DriveLock

WHITEPAPER

ERWEITERTE ENDGERÄTESICHERHEIT

mit Microsoft 365 und DriveLock

Von Marc Lemarquis und Falk Trümner

HYBRIDE SICHERHEIT NEU GEDACHT

MICROSOFT 365 UND DRIVELOCK IM ZUSAMMENSPIEL

Durch die intelligente Kombination von Microsoft 365-Security und DriveLock entsteht eine hybride IT-Security-Strategie, die das Beste aus beiden Welten vereint. Während Microsoft 365 die zentrale Cloud-Verwaltung und erweiterte Schutzmechanismen liefert, schließt DriveLock gezielt Lücken bei der Anwendungskontrolle, Gerätekontrolle, BitLocker-Management und Security Awareness. Das Ergebnis sind vereinfachte Prozesse und schlankere Workflows. Unternehmen sparen dadurch spürbar Zeit bei Administration und Audits, reduzieren Risiken und gewinnen volle Transparenz über ihre Endgeräteumgebung – ohne die Produktivität der Mitarbeitenden einzuschränken.

Mit der Integration zusätzlicher Module wie DriveLock Security Awareness, Human Risk Assessment, File Encryption, Vulnerability Management und dem sicheren Datenaustausch durch idgard bietet DriveLock heute eine umfassende Zero-Trust-Plattform, die über rein technische Schutzmaßnahmen hinausgeht. Sie adressiert sowohl den technischen Angriffsvektor als auch den Faktor Mensch – nahtlos kombinierbar mit Microsoft 365. Unternehmen erhalten damit eine Lösung, die nicht nur Schutz bietet, sondern auch aktive Risikoreduzierung, Compliance-Fähigkeit und Anwenderfreundlichkeit in einer Plattform vereint.

GRENZEN VON MICROSOFT 365 – UND WARUM EINE ERGÄNZUNG ENTSCHEIDEND IST

Microsoft Intune und die Microsoft 365-Pläne E3 und E5 bringen zwar schon ein solides Paket an Sicherheitsfunktionen mit, doch in der Praxis zeigen sich schnell Grenzen. Manche Features führen zu zusätzlichem Administrationsaufwand, andere sind nur in Basisform vorhanden oder fehlen ganz. Besonders spürbar wird dies bei der Anwendungskontrolle (Windows Defender Application Control), bei der Kontrolle von internen und externen Geräten und Laufwerken, bei der erzwingbaren Verschlüsselung von Wechseldatenträgern mit BitLocker To Go sowie beim Management der Festplattenverschlüsselung durch BitLocker selbst.

Darüber hinaus fehlen in Microsoft 365 native Module für Security Awareness Trainings und Human Risk Assessment, die das Sicherheitsverhalten von Anwendern messbar und steuerbar machen. Auch eine feingranulare Datei-Verschlüsselung auf Endgeräteebene, wie sie DriveLock File Encryption bietet, ist nicht enthalten. Ebenso wenig ist ein vollwertiges Schwachstellenmanagement verfügbar, das Risiken systematisch erkennt, bewertet und priorisiert.
Für den geschützten, DSGVO-konformen Datenaustausch mit Externen gibt es keine native Alternative zu zertifizierten Lösungen wie idgard. Diese Lücken stellen vor allem in regulierten Branchen oder bei hohem Schutzbedarf erhebliche Risiken dar.

INHALT

1

STRATEGISCHE SICHERHEITSARCHITEKTUR: MICROSOFT 365 E3 ERGÄNZT DURCH DRIVELOCK

STRATEGISCHE SICHERHEITS-ARCHITEKTUR: MICROSOFT 365 E3 ERGÄNZT DURCH DRIVELOCK

Microsoft 365 E3 bietet viele zentrale Funktionen für Kommunikation, Kollaboration und Verwaltung – einschließlich Exchange, SharePoint, OneDrive und Teams. Die Frage, ob eine Kombination aus E3 und DriveLock funktional mit einer E5-Lösung mithalten oder diese sogar übertreffen kann, lässt sich mit einem klaren „Ja" beantworten – wenn man Sicherheit ganzheitlich betrachtet: in Bezug auf Schutzwirkung, Steuerbarkeit, Nutzerfreundlichkeit und Integrationsfähigkeit.

Während E5 zusätzliche Sicherheits- und Compliance-Funktionen wie Defender for Endpoint Plan 2 oder Microsoft Purview enthält, bleiben wichtige Anforderungen wie granulare Gerätekontrolle, automatisierte USB-Verschlüsselung, MFA-fähiges BitLocker-Management, verhaltensbasierte Awareness und revisionssicherer Datentransfer weiterhin nur eingeschränkt erfüllt oder setzen Drittanbieterlösungen voraus.

DriveLock schließt genau diese Lücken: mit einem modularen Zero-Trust-Ansatz, der technische Kontrolle, menschliche Risikobewertung und intelligente A utomatisierung vereint. Hervorzuheben sind dabei unter anderem:

- vollständige Gerätekontrolle bis zur Seriennummer,
- kontextsensitive Awareness-Maßnahmen beim Geräteanschluss,
- lernfähige Anwendungskontrolle,
- integriertes Schwachstellenmanagement,
- automatische Schlüsselrotation bei BitLocker,
- DSGVO-konformer Datentransfer mit idgard.

Alles gesteuert über eine zentrale Plattform mit offenen Schnittstellen, rollenbasiertem Zugriff und flexiblen Betriebsmodellen – On-Premises, in der zertifizierten Cloud oder als SaaS.

Diese Architektur senkt den Administrationsaufwand, reduziert Helpdesk-Tickets und bietet gleichzeitig ein hohes Maß an Sicherheit und Kontrolle – gerade in sensiblen oder regulierten Umfeldern ist E3 + DriveLock oft die überlegene Lösung gegenüber einer reinen E5-Strategie.

FAZIT

Die Kombination von Microsoft 365 E3 und DriveLock bietet ein höheres, praxisnäheres Sicherheitsniveau als E5 allein – bei gleichzeitig höherer Effizienz und Zukunftssicherheit. Sie ist ideal für den Einsatz im öffentlichen Sektor Bayerns als auditfähige, souveräne Sicherheitsarchitektur.

2

GERÄTEKONTROLLE

GERÄTEKONTROLLE

DRIVELOCK VERBINDET LÜCKENLOSE GERÄTEKONTROLLE MIT MAXIMALER BENUTZERFREUNDLICHKEIT.

Mit DriveLock steuern Sie bis zur Seriennummern-Ebene*, welche internen oder externen Laufwerke, USB-Sticks, Bluetooth-Geräte oder auch andere Geräte genutzt werden dürfen – und das ganz bequem über zentrale Richtlinien. Endgeräte erhalten neue Regeln in Sekunden, denn Benutzer können Freigaben selbst anstoßen, ein genehmigender Workflow greift, und die Entscheidung des Administrators wird in Sekunden auf das Zielgerät gepusht. So ist produktives Arbeiten sofort wieder möglich, ohne Help-Desk-Runden.

- **Einheitliches Operations Center**
  Alle Freigaben erfolgen in einer intuitiven Weboberfläche – egal ob USB-Stick, externe SSD oder Bluetooth-LE-Headset. Bei Bluetooth lassen sich zusätzlich Haupt- und Unterklassen (z. B. „Eingabegerät – Maus") granular steuern.
- **Umfassende Kontrolle über alle Geräte- und Laufwerksklassen**
- **Sicherer Datenfluss statt Malware-Risiko**
  Sie können zum Beispiel das Lesen oder Ausführen von ausführbaren Dateien wie EXE oder VBS auf Wechselmedien per Mausklick verbieten oder vor jeder Freigabe einen automatischen Virenscan auslösen. Nur saubere Datenträger erhalten Zugang – Schadsoftware bleibt draußen.
- **Nahtlose Zusammenarbeit mit Datenschleusen**
  DriveLock integriert sich in gängige Datenschleusen und File-Transfer-Gateways. Fremde USB-Medien werden so kontrolliert eingeschleust, ohne die Akzeptanz der Anwender zu verlieren.
- **Schutz vor bösartigen Geräten (Bad-USB)**
  Durch den erweiterten Schutz gegen bösartige Geräte (Bad-USB) werden Techniken wie zum Beispiel Hardware-ID-Spoofing abgewehrt. Vertrauenswürdige Geräte können automatisch vom Agenten angelernt werden, um einen schnellen Rollout zu unterstützen.
- **Security Awareness genau im Moment des Risikos**
  Kontextsensitive Hinweise und Lern-Häppchen informieren Nutzer sofort, wenn sie z.B. ein neues Gerät anschließen. Das reduziert Fehlbedienungen, vereinfacht den Roll-out und verhindert das typische Ticket-Aufkommen in der Startphase.
- **Vollständige Transparenz & Reporting**
  DriveLock verknüpft Benutzer, Computer, Geräte und einzelne Dateien zu einem durchgängigen Inventar – samt aller sicherheitsrelevanten Ereignisse. Dashboards und Reports liefern Audit-Nachweise auf Knopfdruck.
- **Offene API für bestehende Systeme**
  Über die REST-API lesen Sie Ereignisse aus, automatisieren Freigaben und binden UEM-, SIEM- oder CMDB-Lösungen an – so fügt sich DriveLock reibungslos in Ihre Infrastruktur ein.

*Bei Laufwerken und MTP-Geräten

GERÄTEKONTROLLE

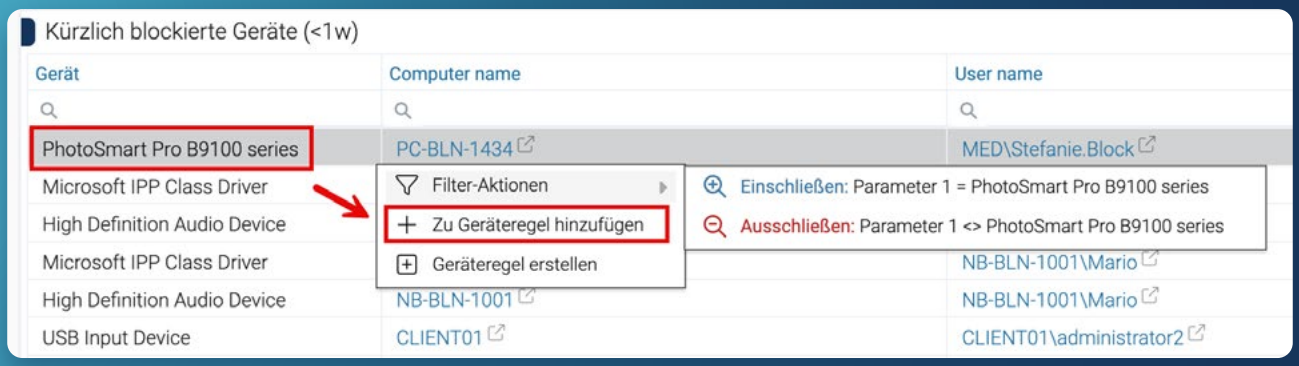
ABGRENZUNG ZU MICROSOFT 365

- **Grundlegende Gerätekontrolle via Intune:**
  Eingeschränkte Steuerung auf Basis von Richtlinien.
- **Keine kontextsensitive Awareness:**
  Es gibt keine unmittelbaren Schulungsmaßnahmen bei Sicherheitsverstößen.
- **Keine vollständige Integration von Genehmigungsprozessen:**
  Freigaben müssen häufig manuell und über andere Tools erfolgen.
- **Kein nativer Schutz gegen Bad-USB-Angriffe.**

MEHRWERTE AUF EINEN BLICK

- Schnellere Freigabe von Laufwerken und Geräten
- Deutlich weniger Administrationsaufwand
- Nachweislich geringeres Malware-Risiko und volle Compliance-Transparenz – alles in einer einzigen Lösung

Vereinfachte Freigabe eines geblockten Geräts über zwei Mausklicks:



So schafft DriveLock die Balance aus maximaler Kontrolle und minimalem Aufwand – und ergänzt Microsoft 365 perfekt, wo Intune und Defender for Endpoint an ihre Grenzen stoßen.

3

VERSCHLÜSSELUNG MOBILER DATENTRÄGER

VERSCHLÜSSELUNG MOBILER DATENTRÄGER

DRIVELOCK – USB-VERSCHLÜSSELUNG OHNE REIBUNGSVERLUSTE

DriveLock erzwingt die Verschlüsselung jedes USB- und sonstigen Wechselmediums, noch bevor sensible Daten geschrieben werden. Gleichzeitig bleiben Arbeitsabläufe geschmeidig: Optionale Dialoge erlauben in klar definierten Ausnahmefällen temporären Klartextzugriff oder alternative Verschlüsselungsmethoden, ohne die Sicherheit zu gefährden.

- **Automatische Verschlüsselung ab dem ersten Byte**
  Medien werden beim ersten Anschließen oder Schreibzugriff sofort verschlüsselt; kein manuelles Eingreifen nötig.
- **Flexible Ausnahme-Workflows**
  Administratoren entscheiden, ob und wann Anwender zeitlich begrenzten Klartextzugriff erhalten. Entweder über benutzerdefinierte Dialoge ohne Zuhilfenahme des Helpdesks oder per Unlock-Mechanismen.
- **Transparenter Zugriff & Auto-Unlock**
  Benutzer-, Computer- oder Gruppen-SIDs entsperren Medien nahtlos; mehrere Schlüsselträger sind möglich.
  Ebenso ist es möglich persönliche Kennwörter zu verwenden, ist dies nicht gewünscht, kann ein Unternehmenskennwort festgelegt werden, so ist der Zugriff nur auf einem Unternehmensendgerät möglich.
- **Sofort-Recovery online & offline**
  Verlorene Passwörter können per Challenge-Response wieder zurückgesetzt werden. Auf unternehmensfremden Geräten ist der Zugriff bei Verlust des Kennworts wie gewohnt über den BitLocker Recoverykey möglich.
- **Sichere Wiederherstellung**
  Recovery-Keys werden automatisch verschlüsselt in der zentralen DriveLock Datenbank abgelegt. Beim Zugriff auf die Wiederherstellungsschlüssel werden diese automatisch rotiert. Zyklisches rotieren des Schlüssels ist ebenso möglich.
- **Offene API für nahtlose Integration**
  Verschlüsselungs-Events fließen per REST-API oder Syslog in SIEM-Systeme. Zudem können über die API Widerherstellungsinformationen abgerufen werden. Eine Integration in ITSM-Systeme ist somit möglich.

*Bei Laufwerken und MTP-Geräten

VERSCHLÜSSELUNG MOBILER DATENTRÄGER

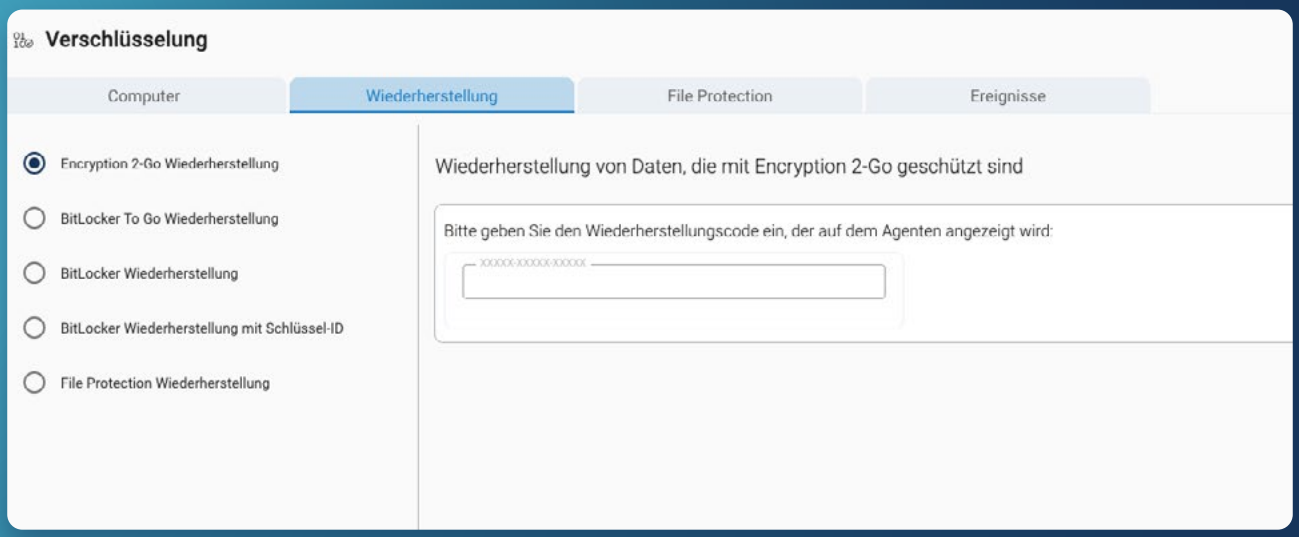
ABGRENZUNG ZU MICROSOFT 365

- **Nur Basisschutz vorhanden:**
  BitLocker To Go kann Wechselmedien verschlüsseln, bietet jedoch keine zentrale, regelbasierte Verwaltung der Verschlüsselung.
- **Keine Ausnahmeverwaltung oder Auto-Unlock-Mechanismen.**
- **Kein Recovery-Portal.**
- **Administrativer Overhead für Helpdesk deutlich höher.**

MEHRWERTE AUF EINEN BLICK

- Zero-Touch-Compliance für DSGVO, ISO 27001, BSI-Grundschutz und andere Compliance Vorgaben
- schnelle Recovery-Wege
- nahtlose Microsoft-Integration und minimale Benutzerunterbrechung

Vereinfachte Möglichkeit der Wiederherstellung von Passwörtern über wenige Mausklicks:



4

ANWENDUNGS-KONTROLLE

ANWENDUNGSKONTROLLE

DRIVELOCK – PRÄZISE ANWENDUNGSKONTROLLE, BLITZSCHNELL PRODUKTIV

DriveLock vereint flexibles Allow-/Denylisting mit smarten Assistenten und bringt Anwendungskontrolle in Rekordzeit zum Laufen. Regeln entstehen per Mausklick – kombiniert nach Pfad, Hash, Version, Produkteigenschaft, Besitzer, Beschreibung oder Signatur.

- **Regel-Assistent & Lernmodus**
  Ganze Ordner, Laufwerke, MSI-Pakete oder aufgezeichnete Events können mit einem intelligenten Regelassistenten schnell und einfach in Freigabe- oder Blockregeln umgewandelt werden; der lokale Lernmodus scannt installierte Anwendungen und aktiviert sofortigen Schutz.
- **Trusted Installer & sichere Quellen**
  Autorisierte UEM- und Patch-Tools, Ablageorte oder Benutzer installieren Updates und neue Applikationen, auch wenn diese noch unbekannt sind; neue Versionen sind danach automatisch erlaubt.
- **Drag-and-Drop-Pflege im Operations Center**
  Zentrale und lokale Regeln lassen sich kombinieren, blockierte Apps mit allen Metadaten analysieren und bei Bedarf freigegeben werden – alles schnell und intuitiv im Browser.
- **Feingranulare Rechte für freigegebene Apps**
  Definieren Sie Datei- und Registry-Zugriffe, erlaubte Kommandozeilenparameter oder Prozessketten für erlaubte Anwendungen bis ins Detail. So können Living off the Land Angriffe oder die Ausnutzung bereits genehmigter Applikationen verhindert werden.
- **Umfassende Skriptkontrolle**
  PowerShell-, VB-, Batch- und eigene Skripttypen werden identisch geprüft – nach Pfad, Hash oder, wenn möglich, Signatur.
- **Stufenweiser Roll-out ohne Risiko**
  Protokoll-, Simulations- und Erzwingungsmodus sorgen für eine Einführung ohne Produktivitätsverlust. Das Regelwerk kann vor Inbetriebnahme sicher im Feld getestet und so ein erfolgreicher Rollout gewährleistet werden.
- **Vollständiges Software-Inventar & Reporting**
  DriveLock inventarisiert Software, Zertifikate und Prozesse und verknüpft sie mit Benutzer- und Geräteobjekten – perfekt für Audits und Compliance-Berichte.

*Bei Laufwerken und MTP-Geräten

ANWENDUNGSKONTROLLE

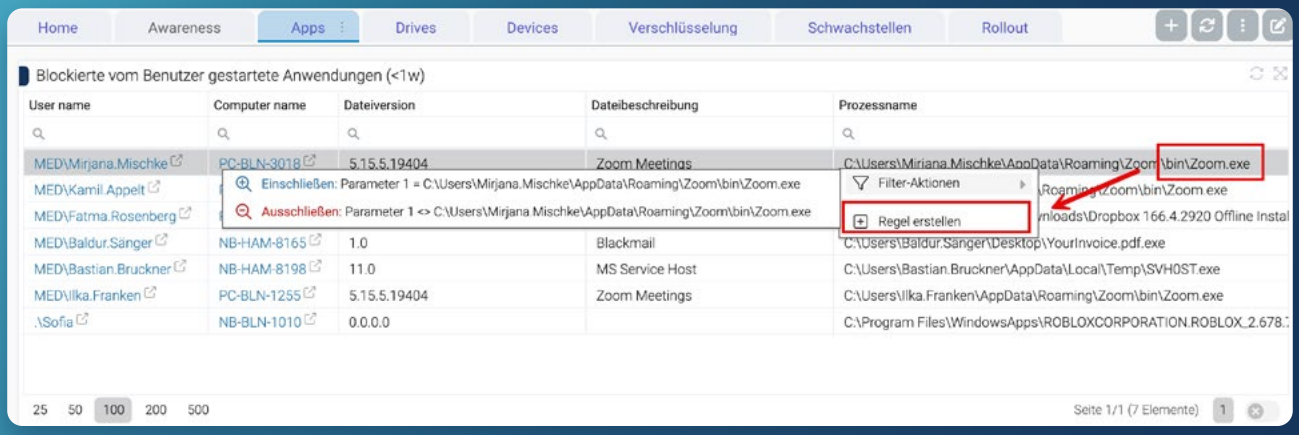
ABGRENZUNG ZU MICROSOFT 365

- **Komplizierte Einrichtung:**
  Hohes Know-how erforderlich, Regeln müssen über XML oder PowerShell gepflegt werden.
- **Keine Unterstützung für dynamisches Lernen oder Simulationsbetrieb.**
- **Keine Integration in kontextsensitive Awareness oder Risk Scores.**
- **Eingeschränkte Audit-Funktionalitäten.**

MEHRWERTE AUF EINEN BLICK

- Schneller Schutz
- Reibungslose Updates
- Granulare Rechteverwaltung
- Risikoarmer Roll-out und lückenlose Transparenz – alles zentral steuerbar

Vereinfachte Freigabe einer geblockten Anwendung über zwei Mausklicks:



5

VULNERABILITY MANAGEMENT RISIKEN ERKENNEN, BEVOR SIE AUSGENUTZT WERDEN

VULNERABILITY MANAGEMENT RISIKEN ERKENNEN, BEVOR SIE AUSGENUTZT WERDEN

DRIVELOCK – SCHWACHSTELLENANALYSE MIT DIREKTEM HANDLUNGSPFAD

Das Modul Vulnerability Management ergänzt DriveLock um eine proaktive Erkennung und Bewertung sicherheitskritischer Schwachstellen in Betriebssystemen, Anwendungen und Konfigurationen – bevor Angreifer sie ausnutzen können. Microsoft 365 bietet mit Defender for Endpoint nur rudimentäre Schwachstellenberichte, meist ohne automatische Priorisierung oder direkte Verknüpfung mit Kontrollrichtlinien.

Funktionen des DriveLock Vulnerability Management:

- **Automatische Schwachstellenerkennung** basierend auf CVE-Datenbanken
- **Bewertung nach CVSS-Score,** Asset-Bedeutung und Exposition
- **Kombinierbar mit Application Control,** um gefährdete Software direkt zu blockieren
- **Zentrale Auswertung im Dashboard –** ideal für Compliance, Audits & Patch-Management
- **Handlungsempfehlungen & Alerting,** inklusive Eskalation bei kritischen Risiken

Beispiel aus der Praxis:

Ein veralteter Browser mit bekannter Zero-Day-Schwachstelle wird erkannt. DriveLock priorisiert diesen Fund automatisch und blockiert über die Anwe dungskontrolle den Start der betroffenen Anwendung, bis ein Patch verfügbar ist. Zusätzlich wird der betroffene Nutzer durch einen Awareness-Hinweis informiert.

VULNERABILITY MANAGEMENT RISIKEN ERKENNEN, BEVOR SIE AUSGENUTZT WERDEN

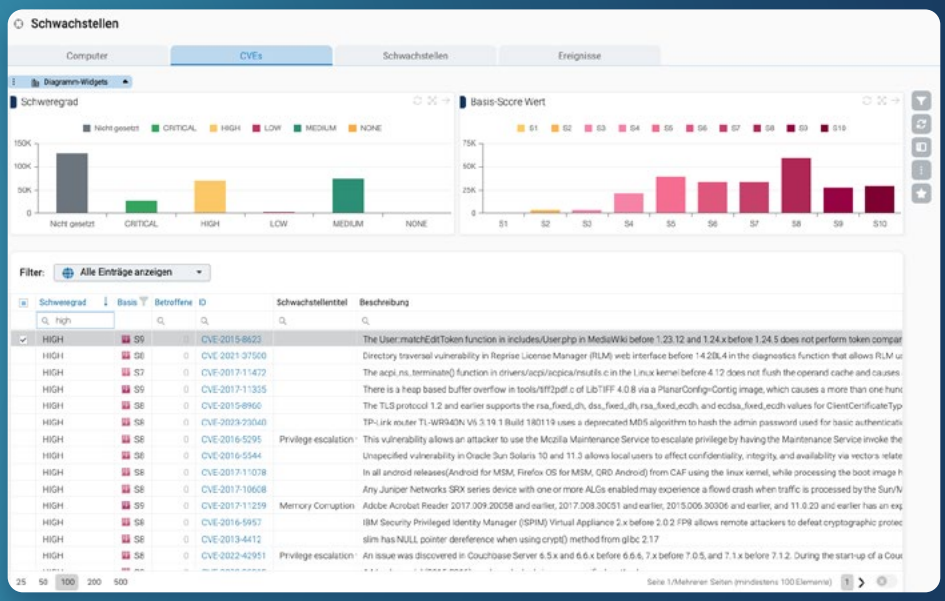
ABGRENZUNG ZU MICROSOFT 365

Microsoft Defender bietet teilweise eine Schwachstellenanalyse, allerdings:

- **Nur im E5-Plan vollständig verfügbar**
- **Keine native Anbindung an Gerätekontroll- oder Blockierungsmechanismen**
- **Kein Asset-übergreifendes Reporting für IT- und Sicherheitsverantwortliche**

MEHRWERTE AUF EINEN BLICK

- Frühzeitige Identifikation & Risikobewertung
- Automatische Reaktion durch dynamische Richtlinien-Verknüpfung
- Zentrale Übersicht für IT-Security, Management und Revision



6

BITLOCKER MANAGEMENT

BITLOCKER MANAGEMENT

DRIVELOCK – ZENTRALES BITLOCKER-MANAGEMENT, MAXIMAL ABGESICHERT

DriveLock erweitert Microsoft BitLocker um richtliniengestütztes Management, MFA-fähige Pre-Boot-Authentifizierung und automatische Schlüsselrotation – alles in einer einzigen Konsole.

- **Wizard-gestützter Roll-out**
  TPM-only, Microsoft-PBA (PIN/Passwort) oder mehrbenutzer-fähige DriveLock-PBA (MFA mit YubiKey, Smartcard, Netz-Boot) in wenigen Minuten einsatzbereit; bereits verschlüsselte Geräte werden ohne Neuverschlüsselung übernommen.
- **Flexible Pre-Boot-Authentifizierung,**
  Wechsel von TPM-only zu PBA-Passwort erfolgt automatisch bei Geräteausgabe an den Endnutzer.
- **Automatische Schlüsselrotation & TPM-Hardening**
  Schlüssel wechseln zeit- oder ereignisbasiert, z. B. direkt nach Recovery – das Kennwort für die BitLocker PBA kann ebenfalls zyklisch geändert werden; TPM-Konfiguration wird zentral erzwungen.
- **Conditional-Access-Signal & Azure-Key-Integration**
  Recovery-Keys landen sicher in Azure AD; Geräte ohne korrekte Verschlüsselung verlieren Cloud-Zugriff, bis DriveLock den Soll-Status meldet.
- **Dashboards & Echtzeit-Reporting**
  Verschlüsselungsgrad, PBA-Modus und Events stehen live bereit und lassen sich via API an andere Systeme weiterleiten.
- **Offene API & Self-Service Recovery**
  Help-Desk-Mitarbeiter oder Endnutzer rufen Keys über gesicherte Workflows ab – ohne Medienbruch.

BITLOCKER MANAGEMENT

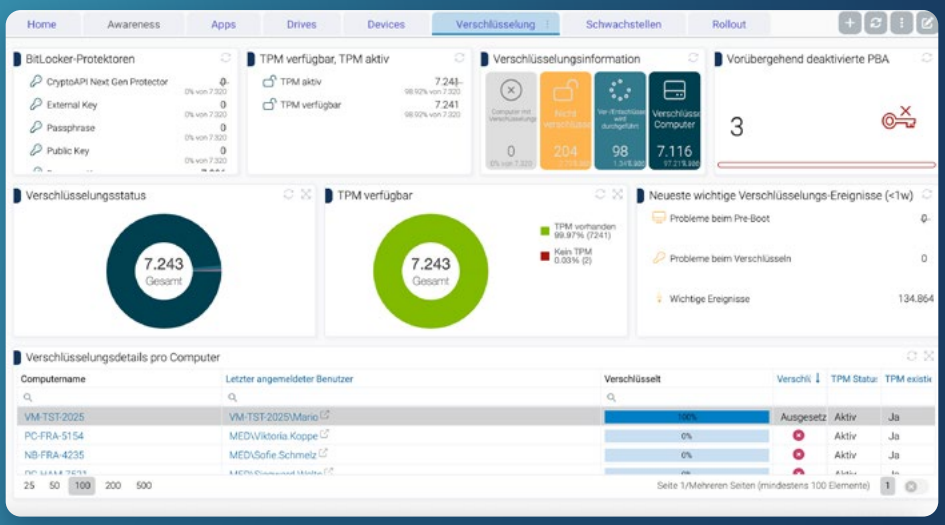
ABGRENZUNG ZU MICROSOFT 365

- **Nur Basis-Management über Intune:**
  Keine MFA-Unterstützung für PBA.
- **Keine automatische Rotation oder erweiterte Recovery-Prozesse.**
- **Kein zentralisiertes, detailliertes Reporting oder Dashboards.**
- **Begrenzte Steuerung und Kontrolle in hybriden Szenarien.**

MEHRWERTE AUF EINEN BLICK

- Schneller Roll-out
- MFA-fähige PBA
- automatische Schlüsselrotation
- Echtzeit-Dashboards
- nahtlose Microsoft-Integration – mehr Kontrolle bei weniger Aufwand.

Zentrale Übersicht über den Verschlüsselungsstatus aller Systeme:



7

SECURITY AWARENESS & HUMAN RISK ASSESSMENT

SECURITY AWARENESS & HUMAN RISK ASSESSMENT

DriveLock – Nutzer sensibilisieren, Risiken erkennen, Verhalten nachhaltig verbessern

Ein entscheidender Unterschied zwischen DriveLock und Microsoft 365 liegt in der verhaltensbasierten Sicherheitsstrategie. Während Microsoft 365 sich primär auf technische Schutzmaßnahmen konzentriert, bietet DriveLock über die Lösung DriveLock Security Awareness zwei entscheidende Module, die es so in Microsoft 365 nicht gibt: Security Awareness Training und Human Risk Assessment.

Integriertes Security Awareness – genau im Moment des Risikos

DriveLock hebt sich durch kontextbezogene Security Awareness Maßnahmen hervor. Diese sind direkt mit sicherheitsrelevanten Ereignissen aus anderen Modulen (z. B. Device Control, Application Control) verknüpft und können so just-in-time Lerninhalte anzeigen, wenn ein Risiko tatsächlich auftritt – etwa beim Einstecken eines neuen USB-Sticks oder dem Versuch, eine nicht genehmigte Applikation zu starten.

Beispiel

Ein Benutzer steckt einen unbekannten USB-Stick ein > DriveLock blockiert den Zugriff > gleichzeitig erscheint ein kurzer DriveLock Security Awareness Clip zum Thema „Gefahren durch unbekannte USB-Geräte". Das sorgt für sofortige Verhaltensänderung, ohne Helpdesk-Tickets oder abstrakte Schulungen.

Human Risk Assessment – der Risikofaktor Mensch messbar gemacht

Über DriveLock Human Risk Assessment lassen sich anonymisierte, verhaltensbasierte Risikoanalysen pro Nutzergruppe durchführen. Dabei werden etwa Klickverhalten, Passwortsicherheit, Social Engineering Anfälligkeit und Reaktionszeiten auf simulierte Phishing-Versuche ausgewertet. Die Ergebnisse fließen in einen Human Risk Score, der sich mit DriveLock zentral auswerten und zur Priorisierung von Maßnahmen nutzen lässt.

Microsoft 365 bietet keine vergleichbare Komponente. Zwar gibt es im M365 Defender rudimentäre Nutzerstatistiken und Angriffsverläufe, aber kein strukturiertes Trainings- oder Bewertungsframework für menschliche Sicherheitsrisiken.

SECURITY AWARENESS & HUMAN RISK ASSESSMENT

VORTEILE DURCH DIE KOMBINATION MIT DEN DRIVELOCK-KERNMODULEN

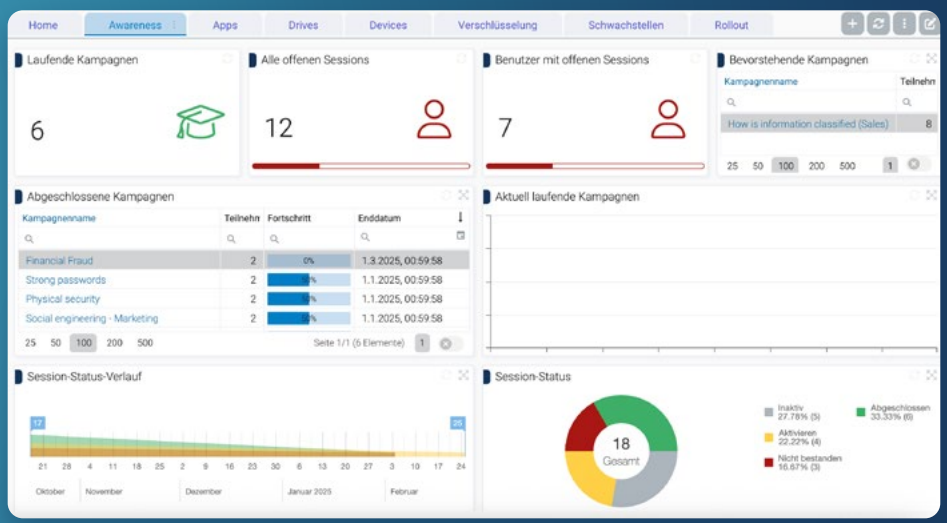
Die Verknüpfung mit den klassischen DriveLock-Modulen schafft einen einzigartigen Mehrwert:

- **Kontextuelle Awareness beim Auftreten realer Risiken** (z. B. verdächtige App-Ausführung → Awareness-Clip zu Malware-Methoden)
- **Maßnahmen aus dem Human Risk Score** können direkt in Regelwerke übersetzt werden (z. B. höhere Kontrollstufe für risikobehaftete Nutzergruppen)
- **Managementberichte und Dashboards** enthalten nun auch verhaltensbasierte Kennzahlen – perfekt für Audits und Awareness KPIs

MEHRWERTE AUF EINEN BLICK

- **Grundlegende echte Verhaltensänderung** statt nur technischer Kontrolle
- **Integration statt Insellösungen** Awareness-Training, Risikoeinschätzung und technische Schutzmaßnahmen greifen ineinander
- **Keine Entsprechung in Microsoft 365** Awareness und Human Risk sind dort nur in Form allgemeiner Empfehlungen oder externer Drittanbieterlösungen verfügbar
- **Ideal für Zero-Trust-Strategien** bei denen der Faktor Mensch nicht außen vor bleiben darf

Zentrale Übersicht aller Security Awareness Kampagnen:



8

DATEI- UND ORDNERVERSCHLÜSSELUNG – GEZIELTE VERSCHLÜSSELUNG SENSIBLER DATEIEN

DATEI- UND ORDNERVERSCHLÜSSELUNG – GEZIELTE VERSCHLÜSSELUNG SENSIBLER DATEIEN

DRIVELOCK – SCHUTZ AUF DATEIEBENE, UNABHÄNGIG VOM SPEICHERORT

Mit dem Modul File Encryption erweitert DriveLock den Schutz von Daten gezielt auf Einzeldateien und Ordner. Während Microsoft 365 in der Cloud auf Azure Information Protection setzt, fehlt eine native, plattformunabhängige Datei-Verschlüsselung direkt am Endpoint. Genau hier setzt DriveLock an – mit starker, regelbasierter Verschlüsselung auf Dateiebene, die nahtlos mit Device Control und Removable Media Encryption kombinierbar ist.

- **Vorteile der DriveLock File Encryption:**
- **Zielgerichtete Verschlüsselung einzelner Dateien**
  auch außerhalb verschlüsselter Datenträger
- **Transparente Nutzung**
  Autorisierte Nutzer arbeiten ohne Mehraufwand mit geschützten Dateien
- **Nahtlose Integration in bestehende DriveLock-Sicherheitsrichtlinien**
- **Individuelle Verschlüsselungsschlüssel pro Benutzer, Datei oder Gerätegruppe**
- **Offline-Nutzung möglich, bei gleichzeitiger Kontrolle der Entschlüsselung**

ABGRENZUNG ZU MICROSOFT 365

Microsoft bietet mit AIP (Azure Information Protection) eine Cloud-zentrierte Rechteverwaltung, jedoch keine granulare Dateiverschlüsselung direkt auf dem lokalen Gerät, die ohne Azure-Cloud funktioniert oder DSGVO-konform vollständig On-Premises bleiben kann.

MEHRWERTE AUF EINEN BLICK

- Grundlegende Schutz einzelner Dateien – auch außerhalb der Microsoft-Welt
- DSGVO-konform, auch bei externer Weitergabe
- Kombinierbar mit weiteren DriveLock-Schutzmechanismen
- Schutz sensibler Daten direkt an der Quelle – nicht erst in der Cloud

9

SICHERER DATEN-AUSTAUSCH MIT DRIVELOCK & IDGARD

SICHERER DATENAUSTAUSCH MIT DRIVELOCK & IDGARD

DRIVELOCK – JETZT MIT IDGARD FÜR REVISIONSSICHEREN, DSGVO-KONFORMEN DATENTRANSFER

Durch die Übernahme von idgard, einem führenden Anbieter für datenschutzkonformen File-Transfer und virtuelle Datenräume, erweitert DriveLock seine Sicherheitsplattform um einen weiteren kritischen Bereich: den geschützten Austausch sensibler Dateien und Dokumente – intern wie extern. Die Kombination aus DriveLock Geräteschutz, Datenverschlüsselung, Human Risk Assessment und idgard bietet einen ganzheitlichen Schutz vom Endgerät bis zur Cloud.

Sichere Alternative zu unsicheren File-Sharing-Lösungen

Microsoft 365 bietet mit OneDrive und SharePoint zwar integrierte Speicher- und Sharing-Funktionen, jedoch fehlt oft die Möglichkeit, hochvertrauliche Dokumente revisionssicher, vollständig DSGVO-konform und ohne Zugriff durch US-Anbieter zu teilen – insbesondere in regulierten Branchen oder bei Ausschreibungen und M&A-Prozessen.

idgard bietet hier:

- Virtuelle Datenräume mit klar definierter Rollenverteilung und Nachvollziehbarkeit
- Ende-zu-Ende-verschlüsselten Austausch, bei dem nur befugte Empfänger Zugriff erhalten
- Zero-Knowledge-Prinzip – selbst Betreiber erhalten keinen Zugriff auf die Inhalte
- Zugriff ohne Softwareinstallation, auch für externe Partner

Kombination mit DriveLock – durchgängiger Schutz bis zur Dateiübertragung

Die Stärken von idgard entfalten sich besonders, wenn sie mit den bestehenden DriveLock-Funktionen kombiniert, werden:

- Nur autorisierte und verschlüsselte Dateien gelangen durch Device Control & Application Control in die idgard-Umgebung
- Nutzer mit hohem Human Risk Score (aus DriveLock Security Awareness) können gezielt restriktiver behandelt oder sensibilisiert werden
- Audit-Trails und Reporting lassen sich gemeinsam auswerten, z. B. bei regulatorischen Prüfungen

SICHERER DATENAUSTAUSCH MIT DRIVELOCK & IDGARD

BEISPIEL

Ein Mitarbeiter will einen vertraulichen Projektbericht an einen externen Partner senden. DriveLock prüft:

- Gerät ist verschlüsselt & zugelassen
- Datei stammt aus erlaubter Applikation
- Nutzer hat ausreichenden Sicherheitsstatus

> Über idgard wird die Datei dann sicher über einen temporären Datenraum bereitgestellt, mit vollständigem Audit-Log – ohne die Risiken klassischer E-Mail-Anhänge oder öffentlicher Cloud-Speicher.

ABGRENZUNG ZU MICROSOFT 365

- File-Sharing vorhanden, aber nicht revisionssicher oder vollständig DSGVO-konform.
- Cloud-Infrastruktur unter US-Jurisdiktion kann problematisch sein.
- Keine granulare Verknüpfung mit Endgeräte- oder Risikozustand.

MEHRWERTE AUF EINEN BLICK

- Ende-zu-Ende-Datenschutz, der weit über Microsoft 365 hinausgeht
- Zertifizierte Lösung für DSGVO, TISAX, ISO 27001 u.a.
- Nahtlose Integration mit DriveLock Modulen
- Deutscher Anbieter – keine Datenübertragung in Drittländer
- Besonders geeignet für sensible Branchen wie Behörden, Gesundheitswesen, Automotive, Legal oder Forschung

10

EIN GANZHEITLICHES SICHERHEITSKONZEPT MIT DRIVELOCK

EIN GANZHEITLICHES SICHERHEITSKONZEPT MIT DRIVELOCK

So schafft DriveLock die Balance aus maximaler Kontrolle und minimalem Aufwand – und ergänzt Microsoft 365 perfekt. Es werden genau jene Lücken geschlossen, an denen die nativen Bordmittel von Microsoft 365, Intune und Defender for Endpoint an ihre Grenzen stoßen. So bildet sich durch DriveLock ein durchgängiger Schutzkreislauf vom BIOS-Start bis zum Datenaustausch – kompakt in einer Webkonsole.

Mit den zusätzlichen Modulen für Security Awareness, Human Risk Assessment, File Encryption, Vulnerability Management und den zertifizierten Datenaustausch via idgard wird DriveLock zu mehr als nur einer Ergänzung – es wird zur strategischen Sicherheitsplattform für moderne Unternehmen. Besonders in hybriden Infrastrukturen mit Microsoft 365 als Grundlage liefert DriveLock die notwendige Verhaltensintelligenz, technische Tiefe und Reaktionsfähigkeit, um ein ganzheitliches Zero-Trust-Konzept erfolgreich und zukunftssicher umzusetzen.

1. Mandantenfähigkeit

DriveLock erlaubt eine klare Trennung verschiedener Organisationseinheiten innerhalb einer gemeinsamen Plattform:

- Ideal für Unternehmensgruppen, internationale Standorte oder Dienstleister mit mehreren Kundenumgebungen.
- Einheitliche Sicherheitsrichtlinien bei gleichzeitiger Eigenständigkeit der einzelnen Bereiche. that underpins trade, innovation, and essential public services.

2. Fein abgestuftes Rollen- und Rechtemanagement

- Rechte und Zuständigkeiten lassen sich exakt auf Benutzergruppen, Aufgabenbereiche und Verantwortlichkeiten zuschneiden.
- Unterstützt die Trennung von Aufgabenbereichen und erfüllt damit zentrale Anforderungen von Audits und Prüfinstanzen.

3. Flexible Betriebsmodelle

- DriveLock kann vollständig im eigenen Rechenzentrum (On-Premises), in einer privaten oder staatlich zertifizierten Cloud (z.B. Delos), oder als Software-as-a-Service (SaaS) betrieben werden.
- Dadurch lassen sich unterschiedliche Anforderungen an Datenschutz, Compliance und IT-Strategie optimal abdecken. third-party suppliers.

EIN GANZHEITLICHES SICHERHEITSKONZEPT MIT DRIVELOCK

4. Ein einziger, modularer Sicherheitsagent

- Alle Sicherheitsfunktionen – von der Gerätekontrolle über Verschlüsselung bis zur Awareness – laufen über einen einzigen, ressourcenschonenden Agenten.
- Das reduziert Installations- und Wartungsaufwand sowie technische Komplexität.

5. Schnittstellen für die Systemintegration

- DriveLock bietet eine offene Programmierschnittstelle (REST-API) für die Anbindung an bestehende IT-Systeme (z. B. SIEM, IT-Service-Management, Unified Endpoint Management).
- Dies ermöglicht die Automatisierung von Abläufen sowie die nahtlose Einbindung in bestehende IT-Prozesse.

6. Zentrales Monitoring und Prüfberichterstattung

- Live-Dashboards, Berichte und Protokolle geben in Echtzeit Einblick in den Sicherheitsstatus Ihrer Umgebung.
- Diese Berichte sind ideal für interne Revisionen, Zertifizierungen (z. B. ISO 27001, BSI-Grundschutz) oder gesetzlich vorgeschriebene Nachweise.

Mit dieser Architektur fügt sich DriveLock nahtlos in bestehende IT-Strukturen ein und ermöglicht Unternehmen, Ihre Sicherheitsstrategie modular, skalierbar und effizient zu gestalten – mit voller Kontrolle über Technik, Verhalten und Prozesse.

DriveLock

Alles aus einer Hand:
DriveLock bietet seine Endpoint Protection-Lösungen als einen Baustein einer HYPERSECURE Platform zur Realisierung einer gesamtheitlichen Sicherheitsstrategie an.

Kontaktieren Sie uns.

DriveLock SE
Landsberger Straße 396
81241 München
Telefon +49 (0) 89 5463649-0
E-Mail info@drivelock.com

www.drivelock.com