VARONIS

MICROSOFT 365 COPILOT SECURITY-SCAN

SORGEN SIE FÜR DIE SICHERHEIT VON COPILOT VOR, WÄHREND, UND NACH DER IMPLEMENTIERUNG

VARONIS + Microsoft

Nasdaq Market Activity News + Insights Solutions About Nasdaq+

Varonis Accelerates Secure Adoption of Microsoft Copilot for Microsoft 365

PUBLISHED
JAN 23, 2024 9:00AM EST

Integration lays the foundation for secure and compliant deployment of Microsoft Copilot for Microsoft 365

NEW YORK, Jan. 23, 2024 (GLOBE NEWSWIRE) -- Varonis Systems, Inc. (Nasdaq: VRNS), a leader in data security, today announced a strategic collaboration with Microsoft to help companies safely harness the power of AI. The integration helps joint customers continually assess and improve their Microsoft 365 data security posture before, during, and after they deploy Microsoft Copilot for Microsoft 365.

„Die Integration mit Varonis bietet Kunden die zusätzlichen Sicherheits- und Compliance-Kontrollen, die für eine schnelle und sichere Einführung von Microsoft Copilot für Microsoft 365 erforderlich sind."

ANAT GIL

Partner Lead,
Microsoft Europe

BEREIT FÜR COPILOT IN 10 TAGEN

Varonis reduzierte das Copilot-Exposure eines Finanzinstituts innerhalb von 10 Tagen um 99,8 %.
Keine Auswirkung auf das Geschäft durch 20 Automatisierungsrichtlinien zum Sperren von ~1 Million Dateien.

992.000 Dateien

Ausgangspunkt

~1 Mio. Dateien in SharePoint, Teams und OneDrive der Organisation. Varonis hat 120.000 vertrauliche Dateien schnell klassifiziert.

57.000 offengelegte Dateien

Copilot-Risiko erkennen

Verwenden Sie Varonis, um PHI und PII sowie Zugangsdaten zu identifizieren, die über Copilot gefährdet sind.

99,8 % Expositionsreduzierung

10 Tage Unterschied

Mit Varonis-Richtlinien wurden automatisch ca. 2.000 Freigabelinks eliminiert und der Zugriff auf 57.000 Dateien richtig dimensioniert.

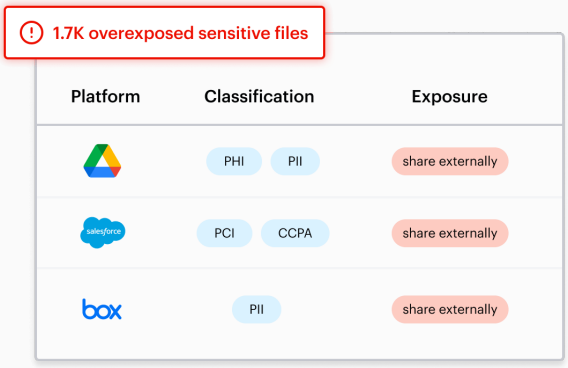
0 Ticketbeschwerden

Keine Auswirkungen auf die Kunden

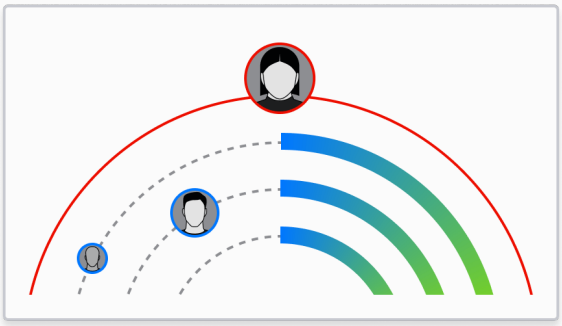
M365-Administratoren wurden proaktiv über den Sanierungsplan benachrichtigt. Das Team hat keine Beschwerden erhalten.

MICROSOFT 365 COPILOT-SECURITY-SCAN

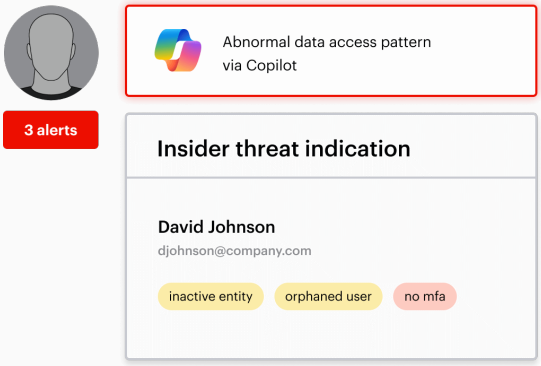
Klassifizieren und kennzeichnen Sie Daten, die Copilot erstellt.



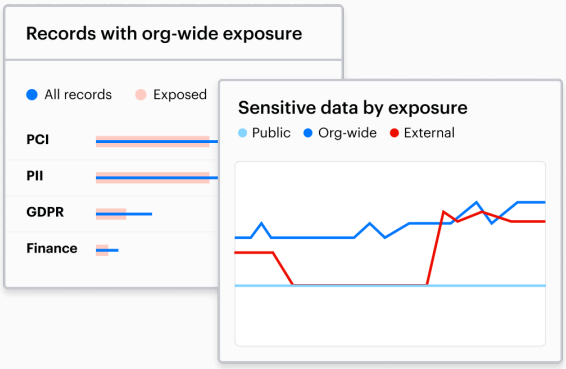
Reduzieren Sie den potenzielle Schaden von Copilot.



Überwachen Sie Copilot-Aktivitäten in Echtzeit.

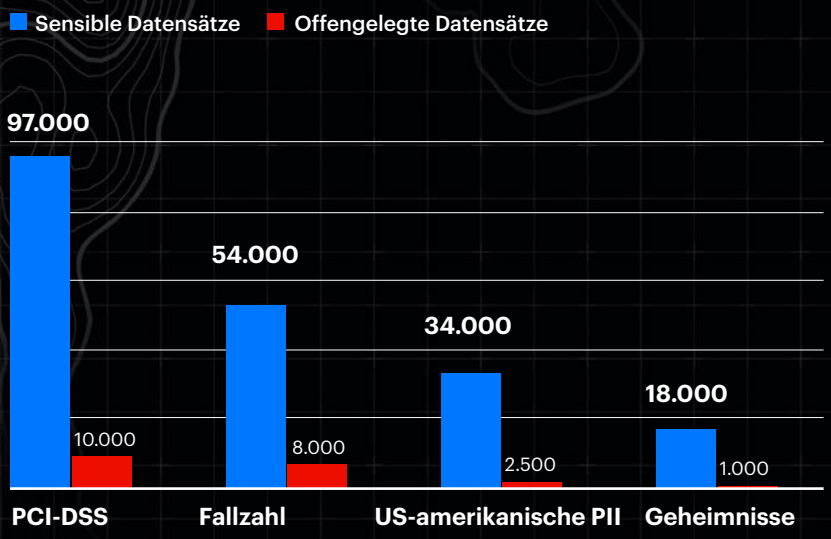


Aktivieren Sie nachgelagerte DLP-Kontrollen.



WELCHE SENSITIVEN DATEN WERDEN COPILOT ZUGÄNGLICH GEMACHT?

Die Dashboards von Copilot helfen Ihnen bei der Entscheidung, ob die Bereitstellung sicher ist.

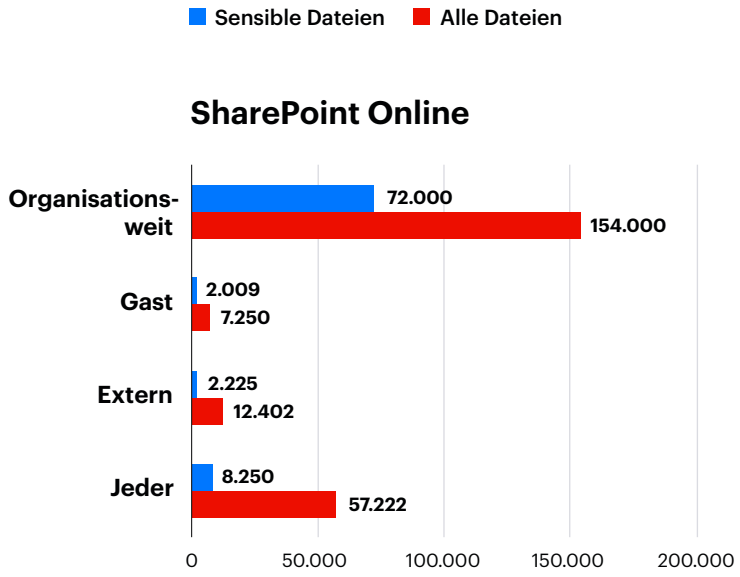


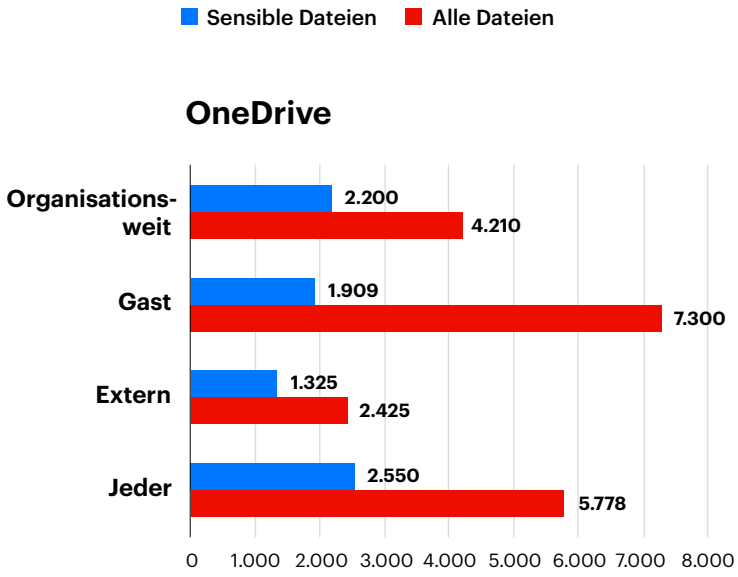
203.000 Sensible Datensätze

1,5K sensible Aufzeichnungen werden extern offengelegt

20K Sensible Datensätze werden unternehmensweit offengelegt

Copilot-Daten-Exposure nach Ebene

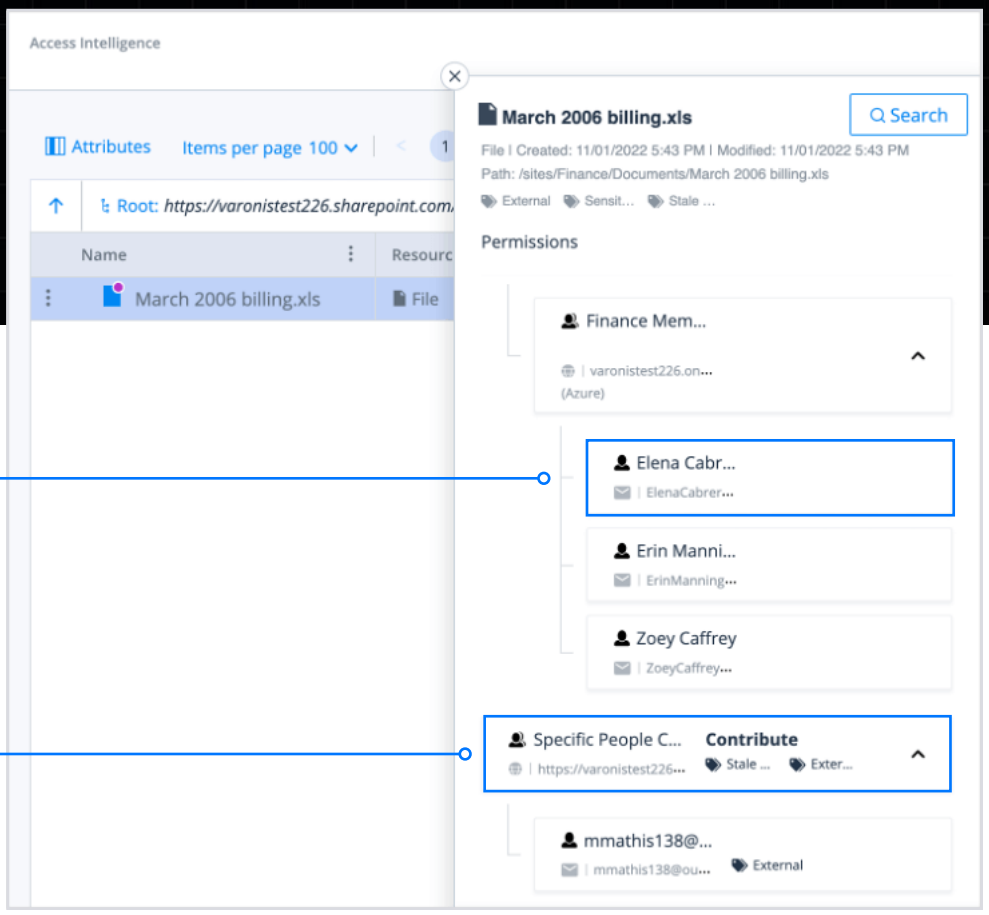




WIE ERHÄLT COPILOT ZUGRIFF AUF SENSITIVE DATEN?

Varonis zeigt Ihnen genau, wie Copilot beliebig auf sensitive Daten zugreifen kann, damit Sie Probleme vor der Bereitstellung beheben können.

+ Direkte Berechtigungen
+ Gruppenmitgliedschaften (Teams, Azure, SharePoint, etc.)
+ Gastberechtigungen
+ „Anyone"-Links
+ Organisationsweite Links
+ Links für spezifische Benutzer



Elena ist nicht im Finanzteam, ist aber der Gruppe über Teams beigetreten.

Sie sollte keinen Zugriff auf Rechnungsdaten haben.

Elena hat diese Datei mit einem privaten E-Mail-Konto geteilt.

Welche sensitiven Dateien sind falsch gekennzeichnet?

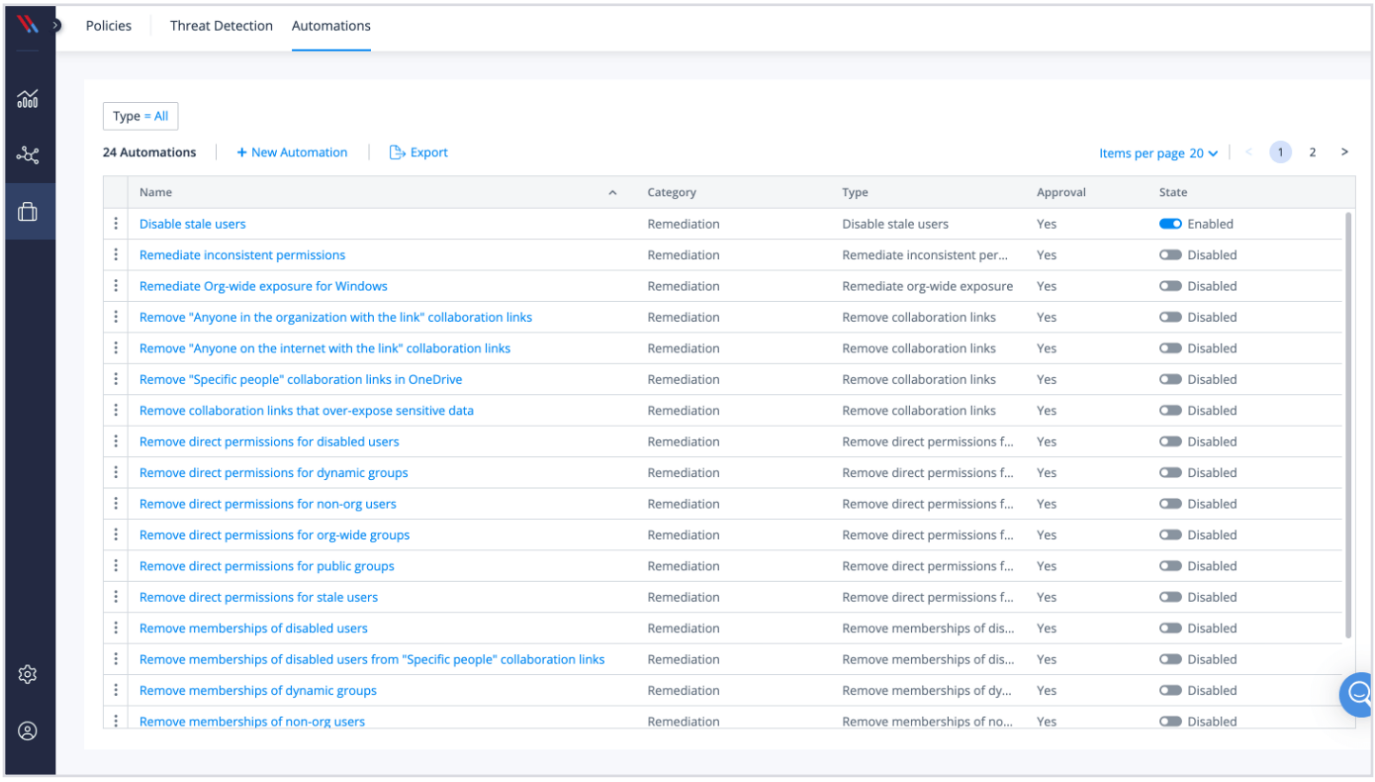
Die Sicherheit von Copilot ist in hohem Maße auf genaue MPIP-Labels angewiesen.
Varonis findet und korrigiert MPIP-Labels.

Wir haben mehr als 27.000 vertrauliche Dateien gefunden, denen kein Label zugewiesen wurde. Copilot betrachtet diese Dateien nicht als sensitiv.

Drag here to set row groups

Path	Classification Results	Classification Labels	Name
C:\Share\Finance	US PII (0/43),HIPAA PHI Data - 2.0 US (0/...	GDPR Regulated Data (0/1)	Finance
C:\Share\Finance\Controllers	US PII (0/29),HIPAA PHI Data - 2.0 US (0/...		Controllers
C:\Share\Finance\Controllers\Finance repor...	US PII (2/7),HIPAA PHI Data - 2.0 US (12/...		Q1 2006
C:\Share\Finance\Controllers\Finance repor...	US PII (2/2),HIPAA PHI Data - 2.0 US (10/...		Inventory
C:\Share\Finance\Controllers\Finance repor...	US PII (3/3),HIPAA PHI Data - 2.0 US (15/...		Revenues
C:\Share\Finance\Controllers\Finance repor...	US PII (20/20),HIPAA PHI Data - 2.0 US (8...		SEC
C:\Share\Finance\data	Passwords (1/2),GDPR Greece (1/1),UK D...	GDPR Regulated Data (1/1)	data
C:\Share\Finance\DEMO94	Passwords (3/3),PCI Data Security Stand...		DEMO94
C:\Share\Finance\data\KolNet	Passwords (1/1),UK Data Protection Act ...		KolNet
C:\Share\Finance\Economics\Costing	[Preview] Document Passwords - 2.0 (6/...		Costing
C:\Share\Finance\Economics\Budget\2006\...	[Preview] Document Passwords - 2.0 (2/...		Final

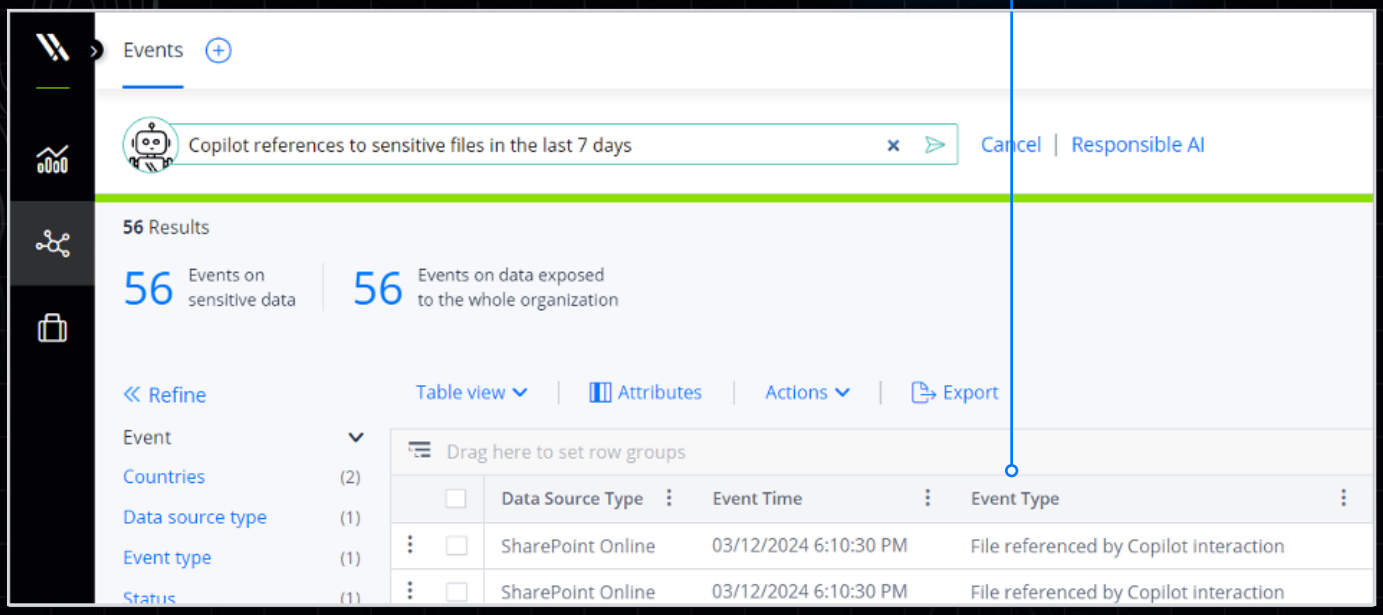
Aktivieren Sie Copilot-Automatisierungsrichtlinien, um M365 innerhalb weniger Tage schnell einsatzbereit zu machen.



WER HAT ÜBER COPILOT-EINGABEAUFFORDERUNGEN ZUGRIFF AUF SENSITIVE DATEN?

Verwenden Sie die KI Athena, um Fragen zu stellen wie: „Welche Benutzer haben heute über Copilot auf sensitive Daten zugegriffen?“

Ein Marketingmitarbeiter gewinnt Finanzdaten über Copilot-Interaktionen.



Wer missbraucht Copilot?

- Unangemessene oder riskante Interaktionen erkennen
- Weitergabe vertraulicher Informationen erkennen
- Abgerufenen Dateien und die entsprechenden Labels verfolgen
- Labels als Reaktion auf Alerts anwenden

3 alerts

Abnormal data access pattern via Copilot

Insider threat indication

David Johnson
djohnson@company.com

inactive entity | orphaned user | no mfa

COPILOT-FLUGPLAN: **SCHRITT FÜR SCHRITT**

Vor Copilot

- Bereitstellung von Varonis
- Die ersten Scans durchführen
- Sensibilitätsbezeichnungen hinzufügen und korrigieren
- Hochrisiko-Exposure beseitigen
- Zugriff auf kritische Daten überprüfen
- Downstream-DLP mit Purview aktivieren

Nach Copilot

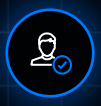
- Überwachung der gesamten Copilot-Nutzung und Warnungen bei verdächtigem Verhalten und dem Zugriff auf vertrauliche Daten
- Automatisieren der Zugriffskontrollrichtlinien
- Automatisieren der DLP und Datenlebenszyklusrichtlinien

VERRINGERN SIE IHR RISIKO, OHNE NEUE RISIKEN EINZUGEHEN.

Die Einrichtung unserer kostenlosen Risikobewertung dauert nur wenige Minuten und bietet sofortigen Mehrwert. In weniger als 24 Stunden haben Sie einen risikobasierten Überblick über die Daten, die am wichtigsten sind, und einen klaren Weg zur automatisierten Problembehebung.

Vollständiger Zugriff auf die Varonis SaaS-Plattform

Erhalten Sie für die Dauer Ihrer Bewertung vollen Zugriff auf unsere Datensicherheitsplattform und erhalten Sie umsetzbare Erkenntnisse für Ihre wichtigsten Daten.



Dedizierter IR-Analyst

Mit der Varonis SaaS Data Security Platform verbunden zu sein bedeutet, dass unsere Experten Ihre Alerts im Auge haben und wir Sie anrufen, wenn wir etwas Alarmierendes sehen.

Bericht zu den wichtigsten Ergebnissen

Eine detaillierte Zusammenfassung Ihrer Datensicherheitsrisiken und eine Präsentation der Ergebnisse und Empfehlungen. Sie können diesen Bericht behalten, auch wenn Sie kein Kunde werden.

Holen Sie sich noch heute Ihre kostenlose Risikenbewertung bei **Varonis.com.**

Tausende von Kunden vertrauen uns

ING · U.S. AIR FORCE · NASA · BlueCross BlueShield · Nasdaq · Coca-Cola · TOYOTA · U.S.ARMY · Penguin Random House · E*TRADE