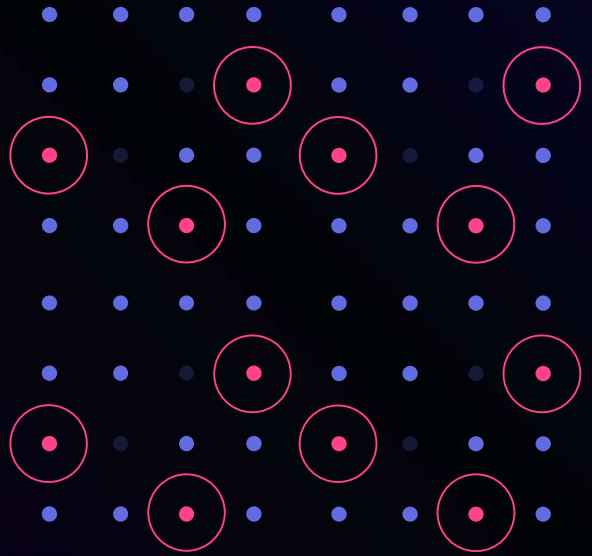
VARONIS

Das Erkennen einer Insider-Bedrohung

ITSA 2022

Agenda

- Erkenntnisse aus dem Varonis Risikobericht zu SaaS-Daten
- Echtzeitbeispiele unseres IR-Teams darüber, wie SaaS-Sicherheitslücken ausgenutzt werden
- CASB-, SSPM- und SASE-Technologien verstehen
- Demo von DatAdvantage Cloud



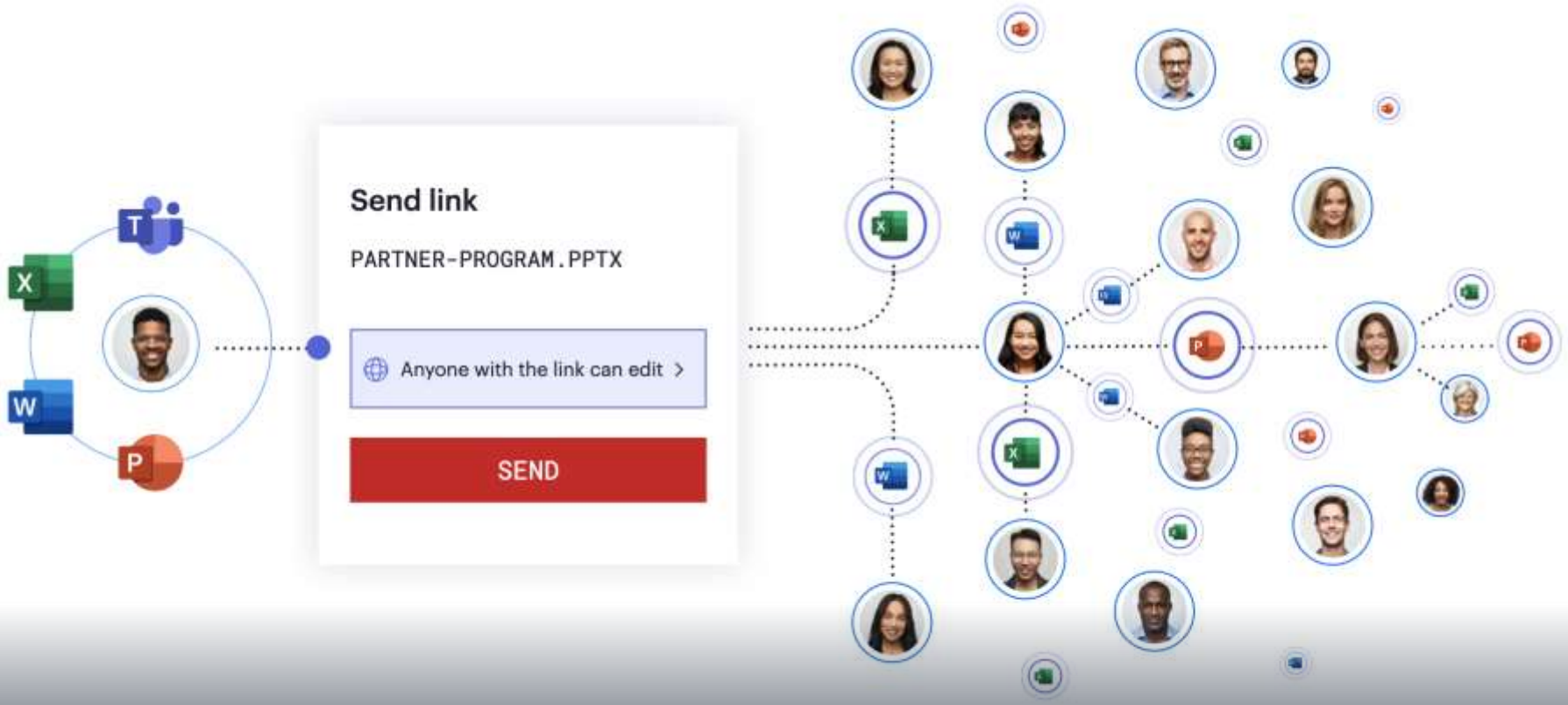
VARONIS

Wie viele, einzigartige Berechtigungen gibt es in der Cloud einer durchschnittlichen Organisation?

VARONIS

40 Millionen

VARONIS



Riskant! Woher kommt dieses Risiko?

4.468 Benutzerkonten ohne MFA

33 Super-Admin-Konten

150.648 gefährdete sensible Datensätze

Können Sie diese Fragen beantworten?

Wo sind Ihre sensiblen Daten?

Wer kann auf Ihre sensiblen Daten zugreifen?

Was machen sie damit?

Wie Angreifer Cloud-Apps ausnutzen

VARONIS

Bedrohungsakteure greifen SaaS an (und Varonis Threat Labs tut dasselbe).

THREAT RESEARCH | JANUARY 18, 2022

Mixed Messages: Busting Box's MFA Methods

By Tal Peleg

THREAT RESEARCH | FEBRUARY 2, 2022

Using Power Automate for Covert Data Exfiltration in Microsoft 365

By Eric Saraga

VARONIS

Wie Cloud-Apps kompromittiert werden können

Smash-and-Grab-Ransomware

- Der häufigste Ransomware-Angriff, den wir in der “freien Wildbahn” beobachten

MFA-Bypass per Man-in-the-Middle

- Umgehen von Microsoft-365-MFA mit Evilginx

Insider-Überfall

- Unternehmensgeheimnisse per Kerberoasting aus einem SVC-Konto stehlen

SSO-Betrüger

- Kompromittieren eines Single-Sign-on-Anbieters und Missbrauch von SaaS-Identitäten

Kompromittierung in der Cloud

- Stehlen von Salesforce-Daten über GitHub und Slack

Cookie-Diebstahl

- Verwenden eines Reverse-Tunnels zum Stehlen von Cookies und Exponieren von Daten in Salesforce und S3

VARONIS

Eine Legende der Cybersecurity zeigt uns, dass MFA kein Allheilmittel ist

Abrufen von Zugangsdaten durch Kennwortsynchronisierung für persönliches Konto

MFA mit kreativer Beharrlichkeit umgangen

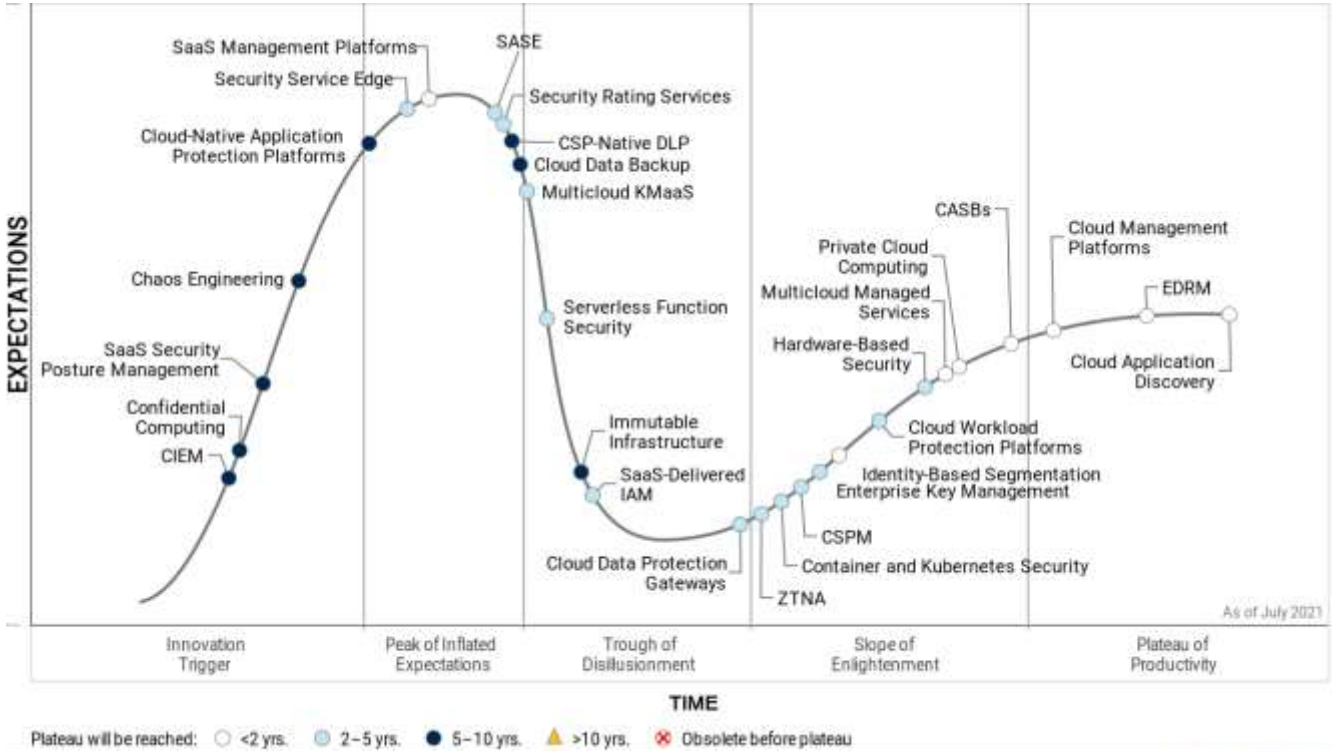
Zugriff auf das VPN erhalten

Zugriff auf Ressourcen erhalten

Was fehlt in Ihrer Cloud-Sicherheitsstrategie?

VARONIS

Gartners Hype Cycle for Cloud Security



Gartner

VARONIS

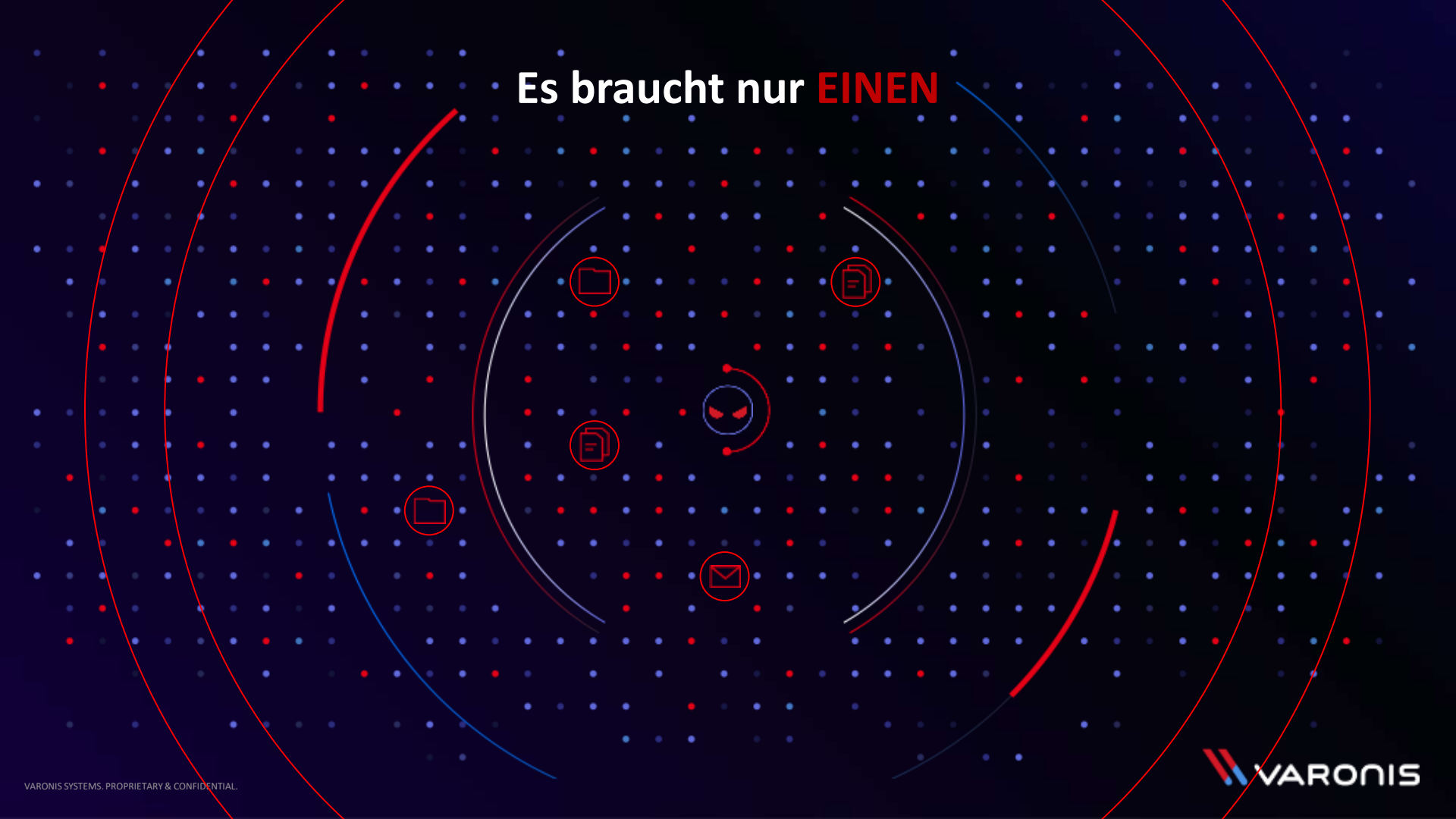
… erzeugen einen riesigen BLAST RADIUS

17 MILLION

DURCHSCHNITTLICHE # ANZAHL
DER VERFÜGBAREN DATEIEN
FÜR JEDEN MITARBEITER

VARONIS

Es braucht nur EINEN



Varonis reduziert den BLAST RADIUS

WENIGER ZUGRIFFE

SCHÄDEN REDUZIEREN

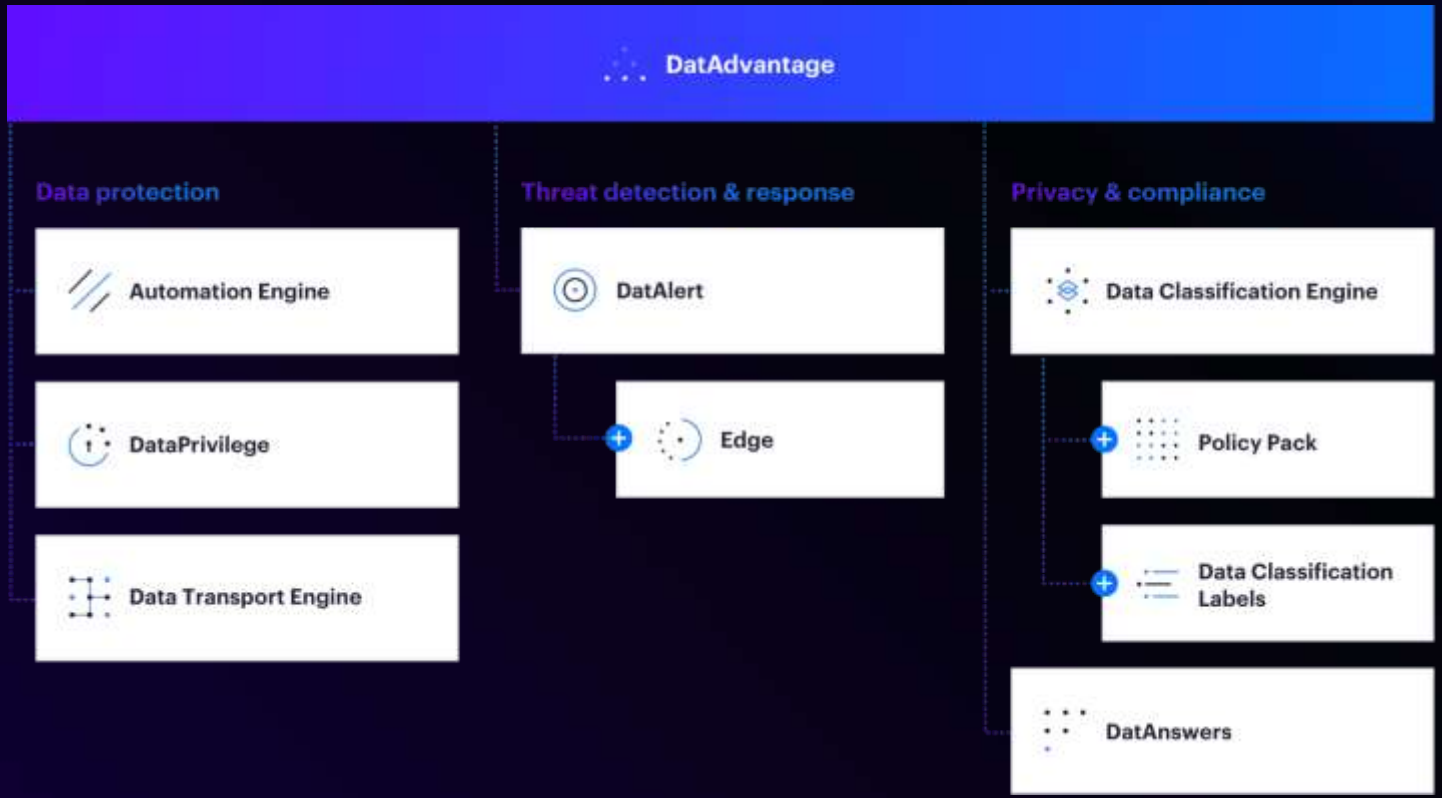
ANGREIFER BREMSEN

VARONIS

Varonis überwacht die DATEN

VARONIS

Die Varonis Data Security Plattform



Vielen Dank

Kommen Sie gerne auf einen leckeren Kaffee vorbei

Stand 319 / Halle 7a