuerung integriert werden. Der Agent oder Updater wird als vertrauenswürdiger Prozess definiert. Das bedeutet, dass der Agent oder Updater Software-Setups starten kann, die nicht auf der Allow-List stehen. Dateien, die von diesen Setups während der Installation geschrieben werden, werden automatisch zur lokalen Allow-List hinzugefügt. Dadurch wird die Pflege der Allow-List erheblich vereinfacht. Die Kombination aus vertrauenswürdigem Prozess und automatischem Lernen ermöglicht es dem Software Deployment Agent, bisweilen unbekannte Anwendungen, wie z. B. Software-Setups, zu starten. Alles, was von diesem oder anderen Sub- Prozessen während der Installation geschrieben wird, wird automatisch zur lokalen Allow-List hinzugefügt.

Dateiablagen können als vertrauenswürdig eingestuft werden

Um die Anwendungssteuerung weiter zu vereinfachen, können zentrale oder lokale Dateiablagen als vertrauenswürdig eingestuft werden. Dabei kann es sich um eine Freigabe oder einen lokalen Ordner handeln, in der die IT-Abteilung vetrauenswürdige Software speichert, wie beispielsweise den Cache eines Software-Verteilungsagenten. Bisher unbekannte Software-Setups, die von einer solchen vertrauenswürdigen Quelle aufgerufen werden, können so gestartet werden. Alle Dateien, die von diesem Prozess oder einem untergeordneten Prozess auf die Festplatte geschrieben werden, werden automatisch zur lokalen Allow-List hinzugefügt, ohne dass ein Administrator eingreifen muss. Administratoren können weitere Berechtigungen oder Einschränkungen vornehmen. So ist es außerdem sinnvoll, die Berechtigungen auf einen vertrauenswürdigen Benutzer oder eine Benutzergruppe zu beschränken, zum Beispiel Mitglieder der IT-Abteilung oder einer Administratorgruppe.

Die Balance zwischen zentralen Vorgaben und der Produktivität der Endbenutzer

Die Aufgaben können zwischen zentraler IT und mündigen Endbenutzer aufgeteilt werden. Endbenutzer können auf dem Computer um Genehmigung gebeten werden, bevor ein Prozess ausgeführt wird. Dadurch wird verhindert, dass Software versehentlich in die Allow-List aufgenommen wird. Diese Antwort speichert die lokale Allow-List für die aktuelle Benutzersitzung, also so lange, bis sich der Benutzer abmeldet oder der Client neu gestartet wird. Die Kombination von zentraler Vorgabe der IT-Abteilung und die Beteiligung der Endbenutzer entlastet auf der einen Seite die IT und steigert auf der anderen Seite die Produktivität der Anwender ohne große Einschränkungen.

Nicht jede Software wird über eine automatische Software-Verteilung installiert. Für manuelle Software-Installationen bietet die DriveLock Applikationskontrolle die Möglichkeit, einen Rechner temporär freizuschalten und den DriveLock Agenten in einen Lernmodus zu versetzen. Definieren Sie, welche Benutzer oder Benutzergruppen die Self-Service-Funktionen nutzen können. Es ist auch möglich, die gelernten Dateien vorab prüfen zu lassen, bevor sie am Ende der temporären Entsperrung der Allow-List hinzugefügt werden. Dies ist eine sehr einfache Möglichkeit, die Allow-List zu pflegen. Für die IT-Administration entsteht dadurch kein nennenswerter Mehraufwand.

Kontrolle für Skripts und Skriptinterpreter

Die Unterstützung von Skripten zusätzlich zum Anwendungs-Allow-Listing ermöglicht es Organisationen, ein hohes Maß an Sicherheit zu erreichen. DriveLock bietet Ihnen einen ganzheitlichen Ansatz und volle Konfigurierbarkeit. Sie können Skriptdateien unter Verwendung eines Hash-Wertes, einer digitalen Signatur, eines Pfades oder eines Dateieigentümers ausführen lassen. Die Skripte und deren Interpreter können jederzeit erweitert werden. Allow- und Block-Lists können auch für Skripte und nicht nur für Anwendungen und DLLs verwendet werden.

Applikationskontrolle reduziert zusätzlich die Angriffsfläche

In den Anwendungs-Berechtigungen ist konfiguriert, was zugelassene Anwendungen dürfen, d. h.
» welche Berechtigungen die Anwendungen erhalten,
» in welche Verzeichnisse Anwendungen schreiben oder
» welche Prozesse diese starten dürfen.

Die Kontrolle über die Ausführung von untergeordneten Anwendungsprozessen reduziert Ihre Angriffsfläche. Das Erstellen bösartiger Sub-Prozesse ist eine gängige Malware-Strategie. Malware, die MS Office als Angriffsvektor missbraucht, führt häufig VBA-Makros aus, nutzt Code zum Herunterladen aus und versucht zusätzliche Nutzlasten auszuführen. Einige legitime Branchenanwendungen können jedoch auch Unterprozesse für gutartige Zwecke erzeugen, z. B. zum Erzeugen einer Eingabeaufforderung oder zur Verwendung von PowerShell zur Konfiguration von Registrierungseinstellungen.

Anwendungsberechtigungen kontrollieren das Anwendungsverhalten

Das Ziel von Anwendungsberechtigungen ist es, erweiterte Anti-Malware-Fähigkeiten sowie eine bessere Prävention gegen die eventuelle Umgehung der Anwendungs-Allow-List bereitzustellen. Sie bieten einen besseren Schutz gegen die bereits erwähnten dateilosen (LotL) Angriffe. Zudem können diese Regeln den Aufruf von bestimmten untergeordneten Prozessen blockieren. Sie können legitime Programme (die auf der Allow-List stehen) auf tatsächlich erforderliche Aktionen und Berechtigungen weiter einschränken, was es für Angreifer noch schwieriger macht. Dadurch wird sichergestellt, dass nur autorisierte Software und Skripte ausgeführt werden. Sie kontrollieren auch den Zugriff auf Skript-Werkzeuge wie MS PowerShell, VBS, Python und die Befehlszeile.

Vorteile der Anwendungsberechtigungen

Sie verhindern, dass aus einer erlaubten Anwendung heraus eine weitere Anwendung (bzw. Prozess, Skript) gestartet wird, die eine potenzielle Gefahr für das System darstellen könnte.

Sie legen fest, welche Art von Zugriff einer bestimmten Anwendung erlaubt wird (z. B. lesend oder schreibend auf Dateien oder Zugriff auf die Registry).

Dazu stehen u.a. folgende Funktionen zur Verfügung:

- Sie geben an, welche Maßnahme ergriffen werden soll, wenn ein Zugriff durch eine bestimmte Anwendung erfolgt (z. B. die Anwendung wird geblockt oder nicht).
- Sie bestimmen, ob eine Anwendungs-Berechtigung an untergeordnete Prozesse vererbt werden soll.
- Verschiedene Datei- und Verzeichnisfilter können angegeben werden.
- Skript-Typen können festgelegt werden, die bei der Ausführung von Skripten verwendet werden dürfen.
- Es kann festgelegt werden, welche Anwendung die Registry lesen oder schreiben darf.
- Ein Regelwerk, in welcher Reihenfolge Anwendungs-Berechtigungen abgearbeitet werden.
- Die Kombination von Regeln: z. B. eine Regel, die dem Browser erlaubt, den Windows Media-Player zu starten (hohe Priorität) und eine weitere Regel, die dem Browser verbietet, andere Programme zu starten (niedere Priorität).
- Vererbung der Dateiberechtigungen an aufgerufene Prozesse, die weitere Prozesse oder Skripts starten. Dadurch können Berechtigungen nicht durch Starten anderer Prozesse umgangen werden.

Um die Administration stark zu vereinfachen und um IT-Abteilungen zu entlasten, kann das richtige Anwendungsverhalten automatisch gelernt werden. Dazu werden Anwendungen über einen gewissen Zeitraum beobachtet und dieses Verhalten entweder als zentrale Richtlinien (Policies) übernommen oder, wie bei einer lokalen Allow-List, für den Computer gemerkt. Danach darf die Anwendung nur noch Operationen durchführen, die erfolgreich gelernt wurden.

3

Anwendungsfälle

Szenarien für Anwendungsfälle – Beispiele

Es gibt eine Reihe allgemeiner Anwendungsfälle, die verdeutlichen, wie Anwendungskontrolle und -berechtigungen wirken.

1. Das Starten von PowerShell verhindern

Sie wollen verhindern, dass bei der Verwendung eines Browsers PowerShell gestartet wird und womöglich Schadsoftware auf den Computern eingespielt wird.

Da Sie verhindern wollen, dass der Browser die Powershell.exe von der Kommandozeile (cmd.exe) aus aufruft (hierbei handelt es sich um einen untergeordneten Prozess), kann das Blockieren von Aufrufen untergeordneter Prozesse vererbt werden.

2. Das Laden einer DLL einschränken

Sie wollen festlegen, dass DLLs nur aus bestimmten Verzeichnissen geladen werden dürfen.

Im konkreten Fall soll verhindert werden, dass der Windows Media Player DLLs von Netzlaufwerken lädt.

HYPERSECURE IT

Application Control

3. Lesen eines bestimmten Verzeichnisses

Sie wollen sicherstellen, dass nur eine bestimmte Applikation lesend auf ein ganz bestimmtes Verzeichnis zugreifen kann. Keine andere Anwendung soll Lesezugriff auf dieses Verzeichnis erhalten.

Durch eine Sicherheitslücke im Browser wäre es möglich, dass eine Schadsoftware sich Lesezugriff auf dieses Verzeichnis verschafft und somit Ihre Bankdaten auslesen kann. Das muss verhindert werden.

Sie erstellen zwei Anwendungsberechtigungen: Bei der ersten erlauben (=nicht blockieren) Sie den Zugriff der Software auf das Verzeichnis. Bei der zweiten geben Sie den Platzhalter * als ausführende Anwendung an, so dass keine andere Anwendung Zugriff (=blockieren) auf das angegebene Verzeichnis erhält. Bezüglich der Prioritäten gilt „Nicht blockieren vor Blockieren".

4. Skriptausführung

Sie wollen verhindern, dass VB-Skripte (*.vbs) von Browsern ausgeführt werden.

DriveLock nutzt fortgeschrittene Techniken wie Verhaltensanalyse und Heuristiken, um schädliche Skriptaktivitäten zu erkennen und zu blockieren, selbst wenn diese noch nicht durch bestehende Regeln erfasst wurden.

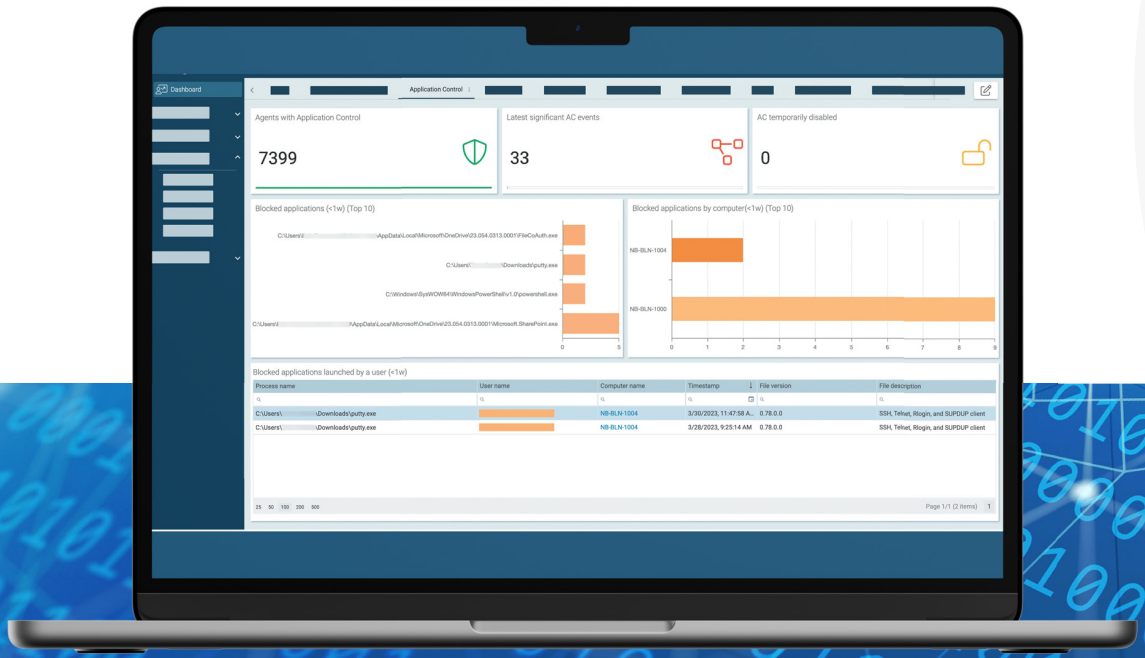
Falls ein legitimes Skript blockiert wird, kann es Ausnahmeverfahren geben, die es erlauben, solche Skripte nach einer Überprüfung schnell freizugeben.

Mehr Sichtbarkeit im Unternehmen

Das **DriveLock Operations Center** – kurz **DOC** – ist eine moderne **Web-Konsole** zur Verwaltung und Visualisierung. Die Dashboards liefern alle Informationen für Administratoren, Helpdesk und IT-Mitarbeiter. Es vereinfacht und optimiert die erforderlichen Managementaufgaben im täglichen Betrieb. Das DOC ist sowohl für unsere DriveLock Managed Services als auch für On-Premise-Kunden verfügbar.

Für Applikationskontrolle stellt die Konsole ein umfangreiches Dashboard sowie View zur Verfügung, um den Administratoren eine Einsicht in die Unternehmensumgebung zu ermöglichen:

- Alle Computer, die Applikationskontrolle aktiviert haben
- Status des Lernverhaltens, Applikationen in der Allow-List, und was der Auslöser für deren Aufnahme war
- Geblockte Applikation pro Computer und welche insgesamt geblockt wurden



Mehr effektive Sicherheit mit der HYPERSECURE Platform

Ein digitales Unternehmen hat keine Grenzen

DriveLock steht als wegweisender Spezialist für modernste IT-Sicherheitslösungen.

Unsere HYPERSECURE IT schützt Endgeräte mit einer einzigartigen Mischung aus präventiven und proaktiven Funktionen.

Die DriveLock HYPERSECURE Platform bietet mehrschichtige Sicherheit und nutzt die Cloud-Technologie für sofortige Verfügbarkeit und kosteneffizienten Betrieb. Cyberbedrohungen werden in Schach gehalten, dank unseres Engagements für Zero Trust auf der nächsten Stufe, in Deutschland entwickelt.

Unsere HYPERSECURE Platform kombiniert die Stärken von Endpoint Protection, Data Loss Prevention, Security Awareness, Risk & Vulnerability Management, Detection & Response, Security Configuration Management und Identity & Access Management und bietet einen beispiellosen Schutz vor modernen Bedrohungen. Sie ist die deutsch-europäische IT-Security Lösung, mit deren Hilfe Informationssicherheitsrisiken in Unternehmen und Einrichtungen erkannt, verwaltet und durch Sicherheitsmaßnahmen minimiert werden können. Die Sicherheitsmaßnahmen berücksichtigen die Bereiche Endpoint-Assets (insbesondere Devices, Applikationen), Benutzer und Daten und bieten effiziente und effektive Kontrollmechanismen.

Kunden erhalten von zentraler Stelle aus einen klaren Überblick und ein zentrales Management aller Sicherheitsvorgänge, was in einer zunehmend komplexen IT-Landschaft entscheidend ist.

In der Vergangenheit war es ausreichend, den Schutz gegen Angriffe von außen zu maximieren. Und das war fast die einzige kritische Sicherheitskontrolle. Heute gehen wir davon aus, dass wir jederzeit und überall kompromittiert werden.

DriveLock

HYPERSECURE IT

Mit der HYPERSECURE Platform
bleiben **Angriffe** auf IT-Systeme da,
wo sie hingehören: **außen vor**.

HYPERSECURE mit DriveLock

HYPERSECURE IT aus Deutschland: DriveLock ist der führende Spezialist für präventive IT-Sicherheitslösungen aus Deutschland.

HYPERSECURE IT schützt Endpoints.

Die digitalisierte Welt erfordert kompromisslose IT-Sicherheit, um Organisationen, Menschen und Dienste vor Cyberrisiken und Datenverlust zu schützen und digitales Arbeiten für alle sicher zu gestalten.

Die **HYPERSECURE Platform von DriveLock** gleicht einer schlagkräftigen Counter-Force aus spezialisierten Abwehrkräften, die in ihrer jeweiligen Disziplin zu den besten zählen. Sie bietet mehrschichtige Sicherheit, ist cloud-basiert, sofort verfügbar und wirtschaftlich effizient mit niedrigen Investitions- und Betriebskosten.

Die neue **Hochleistungsklasse der IT-Sicherheit** schützt digitale Arbeitsplätze konsequent und schafft Synergien aus den folgenden Elementen:

- **Data & Endpoint Protection**
- **Data Loss Prevention**
- **Data Encryption**
- **Security Awareness**
- **Risk & Vulnerability Management**
- **Security Configuration Management**

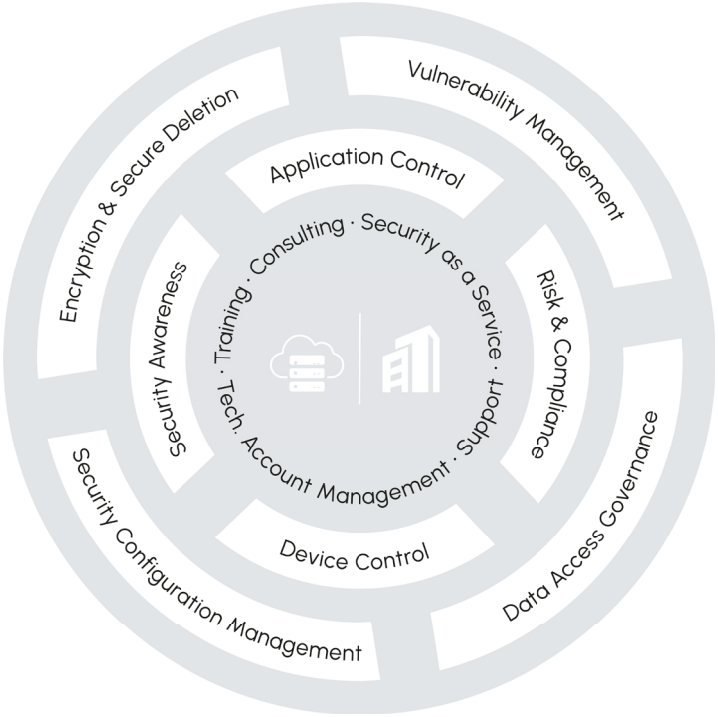
Die DriveLock-Lösungen Device Control und Application Control sind nach Common Criteria EAL3+ zertifiziert: Diese international anerkannte Zertifizierung attestiert die hohe Vertrauenswürdigkeit und den Sicherheitsstandard des DriveLock Agents. DriveLocks wegweisende Tools und ihr engagiertes Team sorgen dafür, dass Cyberattacken dort bleiben, wo sie hingehören: außen vor.

Erfahren Sie mehr und besuchen Sie uns auf www.drivelock.com.

Vorteile von HYPERSECURE IT

1. bietet mehrschichtige Sicherheit
2. ist cloud-basiert
3. ist sofort verfügbar
4. ist wirtschaftlich effizient
5. hat niedrige Investitions- und Betriebskosten
6. ist ohne Backdoor
7. ist Made in Germany: Entwicklung und technischer Support aus Deutschland

HYPERSECURE Platform



Designprinzipien der DriveLock HYPERSECURE Platform

Die DriveLock HYPERSECURE Platform verkörpert Designprinzipien, die sich auf Cloud-First-Strategien für effiziente, skalierbare und stets aktualisierte cloud-verwaltete Endpoint-Sicherheit konzentrieren. Sie betont einen intuitiven Ansatz, der die Komplexität reduziert mit einem zentralisierten Ansatz zur Durchsetzung von Sicherheitsrichtlinien. Die Plattform ist offen, fördert die bidirektionale Integration mit Drittanbietern, priorisiert die Automatisierung für optimierte Prozesse, stellt die Compliance durch Risikoanalyse sicher und bietet plattformübergreifende Sicherheit über verschiedene Betriebssysteme hinweg. Zudem wird ein Open-Cloud-Ansatz verfolgt, der die Nutzung mehrerer Cloud-Anbieter ermöglicht.

DriveLock Lösungen sind Made in Germany und ohne Backdoor

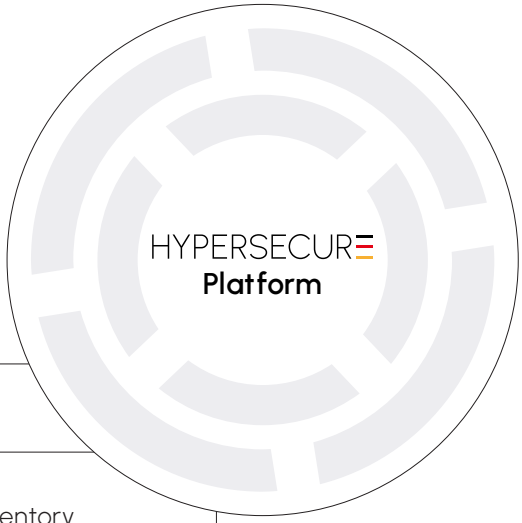
» Schutz von mehreren Millionen verwalteten Endgeräten weltweit

» Kompromisslos abgesicherte Kundenumgebungen mit über 180.000 verwalteten Endgeräten

DriveLock

Ihre Cybersicherheit mit DriveLock

Die DriveLock HYPERSECURE Platform und ihre Module zielen darauf ab, die in ISO 27001 Annex A aufgeführten kritischen Sicherheitskontrollen mit einer umfassenden und kontext-bezogenen Sicherheitsstrategie anzugehen.



Welches DriveLock Modul übernimmt welchen Bereich der kritischen Sicherheitskontrollen:

Security Control	DriveLock Modul
Inventory	Discovery Hardware & Software Inventory
Media Protection	Device Control
Malware Defense	Application Control Defender Antivirus
Secure Configuration	Security Configuration Management
Data Protection	Encryption BitLocker Management
Security Awareness	Security Awareness
Vulnerability Management	Vulnerability Management
Privilege Control	User & Groups Management/SSO
Incident Response	Threat Detection & Response MITRE ATT&CK® Framework

HYPERSECURE IT

MADE IN GERMANY

Jetzt unverbindlich
30 Tage gratis testen

Testversion

Sprechen Sie mit
einem unserer Experten

Termin

HYPERSECURE IT

ISG – Leader Data Leakage/Loss Prevention 2023

Als Ergebnis der Marktuntersuchung „Cyber Security – Solutions & Services Germany 2023" des Technologieberatungsunternehmens ISG wurde DriveLock erneut als ein Leader im Segment „Data Leakage/Loss Prevention" ausgezeichnet.

techconsult – Champion 2024

DriveLock wurde als Champion in zwei Kategorien ausgezeichnet: Endpoint Protection und Vulnerability Management.

Trust Seal www.teletrust.de/itsmig

Trust Seal www.teletrust.de/itsmie

member of bitkom

BDSV Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V.

Mitglied im | Member of TeleTrusT Pioneers in IT security. Bundesverband IT-Sicherheit e.V. IT Security Association Germany

DriveLock

DriveLock SE
Landsberger Str. 396
81241 München

Tel. +49 (89) 546 36 49-0
E-Mail info@drivelock.com

DRIVELOCK.COM

HYPERSECURE IT

Mit der HYPERSECURE Platform
bleiben **Angriffe** auf IT-Systeme da,
wo sie hingehören: **außen vor**.