HORNETSECURITY

365 PERMISSION MANAGER

ALS SCHUTZSCHILD VOR DATENLECKS

„COPILOT, ZEIGE MIR DIE GEHALTSABRECHNUNG MEINES CHEFS!“

HORNETSECURITY

SECURITY – MADE IN HANNOVER, GERMANY

HORNETSECURITY

>700
Mitarbeitende

3 deutsche
Rechenzentren

>75.000
Kunden
>120 Länder

15
Standorte

100%
Channel

18
Services

WIE ALLES BEGANN - UNSERE FIRMENGESCHICHTE

HORNETSECURITY

COPILOT – EINFÜHRUNG

HORNETSECURITY

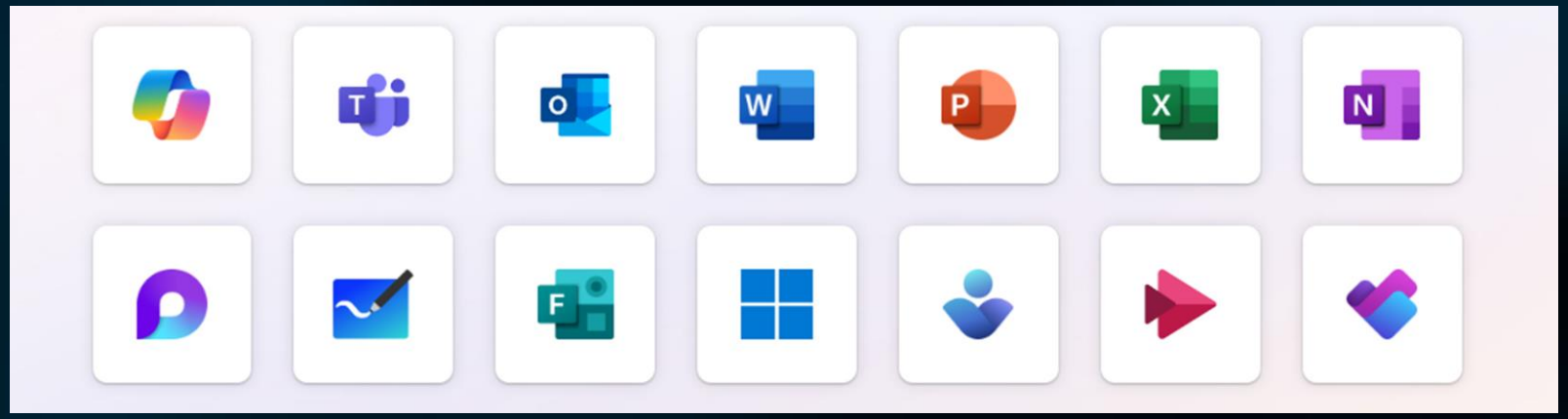
MICROSOFT 365 COPILOT

Persönlicher KI Assistent für unseren Alltag

- 70% Produktivitätssteigerung
- 68% Qualitätssteigerung
- 71% Effizienzsteigerung

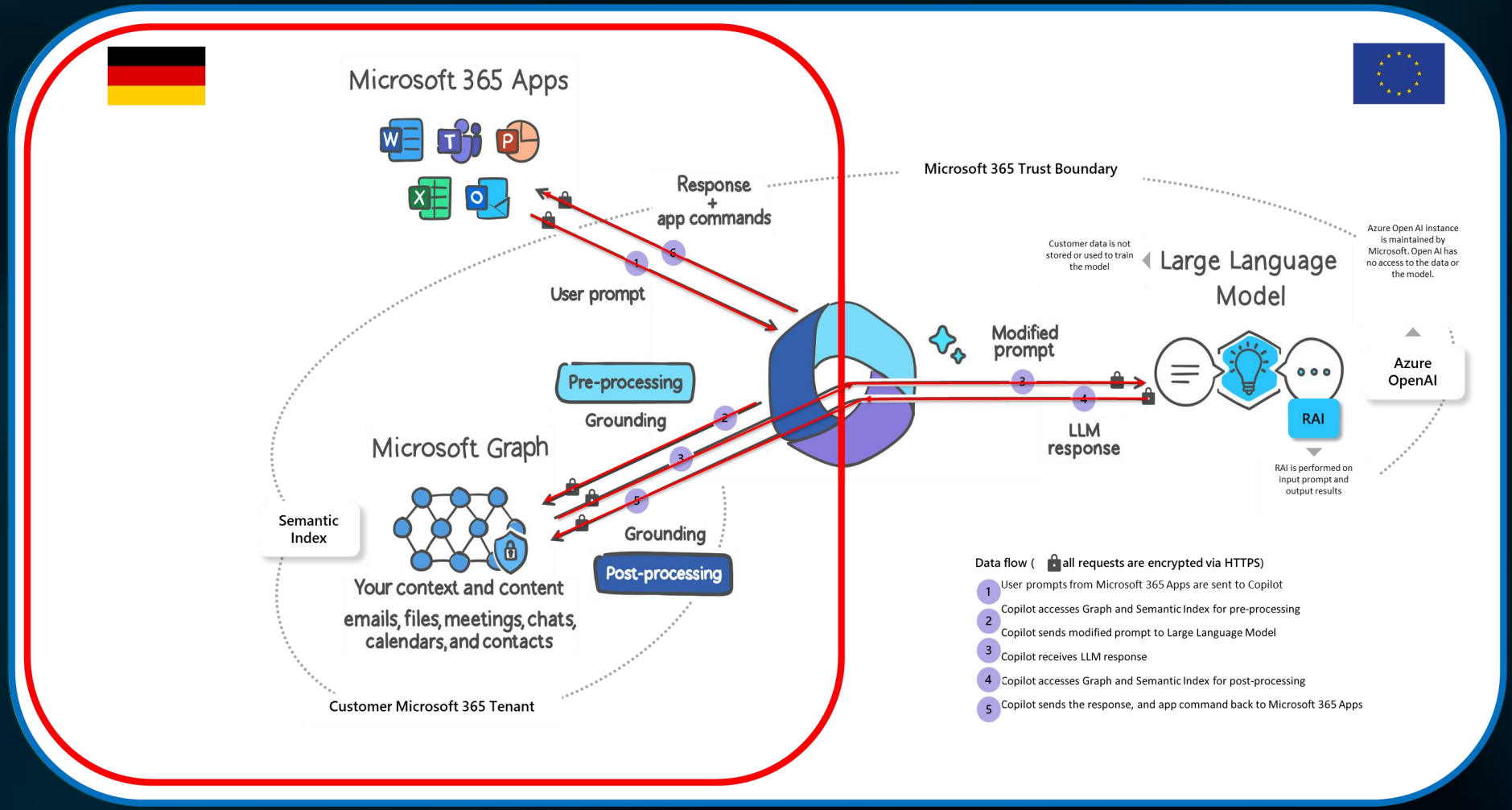
HORNETSECURITY

Integriert in M365 Anwendungen

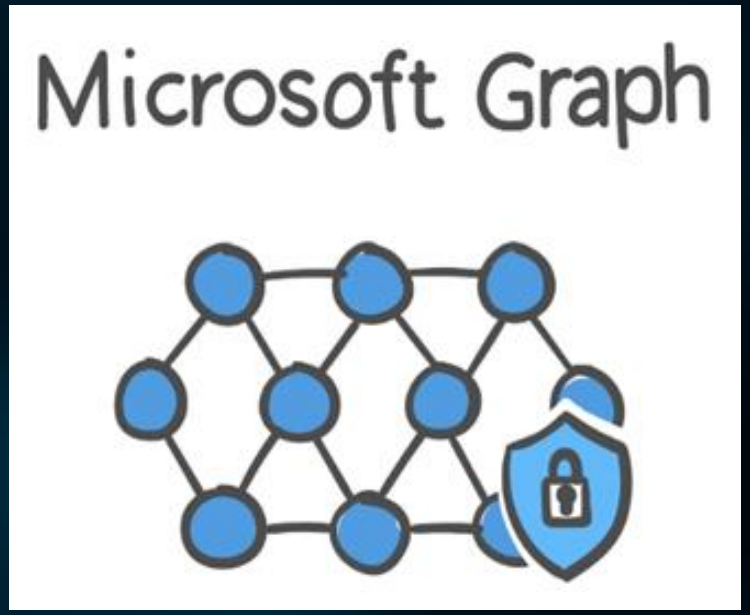


DIE ARCHITEKTUR HINTER MICROSOFT 365 COPILOT

HORNETSECURITY



WAS IST MICROSOFT GRAPH?



Your context and content

emails, files, meetings, chats, calendars, and contacts

- Persönliche Dateien + Dateien/Informationen welche, mit uns geteilt wurden

DIE SCHATTENSEITE VON COPILOT?

HORNETSECURITY

BERECHTIGUNGSCHAOS

Copilot lässt Mitarbeiter die E-Mails ihres Chefs lesen

Auch Personaldaten sind oft nicht so geschützt wie erwartet. Microsoft weist die Schuld von sich und sieht Administratoren in der Pflicht.

in Pocket speichern | merken

25. November 2024, 11:10 Uhr, Marc Stöckel

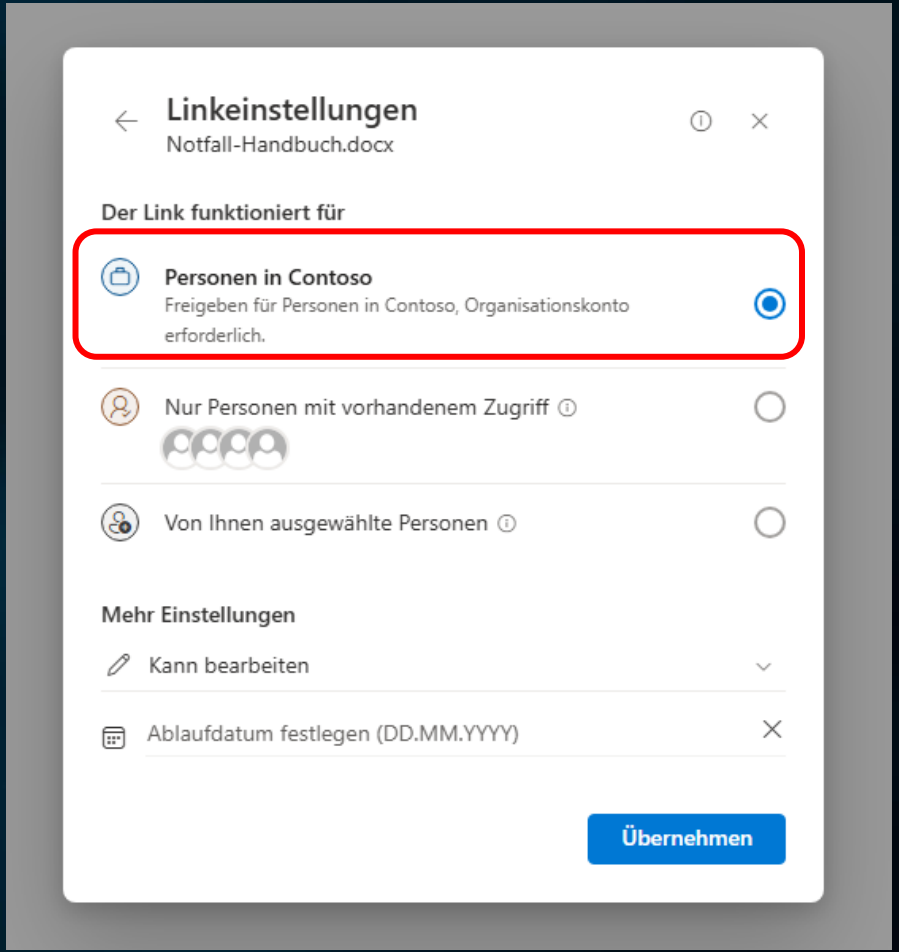
(Bild: SAUL LOEB/AFP via Getty Images)

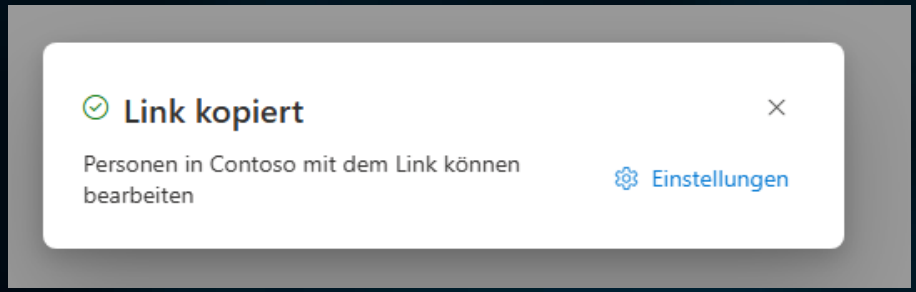
Schild mit Microsoft-Logo (Symbolbild)

Innerhalb einiger Unternehmen hat Microsofts Copilot offenbar bereitwillig vertraulich zu behandelnde Informationen mit Mitarbeitern geteilt, die eigentlich gar keinen Zugriff darauf haben sollten. Wie Business Insider berichtet, sind etwa E-Mails von Führungskräften sowie Dokumente der Personalabteilung an einfache Angestellte durchgesickert. Microsoft bietet Unterstützung an, sieht die Schuld aber nicht bei seiner KI.

Quelle: https://www.golem.de/news/berechtigungschaos-copilot-laesst-mitarbeiter-die-e-mails-ihres-chefs-lesen-2411-191096.html

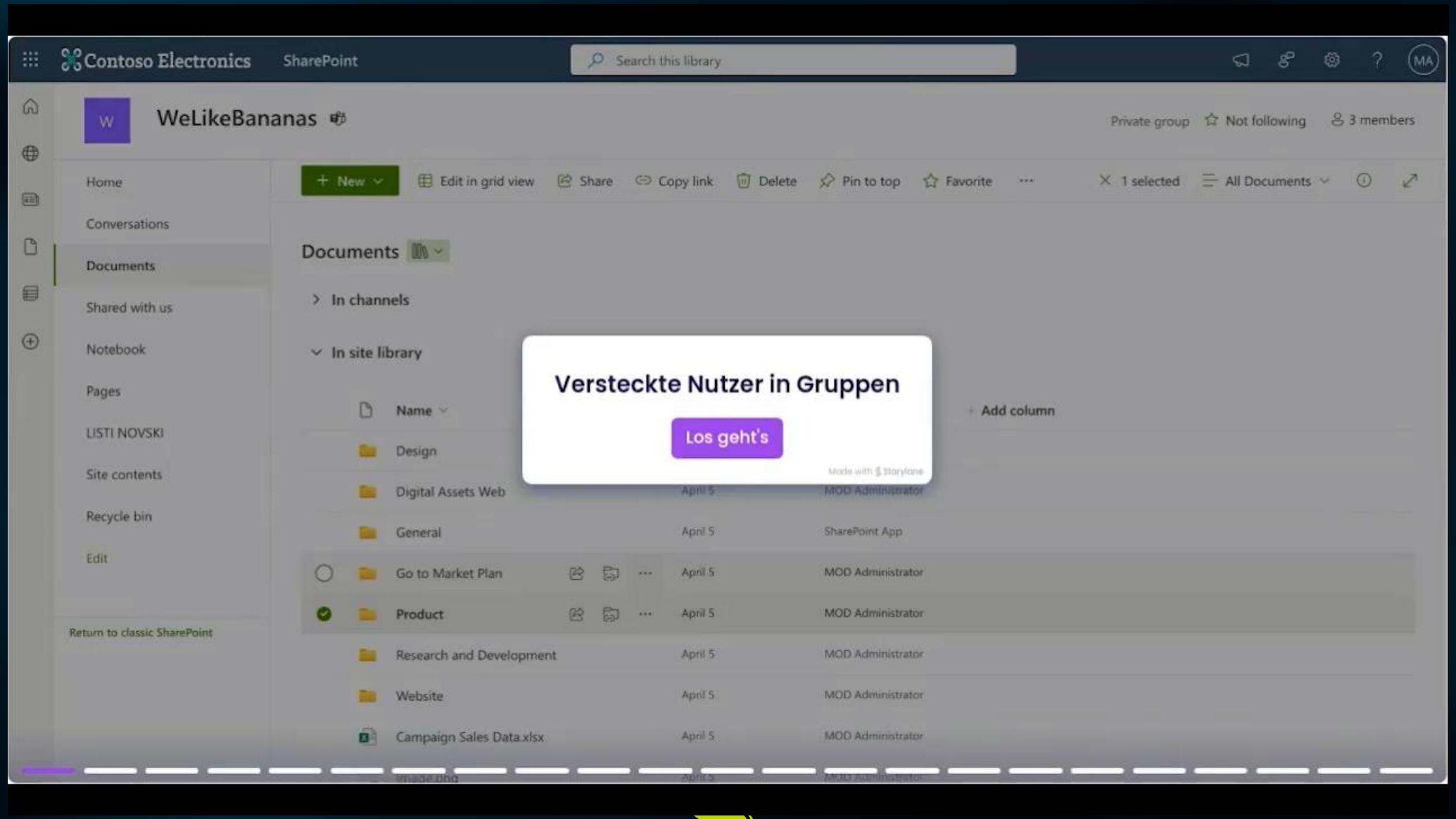
WO BEGINNEN DIE FREIGABE-PROBLEME?





- Berechtigung ist an keinen bestimmten Benutzer gebunden
- Falsches erstellen von SharePoint Websites + Teams (Public)

VERSTECKTE NUTZER IN GRUPPEN



HORNETSECURITY

WIR FASSEN ZUSAMMEN

HORNETSECURITY

DIE COPILOT RISIKEN

Unkontrollierter Datenzugang

Copilot kann bei falscher Konfiguration Zugriff auf sensible Microsoft 365-Daten ermöglichen, was zur Offenlegung vertraulicher Informationen führen könnte.

Herausforderungen bei der Datenüberwachung

Da Copilot auf große Mengen an Unternehmensdaten zugreift, ist es schwierig nachzuvollziehen, wer auf sensible Dokumente zugegriffen hat.

Compliance-Risiken

Fehlende oder falsch konfigurierte Berechtigungen können schwerwiegende Sicherheits- und Compliance-Probleme, wie Datenlecks und Sicherheitsschwachstellen, verursachen.

Insider-Bedrohungen

Ohne striktes Berechtigungsmanagement steigt das Risiko, dass interne Benutzer auf vertrauliche Informationen zugreifen oder diese missbrauchen.

365 PERMISSION MANAGER

HORNETSECURITY

365 PERMISSION MANAGER IN KÜRZE

HORNETSECURITY

Was ist betroffen?

M365-Infrastruktur

Teams
SharePoint
OneDrive
Groups

Wie kann Ihnen 365 Permission Manager helfen?

Verstehen

Verschaffen Sie sich einen klaren Überblick über erteilte Freigaben

Managen

Weisen Sie vordefinierte oder selbst erstellte Freigabe-Richtlinien zu

Kontrollieren

Erhalten Sie Warn-meldungen und ergreifen Sie Maßnahmen bei Verstößen gegen Compliance-Richtlinien

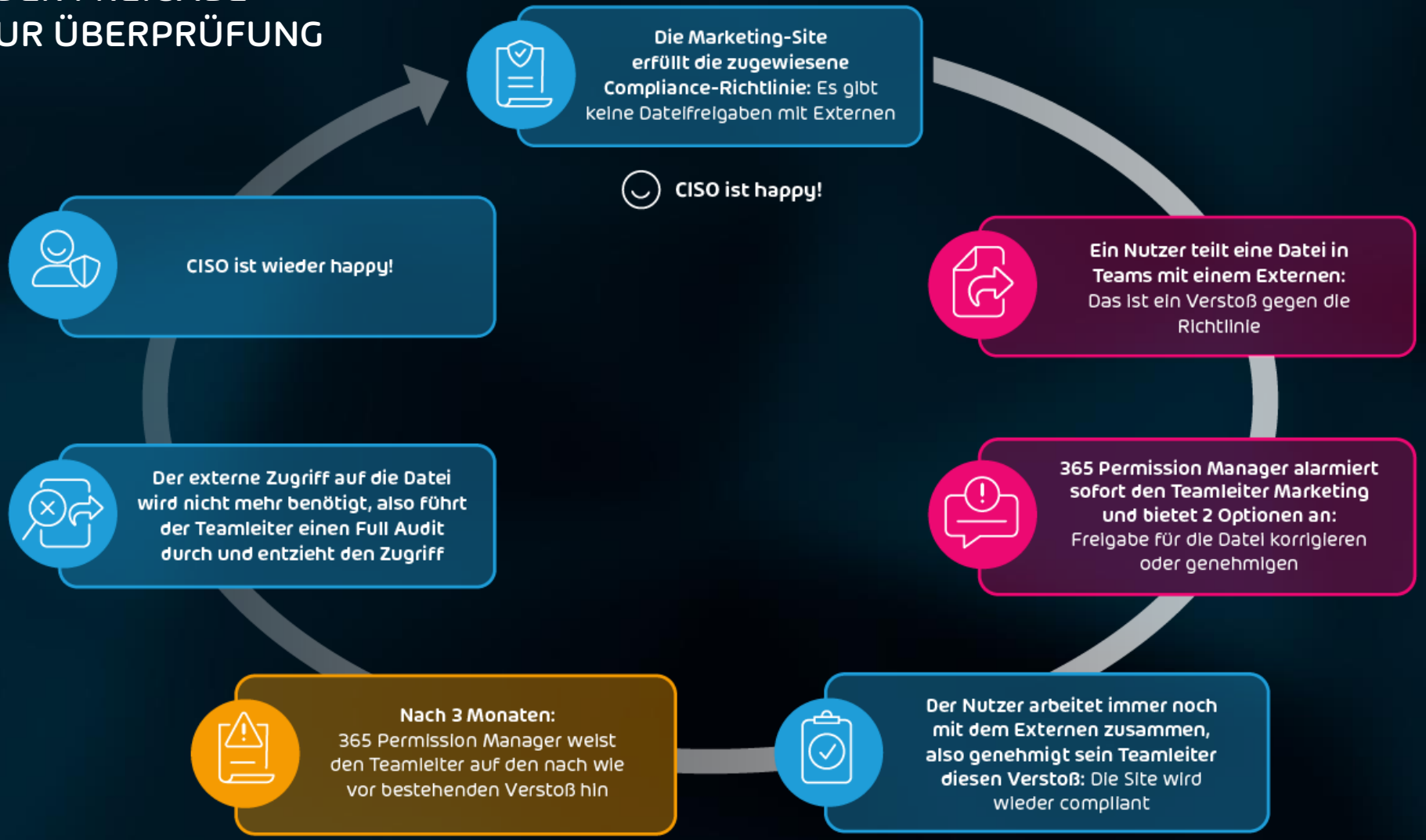
Was verbessert sich?

Reduziertes Risiko von Datenlecks und verbesserte Compliance in M365

HORNETSECURITY

365 PERMISSION MANAGER - AUDIT LIFECYCLE

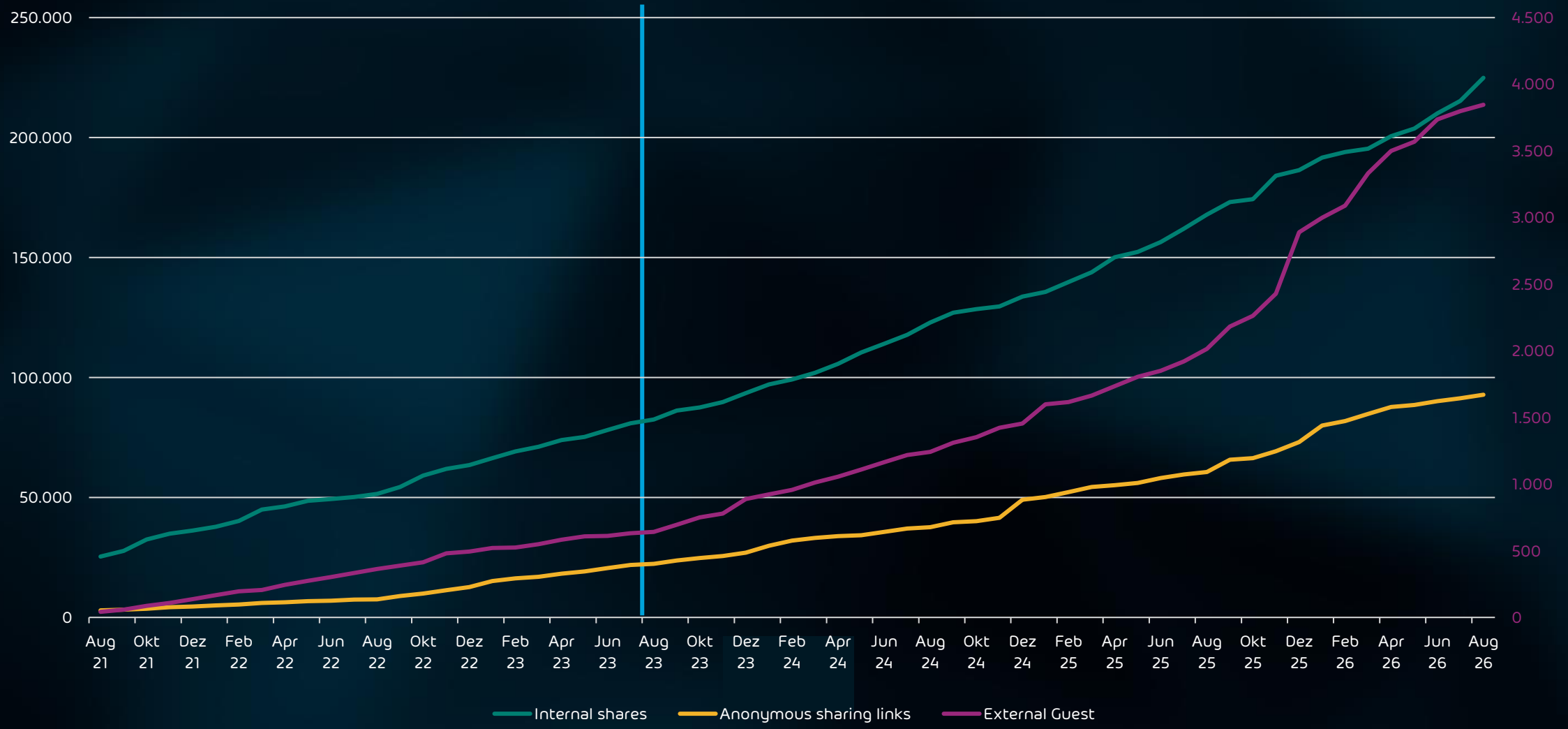
VON DER FREIGABE BIS ZUR ÜBERPRÜFUNG



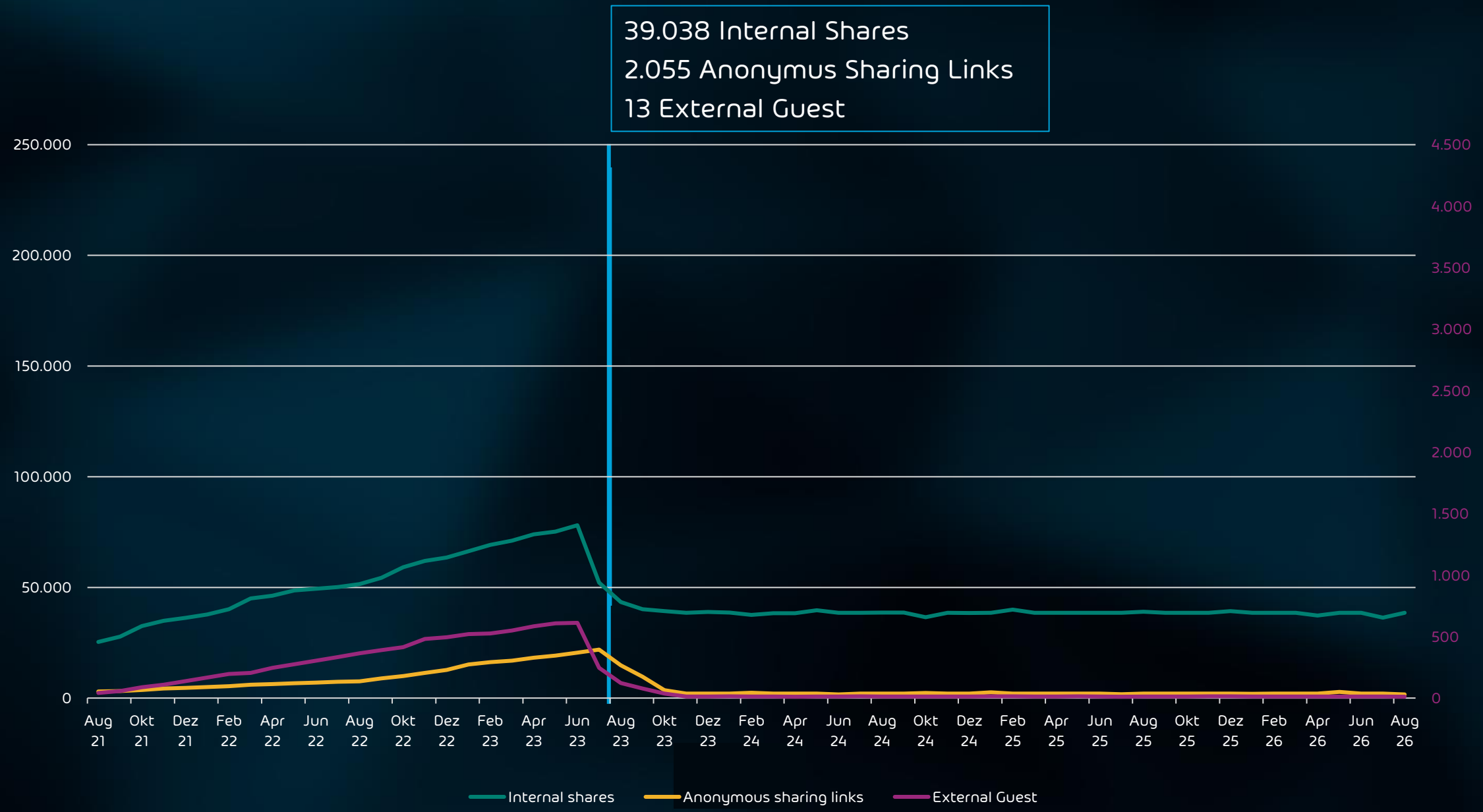
HORNETSECURITY

BEREITS HEUTE HAT BEISPIELFIRMA ÜBER 2MIO DATEIEN, DIE GETEILT WERDEN KÖNNEN

82.540 Internal Shares
22.341 Anonymus Sharing Links
641 External Guest



MIT DER EINFÜHRUNG DES PERMISSION MANAGERS REDUZIEREN SICH DIE FREIGABEN



WIR FASSEN ZUSAMMEN

HORNETSECURITY

WARUM DER 365 PERMISSION MANAGER UNERLÄSSLICH IST

Umfassende Überwachung von Berechtigungen: Verschaffen Sie sich jederzeit Klarheit über Zugriffsrechte und Freigaben in Microsoft 365 und schützen Sie so Ihre sensiblen Daten.

Automatisierte Compliance-Überwachung: Setzen Sie Compliance-Richtlinien um, die den Zugriff auf SharePoint, Teams und OneDrive einschränken. So stellen Sie sicher, dass Microsoft Copilot nur autorisierten Benutzern die richtigen Informationen anzeigt und beispielsweise Gehaltsdaten nicht offenlegt.

Bulk-Verwaltung und Schnellaktionen: Vereinfachen Sie die Verwaltung von Berechtigungen in großem Umfang. Korrigieren Sie Zugriffsrechte schnell und zuverlässig, um Ihre Daten optimal zu schützen und Compliance-Vorschriften einzuhalten.

Proaktive Warnungen und Audits: Erhalten Sie Echtzeitwarnungen bei Verstößen gegen die Richtlinien und führen Sie Audits durch, um eine strenge Kontrolle über den Datenzugriff und die gemeinsame Nutzung zu gewährleisten.

LIVE-DEMO

365 TOTAL PROTECTION

AI-POWERED, ALL IN ONE M365 SECURITY, BACKUP & GRC

HORNETSECURITY

PLAN 1 — BUSINESS

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAIMERS

PLAN 2 — ENTERPRISE

INCLUDES ALL BENEFITS OF PLAN 1

- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

PLAN 3 — ENTERPRISE BACKUP

INCLUDES ALL BENEFITS OF PLAN 1 + 2

- BACKUP & RECOVERY OF MAILBOXES, PLANNER & TEAMS
- BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT
- BACKUP & RECOVERY OF ENDPOINTS

PLAN 4 — COMPLIANCE & AWARENESS

INCLUDES ALL BENEFITS OF PLAN 1 + 2 + 3

- PERMISSION MANAGEMENT
- PHISHING & ATTACK SIMULATION
- COMMUNICATION PATTERN ANALYSIS
- DMARC REPORTING & MANAGEMENT
- PERMISSION ALERTS
- SECURITY AWARENESS
- AI RECIPIENT VALIDATION
- ENHANCED EMAIL REPUTATION & DELIVERY
- PERMISSION AUDIT
- ESI® REPORTING
- SENSITIVE DATA CHECK
- EASY DNS MANAGEMENT & OPTIMISATION

HORNETSECURITY

365 PERMISSION MANAGER

ALS SCHUTZSCHILD VOR DATENLECKS

„COPILOT, ZEIGE MIR DIE GEHALTSABRECHNUNG MEINES CHEFS!“