kuppingercole ANALYSTS

# CoreView

Jonathan Care

October 23, 2025

EXECUTIVE VIEW

CoreView ist eine auf Microsoft 365 spezialisierte Cyber Resilience-Plattform, die die Umsetzung von Zero Trust-Konzepten, eine granulare Least Privilege-Verwaltung und eine umfassende Automatisierung ermöglicht, um komplexe Unternehmensumgebungen zu sichern und in einheitlicher Weise zu schützen. Die eigenentwickelte Virtual Tenant-Architektur, KI-gestützte Workflows und Funktionen für die Umsetzung regulatorischer Compliance adressieren sowohl Sicherheits- als auch Betriebsanforderungen, insbesondere für Unternehmen in regulierten Märkten. Mit kontinuierlichem Wachstum und als profitables Unternehmen liefert CoreView spezialisierte Lösungen, die die IAM-Strategien für den spezifischen Bereich von Microsoft 365 ergänzen.

# Inhalt



# Abbildungen

# Die Microsoft 365 Security Challenge

Microsoft 365 hat sich von einer Produktivitätssuite zum Identitäts- und Kollaborationsrückgrat moderner Unternehmen entwickelt. Dieser Wandel bringt eine nie dagewesene Komplexität und Risiken mit sich. Wenn bei Microsoft 365 Störungen auftreten, kommt der Geschäftsbetrieb zum Erliegen, was sie gleichzeitig zu einer der kritischsten und am schwierigsten zu sichernden Plattformen in der Unternehmens-IT macht.

Die administrative Komplexität von Microsoft 365 darf nicht unterschätzt werden. Unternehmen müssen sich mit Tausenden von Konfigurationseinstellungen auseinandersetzen, die auf mehrere administrative Schnittstellen verteilt sind, von denen jede spezielle Kenntnisse erfordert und unterschiedliche Funktionen unterstützt. Die Plattform stellt Dutzende von Workloads bereit, darunter Teams, SharePoint, Exchange und OneDrive, die alle miteinander verbunden und dennoch individuell konfigurierbar sind. Diese Komplexität wird durch die außerordentlich umfangreichen privilegierten Zugriffsberechtigungen der Microsoft 365-Administrationsrollen noch verstärkt. Globale Administratoren haben uneingeschränkten Zugriff auf alle Tenant-Ressourcen, während selbst vermeintlich eingeschränkte Rollen, wie die des Benutzeradministrators, über Berechtigungen verfügen, die Anforderungen der meisten Anwendungsszenarien weit übersteigen.

Die Verwaltung des Identitätslebenszyklus im Rahmen von Microsoft 365 stellt besondere Herausforderungen dar, die im Laufe der Zeit noch zunehmen. Die Anzahl der Gastnutzer erhöht sich durch intensive Nutzung der externen Zusammenarbeit. Diese Nutzerkonten sind oft noch lange nach Abschluss der Projekte aktiviert, sofern sie nicht adäquat verwaltet und rechtzeitig deaktiviert werden. Mitarbeiter sammeln Berechtigungen an, wenn sie zwischen verschiedenen Rollen wechseln. Nur selten geben Mitarbeitende Zugriffsrechte ab, die sie für ihre aktuelle Position nicht mehr benötigen.". Heutzutage schaffen auch OAuth Consent Flows und Anwendungsregistrierungen IT-Schattenrisiken, da Benutzer Anwendungen von Drittanbietern ohne angemessene Aufsicht autorisieren. Diese Faktoren führen zu einer Umgebung, in der der aktuelle Zustand der Konfiguration und der Benutzerkonten mit ihren Berechtigungen, ohne aktive Verwaltung, unvermeidlich von den definierten und genehmigten Sicherheitsregeln abweicht und damit Sicherheitsrisiken schafft.

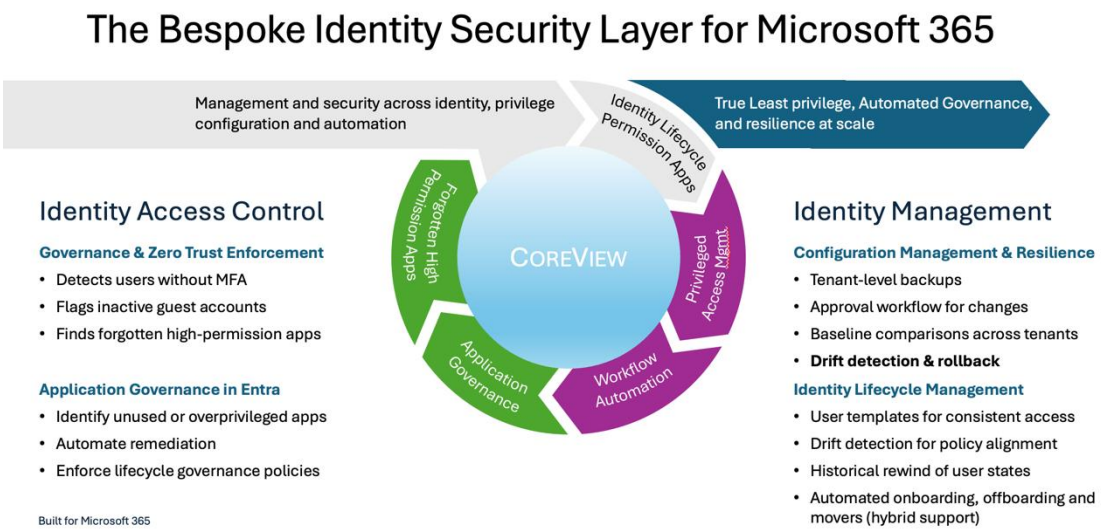


Abbildung 1: CoreView M365 Identity Security & Resilience

Trotz ständiger Verbesserungen der nativen Microsoft-Verwaltungswerkzeuge gibt es nach wie vor erhebliche Lücken bei der Sicherheit und Resilienz. Die von Microsoft bereitgestellten Administrationswerkzeuge bieten zwar einige Delegationsmöglichkeiten, können aber die Tenant-Verwaltung nicht vollständig nach Abteilungen, Regionen oder Geschäftsbereichen aufteilen, wie es Unternehmen benötigen. Die nativen Backup-Funktionen konzentrieren sich in erster Linie auf die Datenerhaltung und nicht auf den Konfigurationsstatus, wodurch Unternehmen anfällig für Manipulationen der Konfiguration von Microsoft 365, einschließlich der Sicherheitseinstellungen, ebenso wie gegen versehentliche Konfigurationsfehler sind. Komplexe, mehrstufige Workflows erfordern umfangreiche PowerShell-Skripte oder manuelle Prozesse. Beim Logging und damit in den Audit-Protokollen fehlt der Geschäftskontext, der für ein effektives Sicherheits- und Resilienzmanagement sowie für die Erstellung aussagekräftiger Berichte notwendig ist. Diese Berichte und Auswertungen sind ein wesentlicher Dreh- und Angelpunkt für eine starke Sicherheit- und Cyber-Resilienz.

Herkömmliche Plattformen für Identity and Access Management (IAM) und Privileged Access Management (PAM) gehen diese Herausforderungen aus einer eher generischen, unternehmensweiten Perspektive an und bieten umfassende Funktionen, die Microsoft 365 aber einfach als eine weitere Anwendung im Portfolio behandeln. Dieser generalisiert Ansatz wird der einzigartigen Komplexität und dem kritischen Charakter des Microsoft 365-Ökosystems nicht gerecht. In ähnlicher Weise unterstützen SaaS Security Posture Management (SSPM)-Tools Hunderte von Anwendungen und bieten so einen breiten Einblick, aber ohne die für ein effektives Microsoft 365-Sicherheits- und Resilienzmanagement erforderliche Tiefe. Die Kombination aus Komplexität, Kritikalität und der Unzulänglichkeit bestehender Lösungen schafft einen klaren Bedarf an spezialisierten Microsoft 365-Sicherheits- und Resilienzlösungen.

# CoreView Übersicht

Das 2014 gegründete Unternehmen CoreView mit Hauptsitz in Italien entstand aus der Erkenntnis, dass Microsoft 365 speziell entwickelte Sicherheits- und Resilienzfunktionen benötigt, die über die von nativen Tools oder generischen Plattformen bereitgestellten Funktionen hinausgehen. Das Unternehmen ist auf mehr als 500 Unternehmenskunden weltweit angewachsen und ist besonders stark in regulierten Branchen wie dem Finanzdienstleistungssektor, dem Gesundheitswesen und dem öffentlichen Sektor, wo Sicherheits- und Resilienzlücken schwerwiegende Folgen haben.

CoreViews strategische Entscheidung, sich ausschließlich auf Microsoft 365 zu konzentrieren, ist sowohl seine größte Stärke als auch sein entscheidendes Merkmal. Diese Spezialisierung ermöglicht eine tiefe API-Integration mit allen Microsoft 365-Diensten, eine umfassende Automatisierung, die weit über die nativen Funktionen hinausgeht, und die Entwicklung spezieller Workflows für Microsoft 365-spezifische Szenarien. Die Plattform hält mit der raschen Entwicklung der von Microsoft entwickelten Funktionen Schritt, so dass Sicherheits- und Resilienzfunktionen für neue Microsoft 365-Funktionen oft schon wenige Wochen nach deren Veröffentlichung zur Verfügung stehen.

Dieser fokussierte Ansatz unterscheidet sich von anderen Plattformen mit einer breiten Unterstützung einer Vielzahl von Systemen durch die Tiefe in der Unterstützung von Microsoft 365 - eine bewusste strategische Entscheidung, die bei Unternehmen, in denen Microsoft 365 eine kritische Komponente der IT-Infrastruktur darstellt, Anklang findet. Anstatt mit den IAM-Plattformen von Unternehmen zu konkurrieren, positioniert sich CoreView als ergänzenden Layer, der die für einen sicheren und stabilen Betrieb von Microsoft 365 erforderlichen speziellen Sicherheits- und Resilienzfunktionen bietet. Diese Positionierung hat ein stetiges Wachstum und Rentabilität ermöglicht und die Marktnachfrage nach spezialisierten Microsoft 365-Sicherheits- und Resilienzlösungen bestätigt.

## Kernkompetenzen

### Konfigurationsmanagement und Backup

Die Bedrohung durch Ransomware und Insider-Angriffe hat das Konfigurationsmanagement von einer nützlichen Funktion im IT-Betrieb zu einer wichtigen Sicherheitsanforderung gemacht. Eine angegriffene oder falsch konfigurierte Tenant-Umgebung kann den Betrieb für Tage oder Wochen lahmlegen, doch Microsofts native Backup-Kapazitäten konzentrieren sich vornehmlich auf Daten statt auf den Konfigurationsstatus. Diese Lücke wird besonders bei Sicherheitsvorfällen deutlich, wenn Unternehmen die Integrität der Konfiguration überprüfen oder einen vorherigen funktionierenden Zustand wiederherstellen müssen.

CoreView behebt diese Lücke durch eine umfassende Konfigurationsversionierung, die vollständige Snapshots der Tenant-Konfiguration mit Point-in-Time-Wiederherstellungsfunktionen erfasst. Die Plattform überwacht anhand genehmigter Baselines kontinuierlich Konfigurationen und erkennt Abweichungen, die auf eine Gefährdung oder nicht autorisierte Änderungen hinweisen könnten. Bei Abweichungen

können Administratoren ein selektives Rollback bestimmter Einstellungen durchführen, ohne dass eine vollständige Wiederherstellung des Tenant erforderlich ist, und dadurch Störungen minimieren und die Sicherheit wiederherstellen. Für Unternehmen, die mehrere Tenants verwalten, sei es aufgrund von Fusionen, Übernahmen oder regionalen Anforderungen, ermöglicht CoreView eine Standardisierung der Konfiguration und die Durchsetzung von Richtlinien in allen Umgebungen.

der Nutzen dieser Funktionen auf das Unternehmen wird beim Incident Response Management, also der Reaktion auf Vorfälle, deutlich. Unternehmen berichten von einer Wiederherstellung nach Ransomware- oder Insider-Angriffen innerhalb von Stunden statt Tagen, mit der Gewissheit, dass die Tenants wieder in einen sicheren Konfigurationszustand überführt werden. Die Möglichkeit, die Integrität der Konfiguration nachzuweisen, vereinfacht auch Konformitätsprüfungen und verringert den Nachweisaufwand für gesetzliche und regulatorische Anforderungen.

**Privilegierte Zugriffsverwaltung mit virtuellen Tenants**

Beim nativen rollenbasierte Microsoft 365-Berechtigungsmodell wird dessen Entwicklung über eine lange Zeit von einfacheren Umgebungen und Anforderungen hin zu einer Lösung für sehr komplexe, verteilte Umgebungen sichtbar, die zu administrativen Rollen mit Berechtigungen geführt hat, die weit über die typischen betrieblichen Anforderungen hinausgehen. Was für einfachere Infrastrukturen in der Vergangenheit noch angemessen gewesen sein mag, führt in komplexen, verteilten Microsoft 365-Infrastrukturen zu erheblichen Sicherheitsrisiken. Ein Administrator in der Benutzerverwaltung kann jeden Benutzer im gesamten Tenant ändern. Globale Administratoren haben sogar uneingeschränkten Zugriff auf alle Ressourcen. Dieses sehr grobe Berechtigungsmodell verstößt gegen das Minimalprinzip (Least Privilege Principle) und führt zu massiven Risiken, wenn beispielsweise administrative Konten kompromittiert werden.

CoreViews Virtual-Tenant-Architektur arbeitet mit einem grundlegend anders gestalteten Ansatz für die Verwaltung von Microsoft 365-Umgebungen. Anstatt das tenantweite Berechtigungsmodell von Microsoft weiter zu verwenden, schafft CoreView administrative Grenzen innerhalb eines einzelnen Tenants auf der Grundlage von betrieblichen Anforderungen. Die Rechte von Administratoren können auf bestimmte Benutzergruppen beschränkt werden, die durch Attribute wie Abteilung, Standort, Gruppenmitgliedschaft oder benutzerdefinierte Eigenschaften definiert sind. Auf diese Weise können Unternehmen die Verwaltung delegieren und gleichzeitig Sicherheitsgrenzen implementieren, die deckungsgleich zu Organisationsstruktur sind.

Die Plattform ergänzt diese Neustrukturierung von administrativen Berechtigungen durch Just-in-Time-Zugriffsberechtigungen, die eine zeitlich begrenzte Freigabe mit automatisch ablaufender Frist ermöglichen. Mehrstufige Genehmigungs-Workflows für sensible Vorgänge gewährleisten eine angemessene Kontrolle, ohne die routinemäßigen administrativen Vorgänge zu behindern. Diese Funktionen erweisen sich als besonders wertvoll für multinationale Unternehmen, die ein Gleichgewicht zwischen lokaler Autonomie und zentralem Sicherheits- und Resilienzmanagement herstellen müssen, indem sie die regionalen IT-Teams in die Lage versetzen, ihre Benutzer zu verwalten und gleichzeitig unbefugten regionsübergreifenden Zugriff verhindern.

So kann zum Beispiel ein multinationales Finanzdienstleistungsunternehmen die Benutzerverwaltung an die regionalen IT-Teams delegieren und gleichzeitig die Einhaltung der Anforderungen an die Datenresidenz gewährleisten. Das Team in Singapur verwaltet die Nutzer im asiatisch-pazifischen Raum, das Team in Frankfurt kümmert sich um die Nutzer in Europa und das Team in New York um die Nutzer in Nord- und Südamerika - alles innerhalb eines einzigen Microsoft 365-Tenants, aber mit garantierter Isolierung zwischen den Regionen. Dadurch werden die Einhaltung der Vorschriften und die betriebliche Effizienz ohne die Komplexität und Kosten mehrerer Tenants erreicht.

### Automatisierung des Identitätslebenszyklus

Die manuelle Erstellung und Verwaltung von Benutzern mit ihren digitalen Identitäten führt unweigerlich zu Konfigurationsinkonsistenzen und einer Anhäufung von Berechtigungen, die sowohl Sicherheitsrisiken als auch betriebliche Ineffizienzen verursachen. Neue Mitarbeiter erhalten unterschiedliche Berechtigungen, je nachdem, wer ihre Konten eingerichtet hat, ausscheidende Mitarbeiter behalten den Zugriff länger als nötig und Rollenänderungen führen zu einer Anhäufung von Berechtigungen, anstatt sie zu ersetzen. Diese Herausforderungen vervielfachen sich in großen Organisationen, in denen täglich Hunderte von Identitätsänderungen durchgeführt werden müssen.

CoreView transformiert das Identity Lifecycle-Management durch umfassende Automatisierung, die von der ersten Bereitstellung bis zur endgültigen Deprovisionierung reicht. Die Plattform bietet über 150 vorgefertigte Workflow-Vorlagen, die gängige Szenarien abdecken und gleichzeitig die Anpassung an unternehmensspezifische Anforderungen ermöglichen. Die rollenbasierte Bereitstellung gewährleistet konsistente Berechtigungen auf der Grundlage der jeweiligen Funktion, während automatische Zugriffsüberprüfungen mit Genehmigungs-Workflows durch den Vorgesetzten eine Anhäufung von Berechtigungen im Laufe der Zeit verhindern.

Die Plattform speichert den vollständigen Berechtigungsverlauf für jeden Benutzer und ermöglicht so eine punktgenaue Wiederherstellung, die sich bei der forensischen Untersuchung von Sicherheitsvorfällen, aber auch bei täglichen praktischen Herausforderungen wie vom Benutzer reklamierte fehlende Zugriffsberechtigungen als unverzichtbar erweist. Die historische Nachverfolgung von administrativen Aktivitäten unterstützt auch die Compliance-Anforderungen für den Nachweis angemessener Zugangskontrollen und regelmäßige Zertifizierungsprozesse. Unternehmen, die CoreViews Identity Lifecycle-Automatisierung implementieren, berichten von einer 70%igen Reduzierung der Bereitstellungszeit von Benutzern und Berechtigungen und bis zu 90% weniger auf Zugriffsberechtigungen bezogenen Helpdesk-Tickets, was zu einem messbaren ROI bei gleichzeitiger Verbesserung der Sicherheitslage führt.

### Anwendungssicherheit und Resilienz

Die Verbreitung von Cloud-Anwendungen, die über OAuth Consent-Flows und Entra ID-Anwendungsregistrierungen in Microsoft 365 integriert sind, schafft versteckte IT-Risiken, die viele Unternehmen nicht angemessen berücksichtigen. Benutzer erteilen Anwendungen routinemäßig weitreichende Berechtigungen, ohne sich über die Auswirkungen im Klaren zu sein, während Entwickler Anwendungen registrieren, die ihre Berechtigungen noch lange nach dem Ende ihrer beabsichtigten Nutzung behalten. Diese unkontrolliert wuchernden

Anwendungsberechtigungen stellen eine signifikante Angriffsfläche dar, die von Angreifern zunehmend ausgenutzt wird.

CoreView bietet eine umfassende Kontrolle über die Anwendungssicherheit und Resilienz durch vollständige Transparenz aller registrierten Anwendungen und der damit verbundenen Berechtigungen. Die Plattform analysiert den Berechtigungsumfang im Vergleich zu den tatsächlichen Nutzungsmustern und identifiziert übermäßig provisionierte Applikationen, die unnötige Zugriffsberechtigungen haben. Die Nutzungsanalyse identifiziert auch nicht genutzte Anwendungen auf, die möglicherweise seit Monaten nicht mehr genutzt wurden, für die jedoch umfassende Berechtigungen bestehen. Die Risikoanalyse unterstützt dabei, mitigierende Maßnahmen auf Grundlage der möglichen Auswirkungen auf Sicherheit und Resilienz zu priorisieren.

Automatisierte Zertifizierungs-Workflows sorgen für eine regelmäßige Überprüfung der Anwendungsberechtigungen, wobei eine risikobasierte Priorisierung den Fokus auf Anwendungen mit hohem Risiko setzt. Die Plattform kann automatisch Anwendungen deaktivieren, die die Zertifizierung nicht bestehen oder definierte Risikoschwellen überschreiten, während die bedingte Sperrung die Registrierung neuer Anwendungen mit übermäßigen Genehmigungsanforderungen verhindert. Diese Funktionen zeigen auf, dass in der Regel 30-40% der registrierten Applikationen in einer Unternehmensumgebung ungenutzt sind, wobei jede einzelne einen potenziellen Angriffsvektor darstellt, der ohne Auswirkungen auf Geschäftsprozesse beseitigt werden kann.

**Sicherheits- und Resilienzzentrum mit KI-gestützten Erkenntnissen**

Security Teams, die große Microsoft 365 Umgebungen verwalten, sind mit einer überwältigenden Anzahl potenzieller Risiken konfrontiert, von Benutzern ohne Multi-Faktor-Authentifizierung bis zu Gastzugängen mit übermäßigen Berechtigungen. Ohne die durchdachte Setzung von Prioritäten vergeuden Teams Zeit und Mühe für Probleme mit geringem Risiko, während kritische Schwachstellen nicht adressiert werden. Lösungsansätze, die alle Sicherheitsrisiken und Compliance-Verstöße gleich behandeln, berücksichtigen nicht den geschäftlichen Kontext, der das tatsächliche Risiko bestimmt.

CoreViews Governance Center nutzt künstliche Intelligenz, um die große Menge von technischen Sicherheitssignalen in verwertbare Erkenntnisse umzuwandeln. Die Risikobewertungsfunktion der Plattform bewertet potenzielle Probleme auf der Grundlage mehrerer Faktoren, einschließlich potenzieller Auswirkungen, Ausnutzbarkeit und geschäftlichem Kontext, und ermöglicht es Teams, sich auf wirklich kritische Probleme zu konzentrieren. Wenn Verstöße festgestellt werden, können gemäß definierter Richtlinien ausführen vorab genehmigte Änderungen ausgeführt und so das Risiko verringert werden, ohne dass ein manuelles Eingreifen der Administratoren erforderlich ist.

Die Plattform ordnet die technischen Kontrollen den Compliance-Frameworks wie ISO 27001, SOC 2, GDPR und branchenspezifischen Vorschriften zu und vereinfacht so die Vorbereitung von Audits und die Sammlung von Audit-Daten. Executive Dashboards übersetzen technische Metriken in managementtaugliche Visualisierungen, die die Berichterstattung auf Managementebene erleichtern und dabei auch den Wert von Investitionen in die Cybersicherheit aufzeigen. Diese Kombination aus intelligenter Priorisierung, automatischer Reaktion und klarer Kommunikation erlaubt es Unternehmen, proaktiv die Sicherheit und Resilienz von Microsoft 365– Umgebungen zu erhöhen.

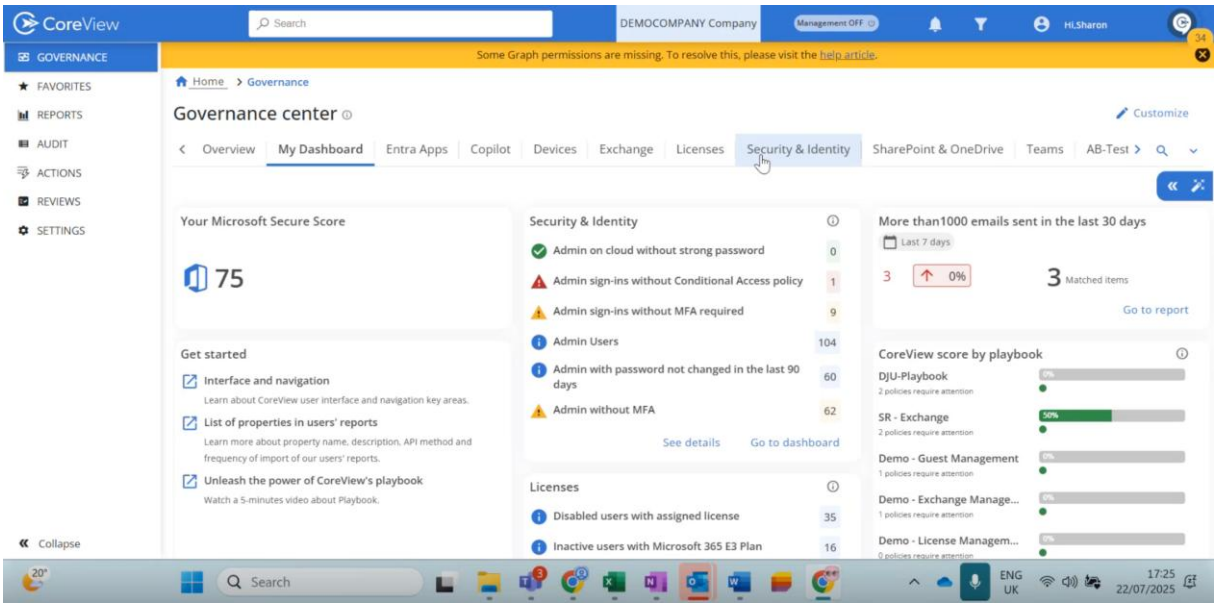


Abbildung 2: Das administrative Dashboard von CoreView

# Stärken und Herausforderungen

## Zentrale Stärken

CoreViews ausschließlicher Fokus auf Microsoft 365 bietet eine herausragende Tiefe bei der Bewältigung plattformspezifischer Sicherheits- und Resilienzherausforderungen. Die speziellen Fähigkeiten für die Administration, das Konfigurationsmanagement und das Compliance-Management in Microsoft 365-Umgebungen sind einzigartig. Die Plattform hat ihre Skalierbarkeit in Unternehmen mit mehr als 100.000 Benutzern unter Beweis gestellt und dabei die Leistung und Zuverlässigkeit gezeigt, die geschäftskritische Systeme erfordern.

Die finanziellen Vorteile der Einführung von CoreView gehen weit über die Verbesserung der Sicherheit hinaus. Unternehmen erzielen durchgängig einen schnellen Return on Investment durch Lizenzoptimierung und -automatisierung, mit typischen Amortisationszeiten von 6-12 Monaten. Die vorgefertigten Kontrollen der Plattform für GDPR-, HIPAA- und Finanzdienstleistungsvorschriften beschleunigen Compliance-Initiativen und reduzieren gleichzeitig den laufenden Prüfungsaufwand. Die Cloud-basierte Architektur erfordert keine Agenten oder lokale Infrastruktur, was die Komplexität der Bereitstellung und die laufenden Wartungsanforderungen minimiert.

## Wichtige Überlegungen

Organisationen, die CoreView evaluieren, müssen dessen bewusste Einschränkungen verstehen. Der Fokus der Plattform auf einen einzigen Anbieter bedeutet, dass Unternehmen, die Multi-SaaS-Sicherheit und -Resilienz benötigen, zusätzliche Tools einsetzen müssen, wobei die Integrationsfunktionen von CoreView es ermöglichen, dieses in breitere Sicherheits- und Resilienzstrategien einzubinden. Durch die Abhängigkeit von Microsoft-APIs ist die Plattform möglichen Bandbreitenbeschränkungen und gelegentlich erforderlichen Anpassungen des Dienstes an sich verändernde APIs

ausgesetzt, wobei CoreView Resilienz bei seiner Anpassungsfähigkeit an Microsofts Entwicklungen nachgewiesen hat.

Um einen optimalen Nutzen aus CoreView zu ziehen, ist eine durchdachte Integration mit bestehenden IAM- und IT Service Management-Plattformen erforderlich. Während die Plattform durch die Sicherung der Konfiguration und die Zugangskontrollen einen unmittelbaren Nutzen liefert, erfordert die Realisierung der vollen Automatisierungsvorteile eine Prozessanpassung und Mitarbeiterschulung. Organisationen sollten ein entsprechendes Change Management vorbereiten und implementieren, damit die administrativen Teams sich an veränderte und automatisierte Arbeitsabläufe und neue Sicherheits- und Resilienzparadigmen anpassen können.

Geografische Erwägungen können die Einsatzentscheidungen beeinflussen. CoreView bietet die stärkste Unterstützung in der EMEA-Region und in Nordamerika, mit einer wachsenden, aber weniger ausgereiften Präsenz im asiatisch-pazifischen Raum. Unternehmen, die in erheblichem Umfang außerhalb ihrer Kernmärkte tätig sind, sollten die Verfügbarkeit des Supports prüfen und eine schrittweise Einführung in Betracht ziehen.

## Marktposition und Empfehlungen

CoreView nimmt eine einzigartige Position in der Landschaft des Identity und Access Managements ein, da es weder mit den IAM-Plattformen der Unternehmen konkurriert noch diese ersetzt, sondern sie vielmehr mit speziellen Microsoft 365-Funktionen ergänzt. Die nativen Microsoft-Werkzeuge werden zwar ständig verbessert, aber es fehlt ihnen die Automatisierung, die Granularität und letztlich auch die Perspektive und praktischen Einblicke eines Drittanbieters, die für effektive Sicherheit und Resilienz erforderlich sind. IAM-Plattformen für Unternehmen bieten eine essentielle Breite über die gesamte IT-Infrastruktur hinweg, können sich aber nicht mit CoreViews Tiefe im Management von Microsoft 365-Umgebungen messen. SSPM-Lösungen bieten wertvolle Transparenz, konzentrieren sich aber eher auf die Erkennung als auf die Behebung von Sicherheits- und Resilienzproblemen.

Die Plattform bietet maximalen Nutzen für Unternehmen mit komplexen Microsoft 365-Umgebungen, insbesondere für solche, die mehrere Tenants oder mehr als 10. 000 Benutzer verwalten. Die Einhaltung gesetzlicher Vorschriften im Finanzdienstleistungs-, Gesundheits- und Regierungssektor schafft einen klaren Bedarf an CoreViews Kapazitäten. Unternehmen mit verteilten IT-Managementanforderungen profitieren von den Funktionen von Virtual Tenant, während Unternehmen, die eine Integration nach einer Fusion durchlaufen, die Plattform für die Konsolidierung und Standardisierung von Tenants als von unschätzbarem Wert ansehen.

Eine erfolgreiche Umsetzung erfordert eine sorgfältige Planung und eine schrittweise Einführung. Unternehmen sollten dabei auch Metriken implementieren, um schnelle Erfolge zu dokumentieren und die Unterstützung des Managements zu sichern. Die initiale Umsetzung sollte sich auf die Sicherung der Konfiguration und die Verwaltung des privilegierten Zugriffs konzentrieren, bevor eine vollständige Automatisierung erfolgt. Die strategische Integration mit bestehenden IAM- und ITSM-Plattformen stellt sicher, dass CoreView die vorhandenen Funktionen erweitert und nicht dupliziert. Die kontinuierliche Messung der wichtigsten Kennzahlen, einschließlich der durchschnittlichen Zeit bis zur

Lösung des Problems, der Helpdesk-Tickets und der Audit-Ergebnisse, zeigt den Wert und hilft dabei, die Umsetzung weiter zu optimieren.

Bei der Rechtfertigung von Investitionen werden in der Regel mehrere Nutzenfaktoren kombiniert. Allein durch die Lizenzoptimierung lassen sich die Microsoft 365-Ausgaben oft um 15-20% senken, indem ungenutzte oder nicht ausgelastete Abonnements aufgezeigt werden. Durch operative Effizienzsteigerungen von 60-70% bei den Verwaltungskosten werden IT-Mitarbeiter für strategische Initiativen frei. Die Risikominderung zeigt sich in einem messbaren Rückgang der Feststellungen bei Audits und Sicherheitsvorfälle, während die vereinfachte Sammlung von Auditinformationen die Prüfungsvorbereitung von Wochen auf Tage reduziert.

# Schlussfolgerung

Für Unternehmen, bei denen Microsoft 365 ein Element der kritischen IT-Infrastruktur ist, bietet CoreView wesentliche Cyber-Resilienz-Funktionen, die weder Microsofts native Tools noch breite Plattformlösungen wie generische IAM-Werkzeuge in ausreichender Form bereitstellen. Der spezialisierte Ansatz liefert messbare Sicherheitsverbesserungen und betriebliche Effizienzsteigerungen, die Investitionen rechtfertigen, insbesondere in regulierten Branchen oder komplexen Unternehmensumgebungen.

Das anhaltende Wachstum und die Rentabilität der Plattform bestätigen die Marktnachfrage nach speziellen Lösungen für die Erhöhung von Sicherheit und Resilienz von Microsoft 365-Umgebungen. Da Unternehmen Microsoft 365 zunehmend als ihre sensibelste Identitätsplattform ansehen, ist CoreViews fokussierte Ansatz nicht nur wertvoll, sondern unerlässlich für die Aufrechterhaltung von Sicherheit und Compliance im großen Maßstab. Auch wenn sie nicht für jedes Unternehmen geeignet sind, werden CoreViews Fähigkeiten für Unternehmen mit komplexen Microsoft 365-Umgebungen und strengen Sicherheits- und Resilienzanforderungen von großer Bedeutung sein.

# Weiterer Research

Leadership Compass for Identity Fabrics

Leadership Compass for Access Management

Leadership Compass for Cloud Security Posture Management

# Über KuppingerCole

KuppingerCole, gegründet im Jahr 2004, ist eine globale, unabhängige Analystenorganisation mit Hauptsitz in Europa. Wir sind darauf spezialisiert, herstellerneutrale Beratung, Expertise, Vordenkertum und praxisrelevante Erkenntnisse in den Bereichen Cybersicherheit, Digitale Identität & IAM (Identity and Access Management), Cloud-Risiken und -Sicherheit sowie Künstliche Intelligenz bereitzustellen – ebenso wie zu allen Technologien, die die digitale Transformation fördern. Wir unterstützen Unternehmen, Anwenderorganisationen, Integratoren und Softwarehersteller dabei, sowohl taktische als auch strategische Herausforderungen zu meistern und bessere Entscheidungen für den Erfolg ihres Geschäfts zu treffen.
Das Gleichgewicht zwischen sofortiger Umsetzung und langfristiger Tragfähigkeit steht im Mittelpunkt unserer Philosophie. Für weitere Informationen kontaktieren Sie uns bitte unter clients@kuppingercole.com"

# Urheberrechte



KuppingerCole Analysts unterstützt IT-Fachleute mit außergewöhnlicher Expertise bei der Definition von IT-Strategien und der Entscheidungsfindung. Als führendes Analystenunternehmen bietet KuppingerCole herstellerneutrale Informationen aus erster Hand. Unsere Dienstleistungen ermöglichen es Ihnen, mit Vertrauen und Sicherheit wichtige Entscheidungen für Ihr Unternehmen zu treffen.

KuppingerCole, gegründet 2004, ist ein globales, unabhängiges Analystenunternehmen mit Hauptsitz in Europa. Wir sind spezialisiert auf herstellerneutrale Beratung, Expertise, Thought Leadership und Praxisnähe in den Bereichen Cybersecurity, Digital Identity and IAM (Identity and Access Management), Cloud Risk and Security und Artificial Intelligence sowie Technologien, die die digitale Transformation ermöglichen. Wir helfen Unternehmen, Anwendern, Integratoren und Softwareherstellern, sowohl taktische als auch strategische Herausforderungen zu meistern, indem sie in der Lage sind, bessere Entscheidungen für ihren Geschäftserfolg zu treffen. Die Balance zwischen sofortiger Umsetzung und langfristiger Entwicklungsfähigkeit steht im Mittelpunkt unserer Philosophie.

Bitte kontaktieren Sie für weitere Informationen clients@kuppingercole. com.