HUMAN-CENTRIC SECURITY

Measuring the Impact of Proofpoint Human-Centric Security

How to operationalize and measure the effectiveness of the Proofpoint human-centric security platform.

proofpoint.

Executive summary

Human-centric security is the force multiplier in a modern cybersecurity architecture, adapting, connecting and elevating your existing security investments. Proofpoint's comprehensive platform is powered by our core Nexus, Zen and Threat Protection Workbench technologies and provides best-of-breed solutions to solve four critical concerns: stopping threats, protecting information, guiding users and securing app and identity posture.

But bringing human-centric security to life is about more than just purchasing the technology. To execute and show the impact of our multilayered platform, your organization must adopt the right operational model and understand how to measure success.

This paper:

- ✓ **Explains how successfully putting our platform into operation** depends on empowering and aligning multiple organizational roles
- ✓ **Introduces some key personas** commonly found in modern enterprises, highlighting their primary focus areas and concerns
- ✓ **Outlines the key metrics** that each persona can use to demonstrate clear, measurable outcomes.

Key roles for implementing human-centric security

Human-centric security aligns security strategy and technology with real human behavior. By recognizing that people and their behaviors—not just systems—are at the core of strong security outcomes, it introduces new responsibilities and a new operational model.

For these reasons, successfully integrating Proofpoint's human-centric security platform with your existing security stack requires a multidisciplinary, cross-functional approach. To succeed, your organization should consider how to align various personas and empower them to achieve their target security outcomes. Of course, every organization has its own unique structure, with varying roles and responsibilities. However, some key personas commonly seen in modern enterprises are described here.

Chief Information Security Officer (CISO)

Owns the overall security architecture and strategy. Must demonstrate ongoing posture improvement and investment impact to validate the effectiveness of human-centric security.

Chief Legal and Chief Compliance Officers

Oversee legal defensibility, corporate governance, data privacy and regulatory compliance. Ensure audit readiness and defensible incident response. Work closely with the CISO to ensure that cybersecurity strategy and governance aligns with legal, privacy and compliance requirements.

Cybersecurity Architect

Encompasses roles such as **identify and access management (IAM)** and **endpoint and IT management**. Focuses on the design, development and integration of security frameworks, policies and technologies. Uses Proofpoint telemetry to design security architectures that are robust, scalable and adaptable to emerging threats. The **CISO** also contributes to this area through their overall ownership of the security architecture.

Security Analyst

Encompasses roles such as **security operations center (SOC)**, **insider threat investigation and data loss protection (DLP)**. Focuses on threat detection and response. Integrates Proofpoint human-centric telemetry for faster, more precise investigations and incident containment.

Security Awareness and Training Lead

Focuses on changing user behavior through education. Uses Proofpoint behavioral data to provide just-in-time coaching and drive meaningful behavioral shifts.

Based on their unique security and reporting objectives, each of these personas typically works with different parts of the Proofpoint human-centric security platform.

These focus areas are shown in the figure on the next page.

Proofpoint human-centric security: focus areas for common cybersecurity personas

THREAT PROTECTION

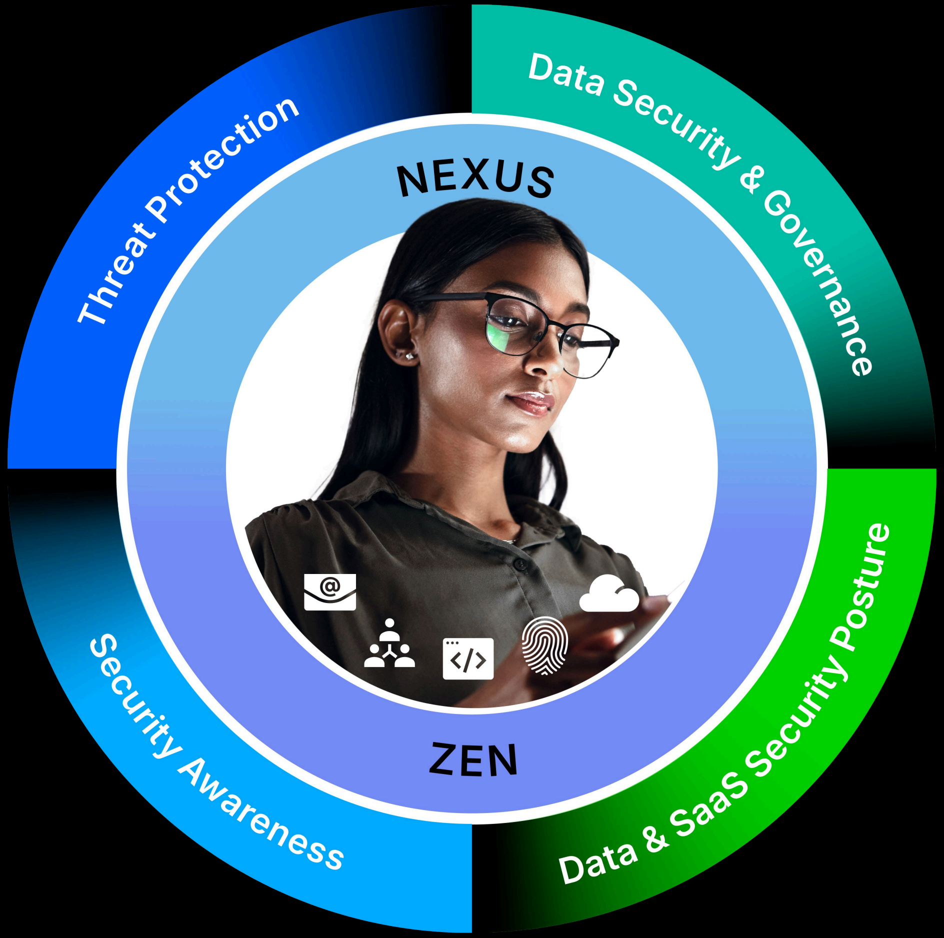
Stop threats targeting your people

- CISO
- Cybersecurity Architect
- Security Analyst
- Security Awareness & Training Lead

SECURITY AWARENESS

Provide employees with continuous guidance

- CISO
- Security Awareness & Training Lead
- Chief Legal & Compliance Officers



DATA SECURITY & GOVERNANCE

Prevent data loss & govern communications

- CISO
- Cybersecurity Architect
- Security Analyst
- Chief Legal & Compliance Officers

DATA & SAAS SECURITY POSTURE

Remediate data & SaaS exposures

- CISO
- Cybersecurity Architect
- Security Analyst

proofpoint.

Putting human-centric security into action

As previously described, successfully executing Proofpoint's human-centric security platform requires aligning several organizational personas. The following sections examine these personas, their areas of focus in the Proofpoint platform, their priorities and some key metrics they can use to measure success.

Chief Information Security Officer (CISO)

FOCUS AREAS

- Threat Protection
- Data Security & Governance
- Data & SaaS Security Posture
- Security Awareness

The CISO is the overall owner of the enterprise security architecture and the strategic voice to the board and senior management. They set security direction aligned to business risk and must demonstrate ongoing improvement in security posture, architectural and program maturity, and return on investment (ROI). Their strategic oversight spans the whole Proofpoint platform.

PRIORITIES

1. Validating that architecture-wide security controls improve organizational resilience

2. Ensuring seamless and effective integration between Proofpoint and other security investments, such as security information and event management (SIEM), security orchestration, automation, and response (SOAR), extended detection and response (XDR), secure access service edge (SASE) and identity and access management (IAM)

3. Demonstrating measurable ROI (for example, reduced user risk, faster mitigation)

KEY SUCCESS METRICS

Risk Posture Delta by Role

Description: The change in an organization's risk score over a defined period, segmented by user group

Example: Reduction in executive team risk scores from 9.2 to 4.7 (on a 10-point scale) over 90 days

Source: Proofpoint Nexus user risk scoring, aggregated by role group in Proofpoint Human Risk Explorer

Time to Strategic Mitigation

Description: The average time from initial detection of a major campaign to establishment of a stakeholder-approved mitigation plan

Example: Average of 22 hours from attack detection to approved mitigation plan

Source: Proofpoint Threat Protection Workbench response timelines and executive incident reports

Platform Leverage Index

Description: The percentage of security stack integrations—such as SIEM, SOAR, XDR, SASE and IAM—that are actively consuming telemetry from Proofpoint

Example: 73% of security stack integrations are consuming Proofpoint telemetry

Source: Integration health and API usage logs in Proofpoint and integrated tools

✓ **These metrics demonstrate the effectiveness of human-centric security in reducing risk and validate Proofpoint's role in driving architecture-wide security outcomes.**

proofpoint.

Security Analyst

PRIORITIES

1. Precision and speed: fewer false positives, faster response
2. Clear visibility of human-centric risk
3. Seamless workflows with enriched context from Proofpoint telemetry
4. Reduced dwell time and improved operational readiness

FOCUS AREAS

- Threat Protection
- Data Security & Governance
- Data & SaaS Security Posture

The Security Analyst monitors, investigates and responds to threats and risky behaviors. Telemetry from the Proofpoint human-centric security platform influences how they prioritize alerts, triage high-risk users, respond to incidents and drive investigations. They benefit from integration of Proofpoint telemetry with SIEM and SOAR platforms, enabling an advanced level of speed and precision.

KEY SUCCESS METRICS

Human-Risk-Driven Triage Rate

Description: The percentage of high-priority alerts initiated by behavioral telemetry

Example: 64% of high-priority alerts initiated by telemetry from Proofpoint

Source: Proofpoint-to-SIEM alert mapping and escalation logic

NOTE: The TAP SIEM API endpoint integrates Proofpoint Targeted Attack Protection (TAP) with SIEM systems for centralized analysis of email threats, malicious URLs and attachments. You can consolidate this threat data into operational intelligence platforms such as Splunk. This enables faster detection and response, simplified security workflows and improved visibility of security incidents across your environment.

False Positive Reduction Rate

Description: The percentage decrease in false positive alerts over a given period

Example: 41% decrease in false positives for VIP impersonation attempts

Source: Feedback and alerts to SOC tools triggered by Proofpoint telemetry

✓ **These metrics show that Proofpoint enhances precision, incident and work prioritization and analyst efficiency.**

proofpoint.

Cybersecurity Architect

FOCUS AREAS

- Threat Protection
- Data Security & Governance
- Data & SaaS Security Posture

The Cybersecurity Architect translates security strategy into enforceable controls. They deploy and maintain security tools across identities and devices. And they enforce Zero Trust principles by linking user behavior with access governance.

PRIORITIES

1. Getting the most value from security investments
2. Implementing effective policies across endpoints, cloud and user workflows
3. Ensuring that controls scale with minimal friction or drift
4. Ensuring that security architecture design, policies and controls are forward-looking, to meet both present and future enterprise needs

KEY SUCCESS METRICS

Access Revocation SLA Adherence

Description: The percentage of compromised or terminated user accounts whose access is revoked within a strict, predefined service level agreement (SLA) time

Example: 94% of compromised accounts revoked within 10 minutes of alert

Source: Okta or SailPoint audit logs triggered by Proofpoint telemetry

Dynamic Access Enforcement Rate

Description: How often, in a given period, the system enforced conditional access policies based on real-time user risk telemetry

Example: 312 instances of dynamically enforced access control in 30 days, based on Proofpoint user risk signals

Source: Policy event logs in Okta, integrated with Proofpoint Nexus

Privileged Access Risk Alignment

Description: The correlation between a user's real-time risk score and their eligibility for privileged access

Example: 89% of privileged access granted only to users with low or medium Proofpoint risk scores

Source: Cross-reference of Proofpoint user risk API and IAM role assignments

✓ **These metrics show how behavior-driven signals from Proofpoint drive access governance and real-time Zero Trust enforcement. They also show that security enforcement is silent, stable and scalable.**

Security Awareness and Training Lead

FOCUS AREAS

- Threat Protection
- Security Awareness

The Security and Awareness Training Lead focuses on influencing and changing user behavior through targeted training, coaching and awareness initiatives. They conduct realistic security simulations—such as fake phishing attempts—to assess and improve user vigilance.

PRIORITIES

1. Ensuring long-term behavioral shifts and fostering a resilient, security-conscious culture

2. Using Proofpoint telemetry to drive real-time user coaching

KEY SUCCESS METRICS

Behavior Correction Rate

Description: The percentage of users who show positive changes in security behavior after an instance of real-time coaching

Example: 72% of users stopped pasting sensitive content into AI tools after just one warning

Source: Proofpoint ZenWeb real-time coaching logs

Phishing Report-to-Click Ratio

Description: The ratio of phishing attempts reported to those clicked

Example: Ratio improved from 1:3 to 3:1 in 90 days

Source: Email gateway click tracking and user report metrics

✓ **These metrics show that Proofpoint helps security awareness teams go beyond tracking training completion to also measuring meaningful shifts in user behavior.**

Chief Legal and Chief Compliance Officers

FOCUS AREAS

- Data Security & Governance
- Security Awareness

Chief Legal and Chief Compliance Officers focus on legal defensibility, corporate governance, data privacy and regulatory compliance. They also watch for future enterprise risk. They work closely with the CISO to ensure that cybersecurity strategy and governance aligns with legal, privacy and regulatory requirements. This includes communications capture and insider incident reviews.

PRIORITIES

1. Preventing regulatory breaches and fines
2. Quickly identifying and correcting misconduct or control failures
3. Protecting the company from present and future legal liability and reputational harm

KEY SUCCESS METRICS

Supervision SLA Completion Rate

Description: The percentage of supervised digital communications that reviewers assess within a strict, predefined SLA time

Example: 98% of supervised Slack or Teams messages reviewed within 48 hours

Source: Proofpoint Supervision

Escalation Defensibility Rate

Description: The percentage of escalated incidents that include evidence for audit readiness and defensibility

Example: 100% of escalated incidents include timeline evidence, behavioral audit trail and message capture

Source: Proofpoint Insider Threat Management and archive APIs

✓ **These metrics validate compliance, audit readiness and legal defensibility.**

Conclusion

Proofpoint's human-centric security platform is the critical element in a modern cybersecurity architecture. Our platform acts as a strategic control plane that amplifies existing security investments and protects against human-centric threats.

However, successfully integrating it with the other tools in your security stack requires a clear vision of who in the organization must be involved, what security outcomes are most important and how you can measure success. With the right operational model, your organization will be ready to show improved resilience, measure gains in operational efficiency and demonstrate immediate and continued return on investment.

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

DISCOVER THE PROOFPOINT PLATFORM →