Anatomie von modernen Attacken

how to break the attack chain…

Gerhard Mayer
Senior Account Manager
gmayer@proofpoint.com
+43 660 3010720

Christian Held
Senior Account Manager
sheld@proofpoint.com
+43 660 5088925

Proofpoint at a Glance

Financial strength

$1.7B Proofpoint Revenue

98% Recurring Revenue

21% Percentage of Revenue Reinvested in R&D

4.4K WW employees, hiring continues

Market Adoption

>230K Customers

150+ Global ISP and Mobile Operators

87% F100 Protected by Proofpoint

>60% F1000 Protected by Proofpoint

#2 DLP market share with examples of Pfizer, Tesla, GM, Intel

47% F100 using Proofpoint DLP

Proofpoint's Data

2.8T Consumer and Enterprise Emails scanned per year

1.3T SMS/MMS scanned per year

0.7T Attachments scanned per year

17T URLs scanned per year

>40% F1000 emails authenticated by Proofpoint

>135M Phishing Tests sent per year

36M BEC attacks stopped per year

84M Telephone Oriented Attacks stopped per year

151 and 0 Win rate over Red Teams in Identity Threat

proofpoint.

Some News

proofpoint.

BERICHT

Der Faktor Mensch 2023

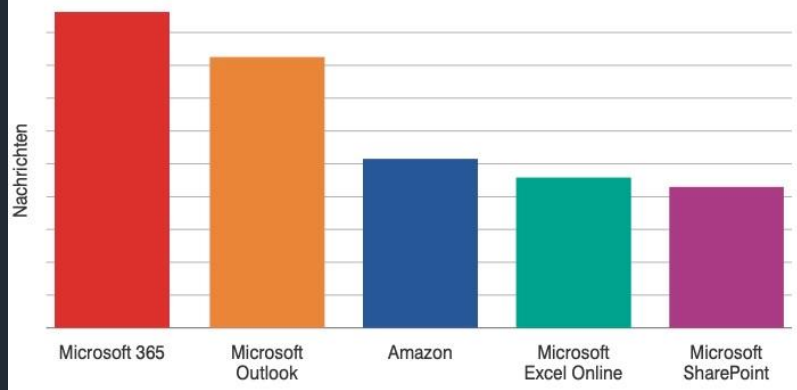
Eine Analyse der Cyber-Angriffskette

13 Millionen

TOAD-Nachrichten erreichten in der Spitze mehr als 13 Millionen im Monat

Häufigste Köder

Der Missbrauch bekannter Marken und unseres Vertrauens darin ist eine der einfachsten Formen von Social Engineering. Und wieder einmal haben die Cyberkriminellen einen klaren Favoriten, wenn es um Markenmissbrauch geht.



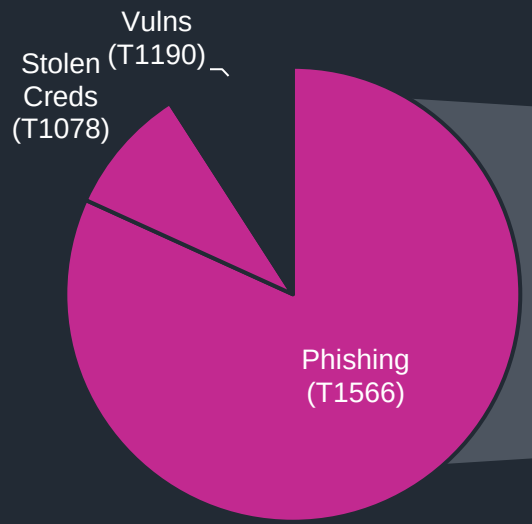
Microsoft-Produkte und -Services belegen vier der Top 5-Positionen bei missbrauchten Marken (unter allen Bedrohungen), wobei Amazon den anderen Platz einnimmt. Bei den von unseren Forschern untersuchten Kampagnen war Amazon dabei die am häufigsten missbrauchte Marke, doch Microsoft belegt immer noch die übrigen vier Plätze.

MFA-Umgehung

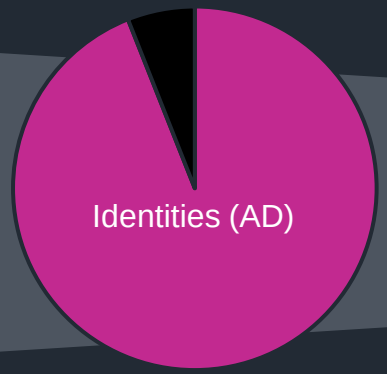
machte mehr als eine Million Nachrichten pro Monat aus

Attacker Tactics Standardize

Initial Access (92.3%)



Privilege Escalation + Lateral Movement (94%)

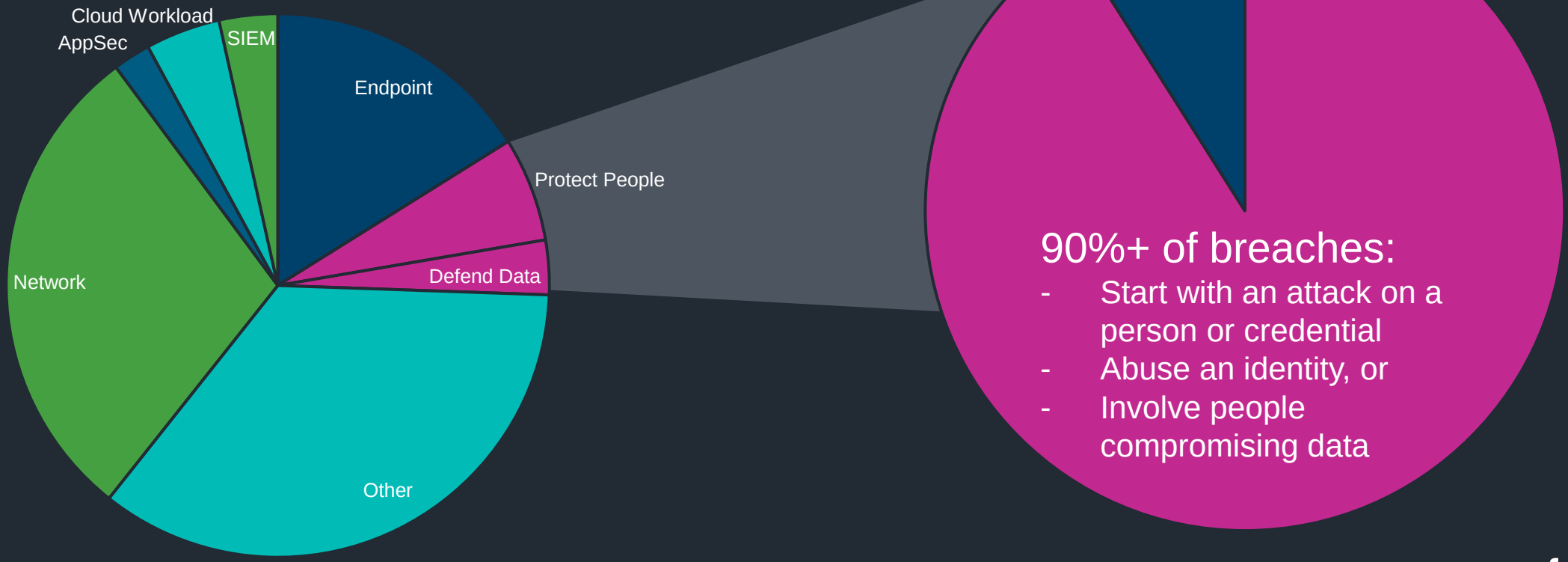


Data Loss (99%)

Sources: DFIR Report 2022 Year in Review, 2022 Verizon DBIR

While Risks Focused on People, Defenders Didn't

2022 Security Spending:
<9% on protecting people



2022 Security Breaches:
>90% people-centric

90%+ of breaches:
- Start with an attack on a person or credential
- Abuse an identity, or
- Involve people compromising data

Aligning People Risk Controls To The Attack Chain

Aegis

- Block targeted phishing, malware, and social engineering attacks
- Protect against impostor attacks
- Detect and respond to cloud account takeovers, including suppliers/vendors

Identity Threat Defense

1. Cut off common attack paths
2. Prevent privilege escalation
3. Detect lateral movement

Sigma

- Detect and block data exfiltration attempts
- Gain insight into risky user behavior

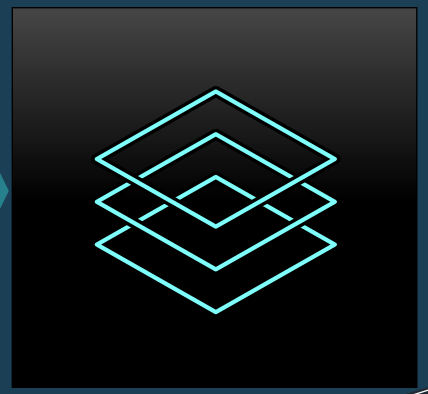
PROOFPOINT AEGIS

The Right Data + Analysis Powers the Industry's Leading Efficacy

CONTENT

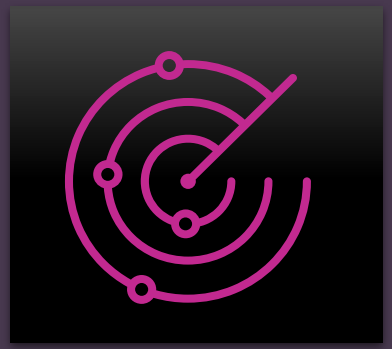
DATA
Daily Telemetry

ANALYSIS
Detection Stack



INTELLIGENCE

DATA
Threat Intel

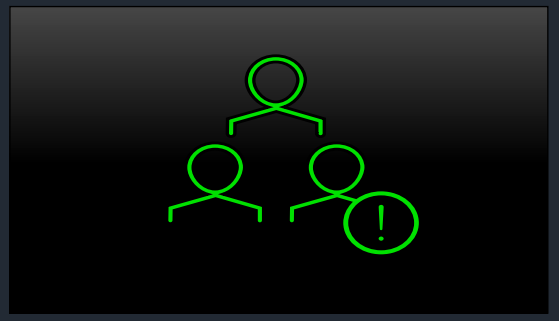


ANALYSIS
Threat Visibility

BEHAVIOR

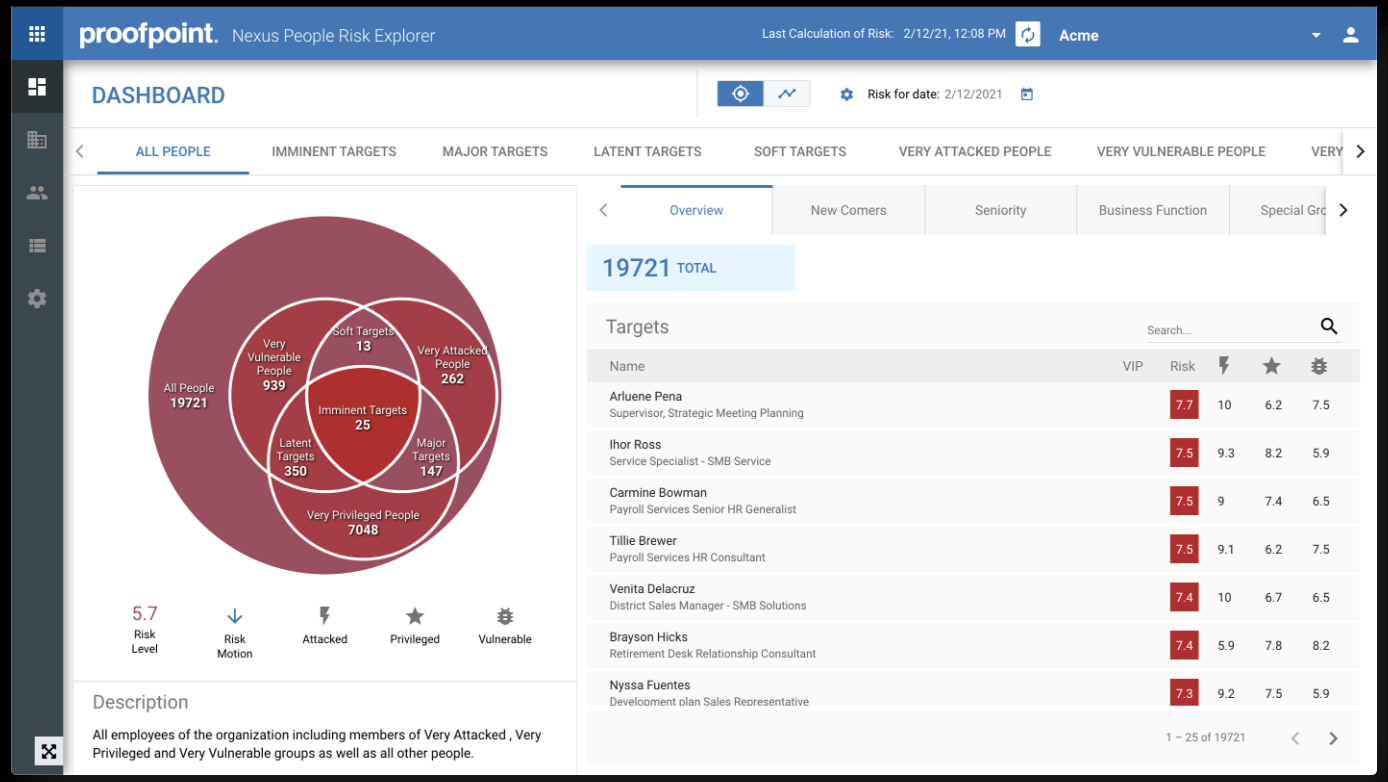
DATA
Interactions

ANALYSIS
ML Models



Assess: Identify Risky Users and Quantify Human Risk

Integrated with Proofpoint Threat Protection Platform



Nexus People Risk Explorer (NPRE)

- ✓ Uncover risky users and departments by evaluating their *vulnerability, attack index, and privilege*
- ✓ Prioritize security efforts and focus on *real risk of the organization*
- ✓ Provide recommended security controls that reduce risk score accordingly

Proofpoint Aegis

The most comprehensive, effective protection against initial compromise

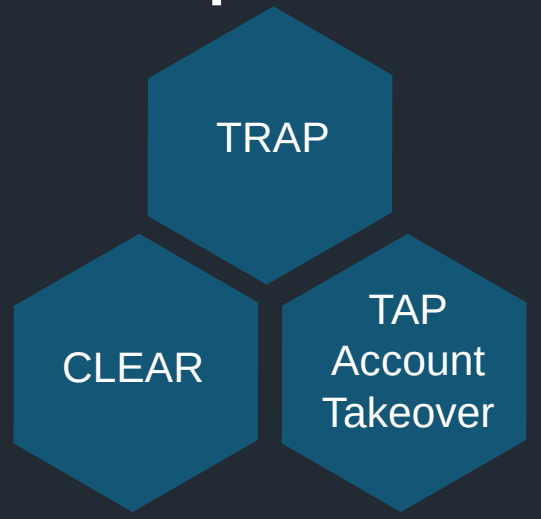
Pre-Attack

- Build user resilience
- Prevent impersonation
- Identify compromised suppliers

Attempted Compromise

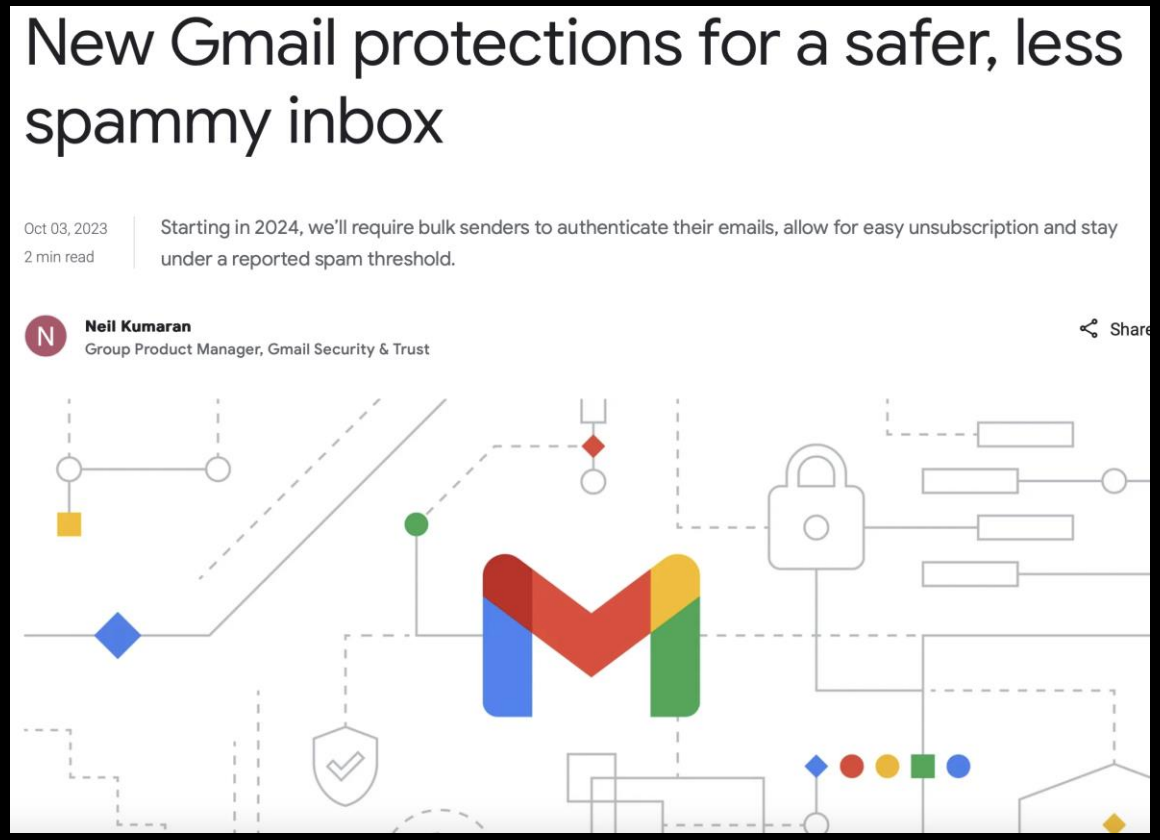
- Block malware, phishing, and impostor attacks
- Warn users about risky messages
- Isolate/block clicks on malicious links

Post-Compromise



- Respond to post-delivery detection and user reports
- Identify cloud ATO activity: logins, malicious messages, rules, and mor

Gmail / Yahoo enforce authentication Feb’24



Requirements:

- Implementation of both SPF + DKIM
- Sending with an aligned “From” domain in either the SPF or DKIM domains
- Sending from a domain with a DMARC policy of at least p=none
- Valid forward and reverse DNS (FCrDNS)
- One-click unsubscribe (RFC 8058)
- Low spam reported rate

[Google and Yahoo Set a Short Timeline to Meet New Email Authentication Requirements. Are You Ready? | Proofpoint US]

Aligning People Risk Controls To The Attack Chain

Aegis

- Block targeted phishing, malware, and social engineering attacks
- Protect against impostor attacks
- Detect and respond to cloud account takeovers, including suppliers/vendors

Identity Threat Defense

1. Cut off common attack paths
2. Prevent privilege escalation
3. Detect lateral movement

Sigma

- Detect and block data exfiltration attempts
- Gain insight into risky user behavior

Threat Defense Plan

100,000+ Endpoints managed with ½ person per month

Works across every environment - no interruptions

1 server supports >150,000 endpoints

1

ASSESS

YOUR ENVIRONMENT

Conduct a risk assessment giving visibility and recommendations

2

SHRINK

TRUE ATTACK SURFACE

Remove errant credentials, fix identity risks in AD and remediate gaps in PAM

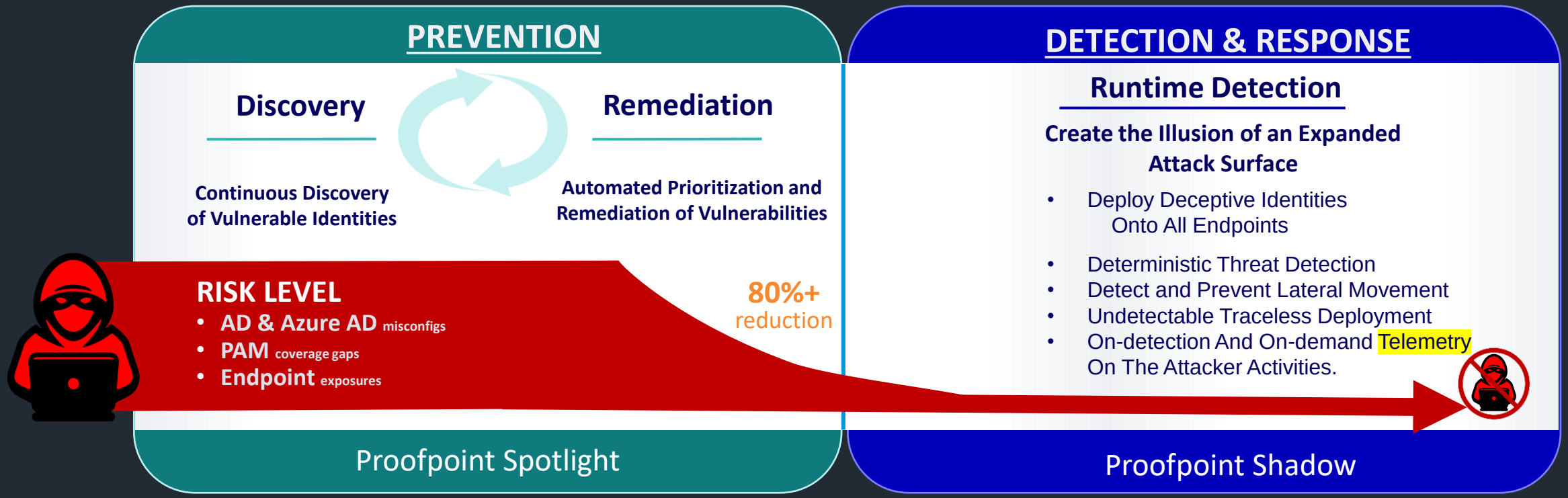
3

EXPAND

PERCEIVED ATTACK SURFACE

Distribute deceptions that force attackers to reveal themselves

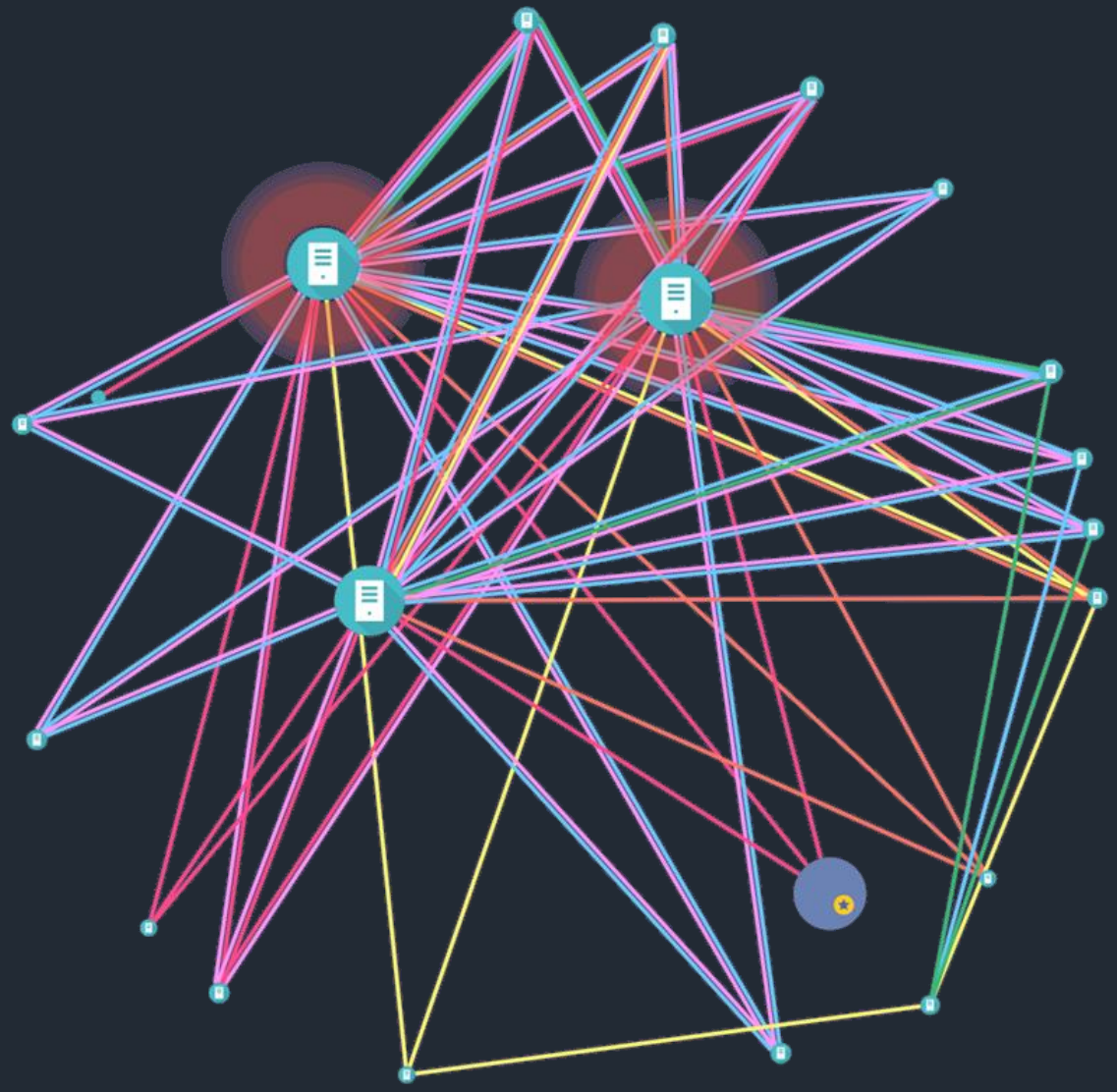
Proofpoint - The Complete Identity Threat Defense



AGENTLESS – NO BYPASS OPTION

Proofpoint Identity Threat Defense – Shadow

- High Fidelity Detection
- Detect Attacks that Bypass Security Tools
- Real-time Forensics
- Stop Ransomware Attacks and Data Exfiltration
- Protect Crown Jewels
- Beat the Red Team!
- Proofpoint 150:0 Red Team



Getting Started: Identity Threat Assessment

Quick & Easy Process

1. **One** endpoint from IT
2. up to **Two** hours of your time
3. **Three** compelling insights

100% of Illusive Audits
Find Privileged Identity Risk

Aligning People Risk Controls to the Attack Chain

Aegis

- Block targeted phishing, malware, and social engineering attacks
- Protect against impostor attacks
- Detect and respond to cloud account takeovers, including suppliers/vendors

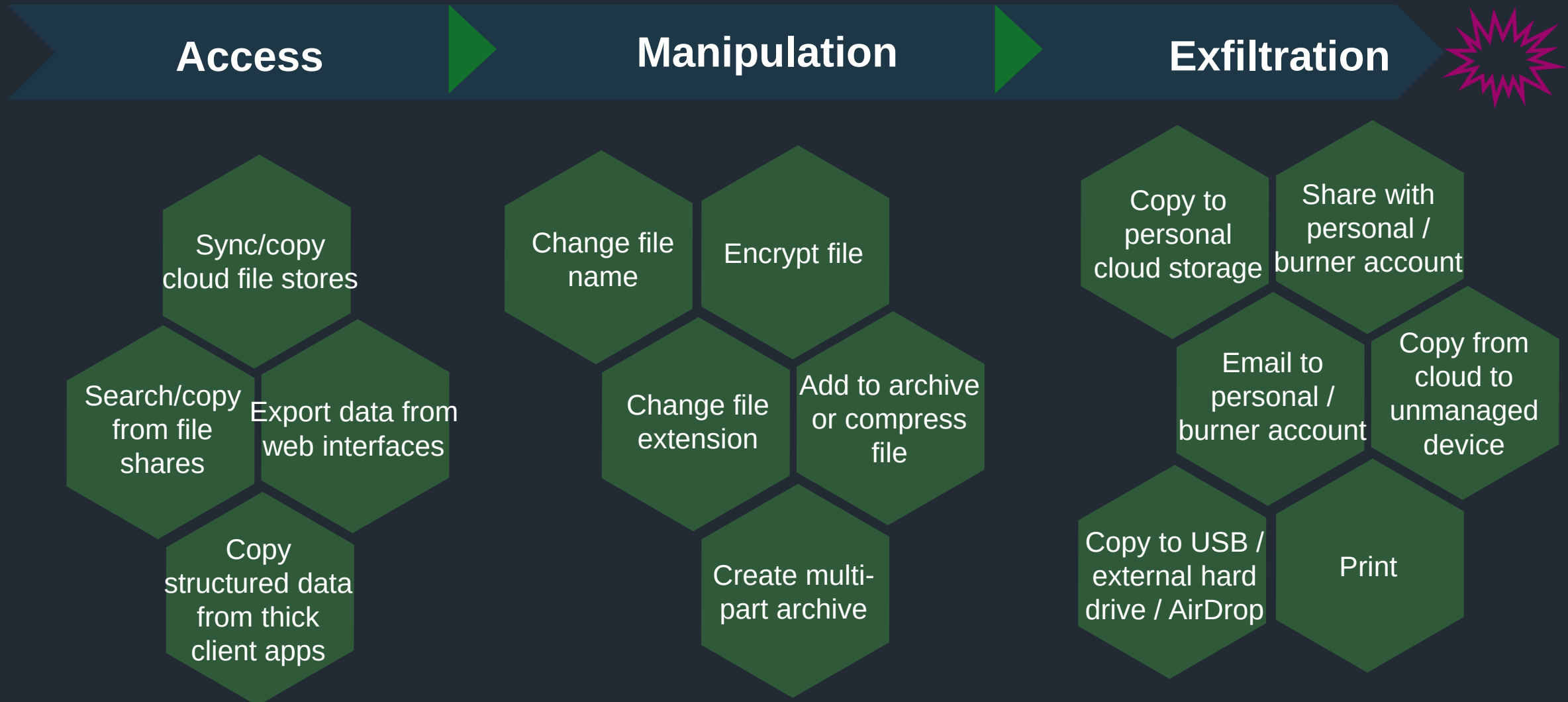
Identity Threat Defense

- Cut off common attack paths
- Prevent privilege escalation
- Detect lateral movement

Sigma

- Detect and block data exfiltration attempts
- Gain insight into risky user behavior

15 Patterns Cover 95%+ of Data Loss Incidents



Break The Attack Chain – Value

EFFICACY

Deploys quickly, covers 100% of your organization wherever they work, and stops threats and data loss **before** they compromise what you care about

"Proofpoint knocks down 85% of my risk—it's my most critical partner."

PHARMA CISO

VISIBILITY

Seeing who is being attacked, who is creating risk, and who is doing the attacking is indispensable in understanding risk

"The data is gold. Without Proofpoint, we'd be blind to what users did with data and clicked on at home."

LIFE SCIENCES CISO

OPERATIONAL EFFICIENCY

A people-centric security platform takes the burden off your users, your team, and your downstream controls

"After we deployed Proofpoint, the number of alerts our SOC needed to deal with went down 79%."

AIRLINE CISO

Ready to Get Started?

Three simple steps to start mitigating people risk in your organization:

Rapid Risk Assessment

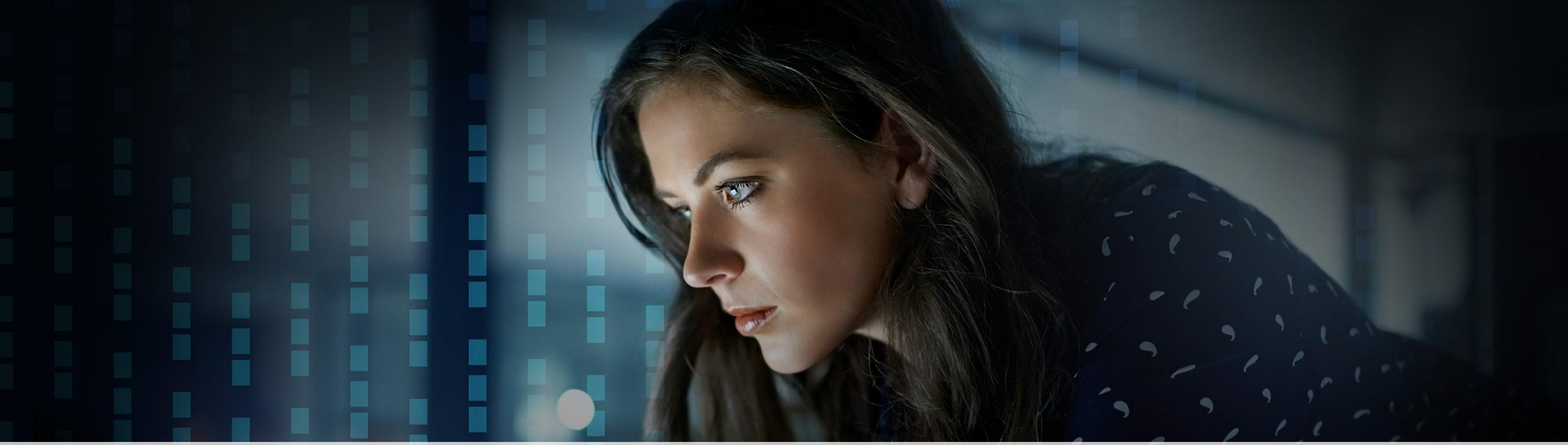
Quickly identify threats in your environment across email and cloud, including malware, credential compromise, and BEC

Identity Threat Assessment

Map out attack paths and identity risk in minutes, gaining the same visibility an adversary would have in your environment

DLP / Insider Risk Workshop

Leverage our experts to map out how to get better visibility into and control over data loss and insider risk in your organization



proofpoint®

Gerhard Mayer
Senior Account Manager
gmayer@proofpoint.com
+43 660 3010 720

Christian Held
Senior Account Manager
sheld@proofpoint.com
+43 660 5088925