

HUMAN-CENTRIC SECURITY

The force multiplier in a modern cybersecurity architecture

Why human-centric security is the critical element in a modern defense strategy, adapting, connecting and elevating your existing cybersecurity investments

proofpoint[®]



Executive summary

A key responsibility of the modern CISO is to determine the critical strategic investments to make in their company's cybersecurity architecture. And there are some well recognized security pillars — such as secure access service edge (SASE), extended detection and response (XDR) and identity — that must be at the core of an organization's defense strategy. These pillars cannot function independently. They must work in concert to ensure that the architecture addresses today's threats and future proofs the organization against tomorrow's. But while each of these pillars is a core component, none of them account for the biggest threat of all — people and their actions.

Human-centric security closes the loop: from the inbox to the endpoint, from identity to insider threats. Because behind every breach is a human: compromised, careless or malicious.

This white paper explores how human-centric security is the critical — and transformational — element in a modern cybersecurity architecture.

This paper:

- ✓ **Explains how human-centric security plays a pivotal role** in your overall architecture, eliminating blind spots in your existing protection and detecting human-driven risks across today's digital workspace.
- ✓ **Introduces the Proofpoint human-centric security platform.** This paper describes how Proofpoint acts as a strategic control plane, amplifying your existing security investments and protecting your organization against people-centric threats.

Beyond perimeters and point products: what's broken

Many CISOs are still fighting modern threats with legacy models. That means siloed controls, fragmented insights and tools that can't adapt quickly enough. But the attack surface has changed — so must our response.

Here's the new reality: Today's attackers target people, not ports. As digital workspaces expand, adversaries are targeting humans across email and numerous other digital channels. These include collaboration and messaging tools, social media platforms, cloud applications, large language models (LLMs) and file-sharing services. Attackers can also hijack trusted business communications, disrupting relationships with suppliers and customers.

At the same time, data doesn't lose itself. Behind every data loss incident are human actions. Careless users mishandle sensitive or critical data. Malicious users walk out with it. Hijackers compromise user accounts to steal it. Non-compliant users abuse it.

Choosing best-in-class tools remains important. But today's CISO must also focus on building an intelligent, cohesive architecture — one that evolves with the threat landscape and ensures that those tools work together to deliver the right defense outcomes.

At Proofpoint, we've built something unique in the industry: a comprehensive human-centric security platform that acts as a force multiplier — amplifying your security investments across email, identity, data and access.

We don't just close security gaps. Through deep integrations with partners such as CrowdStrike, Okta, Zscaler, Microsoft, Palo Alto Networks and others, we minimize dwell time, neutralize attacks earlier and give your security team back its time.

If you've been using us only for email protection, then we're just getting started. Welcome to the platform era.



The core pillars of a modern cybersecurity architecture

Every CISO recognizes them. They're the familiar, core pillars of a modern cybersecurity architecture: **SASE, XDR, identity, and SecOps & Automation**. As described below, each one is essential and solves an important set of risk concerns. But here's the problem: None of them account for the biggest risk in today's security landscape — people. **That's why human-centric security is now the most critical pillar of all.**

SecOps & Automation

Streamlines detection, investigation and response by eliminating manual effort and siloed workflows. Solves for slow response times, alert fatigue and operational inefficiency. Proofpoint automates threat triage and policy enforcement with integrated playbooks, enriched human-risk insights and flexible APIs. This enables security operations center (SOC) teams to act faster and with greater precision.

SASE

Enables secure and optimized access to applications and data, regardless of user location or device. Solves for distributed workforces, cloud access and consistent policy enforcement across remote environments. When informed by human-centric risk signals, SASE can prioritize protection for high-risk users or behaviors.

Human-centric security

Places people at the center of protection by addressing the reality that users — not infrastructure — are the primary targets of cyber threats. The Proofpoint human-centric security platform solves for phishing, data loss and account compromise by combining AI-driven threat detection with real-time user guidance. To reduce human-centric risk, our Nexus and Zen technologies uniquely and accurately identify risky users, behaviors and exposures.

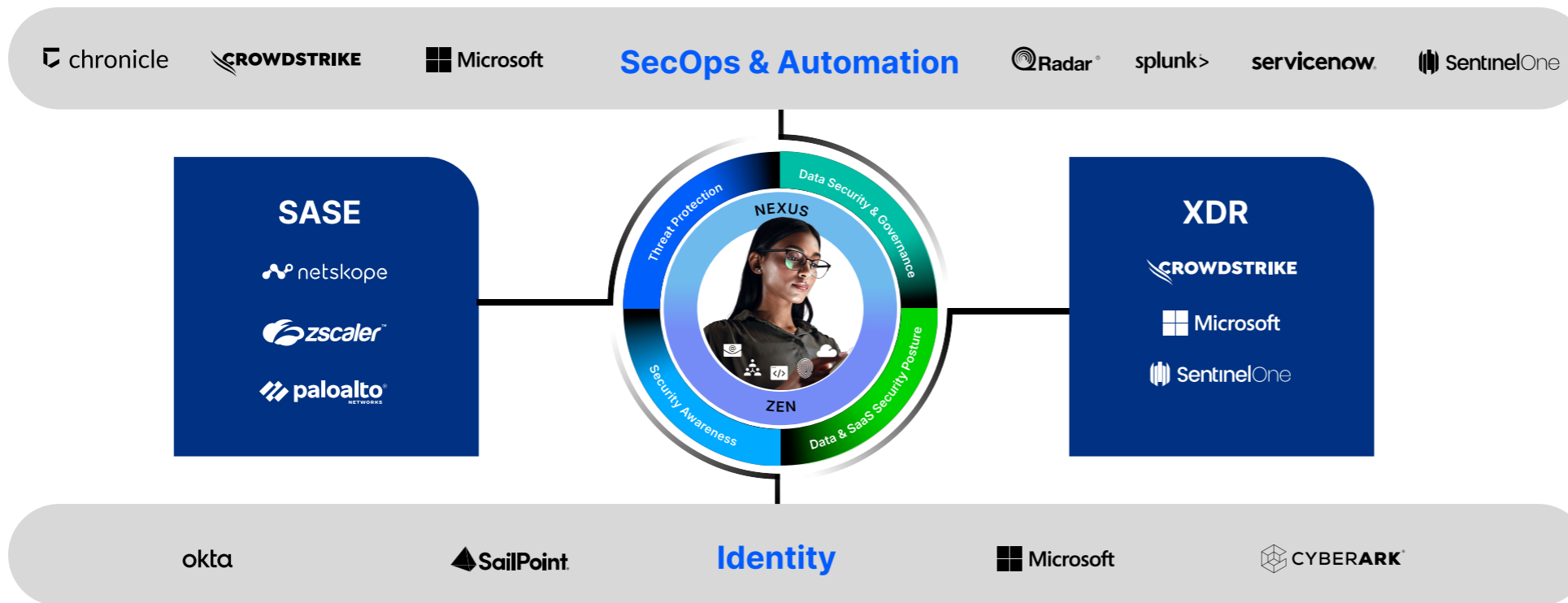
XDR

Unifies telemetry across email, endpoints, cloud and networks, streamlining threat detection, investigation and response. Solves visibility silos and slow responses. Human-centric telemetry from Proofpoint — such as who's targeted and who's risky — can enhance XDR with early and actionable context.

Identity

Secures user identities and access across cloud and on-premise environments by detecting account takeover, credential misuse and software as a service (SaaS) misconfigurations. Solves for identity sprawl and unauthorized access by continuously monitoring permissions, login behaviors and risky app configurations. With Proofpoint visibility of who has access to what — and why — security teams can prevent lateral movement and enforce least privilege.

Human-centric security as a force multiplier



The Proofpoint human-centric security platform acts as a strategic control plane in your cybersecurity architecture. It integrates with your existing security investments by providing human-centric risk signals that transform their effectiveness.

Our platform brings together understanding of data classification, user intent and threat context. It uses AI, machine learning and real-time threat intelligence to derive insights and drive automated policy decisions.

Here are some of the many ways that the **Proofpoint human-centric security platform** integrates with the other pillars in your architecture, transforming your overall protection:

SASE and adaptive access control

With partners such as Zscaler and Palo Alto Networks, Proofpoint integrates threat and behavioral intelligence to influence access policies in real time. Targeted users face step-up authentication or blocked access via Zscaler or Palo Alto Prisma Access. Malicious activity triggers immediate policy enforcement.

This is SASE informed by people, not just packets.

Identity and privileged access protection

We share risk context with Okta, CyberArk and SailPoint to shape access control dynamically. We identify your riskiest users and share those insights with our partners. Suspicious behavior? Enforce multifactor authentication. High-risk user? Apply adaptive controls and policies. Compromised account? Revoke access. Together, we bring Zero Trust to life through adaptive, identity-aware enforcement.

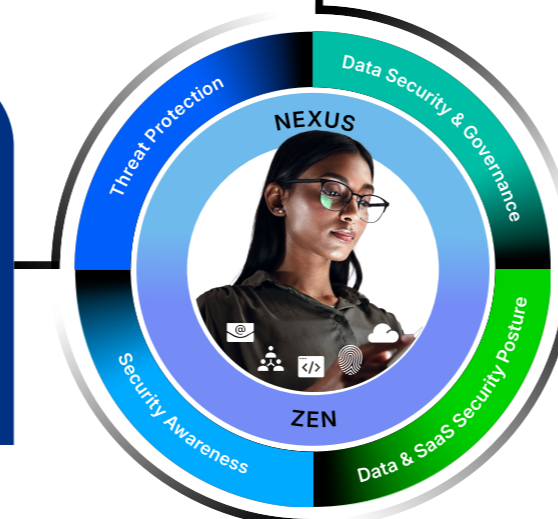
Accelerated, automated response

Proofpoint integrates with security information and event management (SIEM) and security orchestration, automation, and response (SOAR) platforms to reduce mean time to detect, investigate and respond — by delivering human-centric alerts and automating response actions. Risk signals from Proofpoint trigger automated playbooks in Cortex XSOAR or Splunk SOAR that quarantine users or reset credentials. Enriched alerts in Splunk or Microsoft Sentinel reduce false positives and accelerate triage. Proofpoint threat data and user behavior telemetry are shared across systems to enable unified workflows.

XDR that starts where attacks begin

Phishing is still the leading entry point. We close the loop with CrowdStrike, Microsoft Sentinel and SentinelOne. A flagged email triggers endpoint isolation in CrowdStrike or SentinelOne in seconds, not hours. User risk scoring and targeted threat context from Proofpoint enrich alerts in Microsoft Sentinel.

Proofpoint provides visibility of the first touch, so your XDR isn't blind to the beginning of an attack.



Your next moves: strategic, not tactical

The question isn't "what's the next tool?" It's how to build a platform that adapts, connects and elevates everything else that you already have.

Learn more about our integrations

Discover more integration use cases between Proofpoint and other components of your cybersecurity architecture. Visit proofpoint.com/use/partners/technology-alliance-partners.

Speak to Proofpoint today

- **Assess** how ready your security architecture is to handle people-centric threats.
- **Learn** how your existing investments — XDR, SASE and identity— can be amplified by our unified human risk intelligence.
- **See** what platform-driven security really looks like and how to take the first steps towards it. We'll show you how to turn human-centric insights into transformational security outcomes.

proofpoint.





proofpoint®

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 85% of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com

Connect with Proofpoint: LinkedIn

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.

DISCOVER THE PROOFPOINT PLATFORM →

0303-001-01-01