HUMAN-CENTRIC SECURITY

Implementing human-centric security in the modern digital workspace

How Proofpoint's comprehensive, multilayered protection platform brings human-centric security to life in the age of digital transformation

proofpoint®

Executive summary

The modern digital workspace has fundamentally changed how work gets done. Organizations have embraced the cloud, and workers now collaborate across a complex mix of environments. These include email, collaboration and messaging tools, social media platforms, software as a service (SaaS) apps, large language models (LLMs) and file-sharing services.

This shift has enabled faster innovation and greater flexibility. But it has also introduced many new surfaces of risk for threat actors to exploit. Knowledge workers now generate, store and access data in ways that traditional security strategies focused on protecting networks and endpoints can no longer keep up with. These changes demand a modern architecture that aligns with how organizations and individuals work. An architecture that addresses the reality that users — not infrastructure — are the primary targets of cyber threats.

This white paper explores how Proofpoint has delivered an industry first: a comprehensive, human-centric security platform that addresses these new realities by putting people at the center of the modern defense strategy.

This paper:

- **Explains why protecting people matters** more than ever in today's digital workspace
- **Describes the human-centric problems** the Proofpoint platform was built to solve
- **Examines the core technologies** driving an architecture that detects threats proactively, guides and protects users in real time and streamlines investigation and response

People as the new perimeter: Why human-centric security is critical

At the center of today's cybersecurity challenge is the individual. Human-centric threats, including phishing, account takeover, insider risk and data exfiltration, now account for the majority of breaches. Most modern attacks don't exploit technical vulnerabilities — they exploit people. Whether through deception, distraction or manipulation, threat actors target users within increasingly complex digital workspaces.

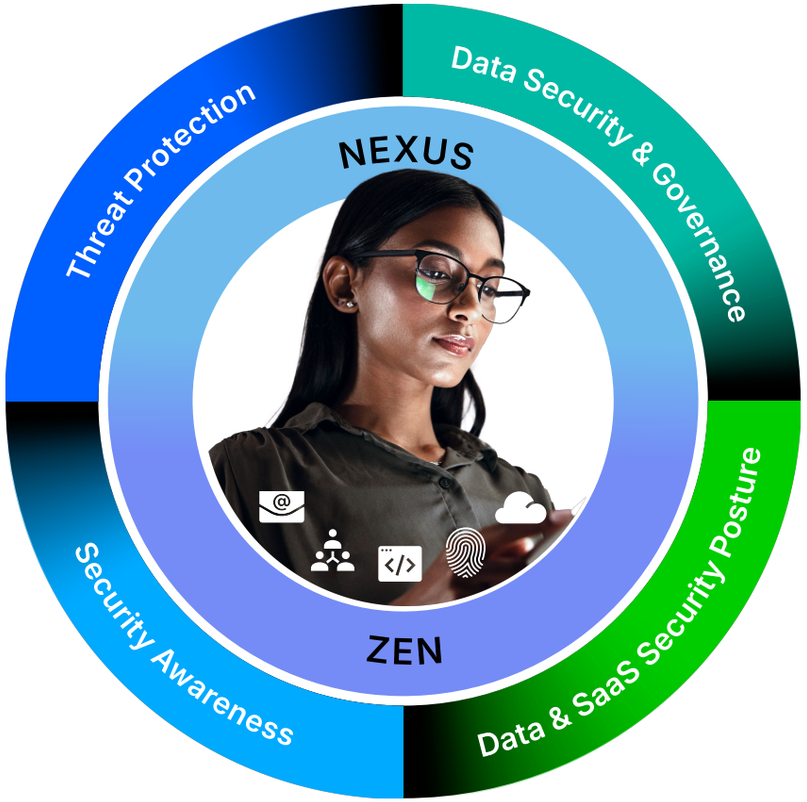
Traditional security models have focused on protecting networks and endpoints. But modern threats target human vulnerabilities. With the Proofpoint cybersecurity platform, organizations can protect people and defend data by taking a human-centric approach. Our platform provides best-of-breed solutions to address four critical concerns: stopping threats, protecting information, guiding users, and strengthening data and SaaS security posture.

THREAT PROTECTION

Stop threats targeting your people

SECURITY AWARENESS

Provide employees with continuous guidance



DATA SECURITY & GOVERNANCE

Data loss and govern communications

DATA & SAAS SECURITY POSTURE

Remediate data & SaaS exposures

Figure 1: The Proofpoint human-centric security platform provides best-of-breed solutions in four key areas.

A comprehensive, multilayered protection platform

Proofpoint's comprehensive platform is based on a multilayered architecture that:

- **Detects threats proactively** across the whole digital workspace by using capabilities such as advanced AI, machine learning and real-time threat intelligence
- **Provides a broad set of end-user control points** that protect people and data, no matter where work happens
- **Alerts, guides and empowers users** to be resilient against human-targeted attacks
- **Streamlines threat investigation and response**

These capabilities are driven by three core technologies: Nexus, Zen and Threat Protection Workbench. The sections that follow explore these technologies.

Nexus

Detection powered by AI and threat intelligence

Proofpoint Nexus® is the detection layer of the Proofpoint architecture. It is a unified detection framework that's powered by AI, machine learning and real-time threat intelligence.

Nexus integrates multiple AI model types. Each one is designed to analyze specific risk signals across all the ways that people work. These include email, cloud apps, collaboration tools and browsers.

Key components of the Nexus detection framework

Nexus Threat Intelligence (TI) continuously ingests signals from both known and unknown threat actors, campaigns and infrastructures to provide Proofpoint products with context-rich detections and the ability to adapt to evolving threat techniques.

Nexus Language Model (LM) harnesses the power of advanced AI language models to evaluate the tone, urgency and linguistic structure of messages used in social engineering attacks, such as business email compromise (BEC).

Nexus Relationship Graph (RG) correlates user activity, behavior history and role sensitivity to assess the likelihood of risky behavior or targeted attacks on high-risk individuals.

Nexus Machine Learning (ML) detects unusual user behavior across communication and collaboration tools, identifying subtle but impactful signals of compromised accounts or insider misuse.

Nexus Computer Vision (CV) recognizes brand impersonation and visual fraud tactics by analyzing layout, logo placement and design mimicry. Using advanced computer vision technology, it detects threats hidden in visual elements, such as phishing sites, QR codes, malicious attachments and spoofed emails.

Nexus detects advanced phishing attacks, credential theft, impersonation attempts and ransomware campaigns. In one real-life case, Nexus identified a supplier compromise that led to invoice fraud targeting a finance department. Nexus blocked the attack before execution by identifying unusual language and visual mismatches and by applying existing threat intelligence from its global dataset.

Nexus also excels at protecting data. In another real-life case, when an employee pasted customer data into an unauthorized generative AI tool, Nexus detected the sensitive data pattern, elevated the risk score and blocked the action.

Nexus analyzes more than **2.6 billion emails per day, inspects over 450 million URLs daily** and correlates signals from hundreds of threat actors. This enormous scale enhances both accuracy and responsiveness across the whole threat landscape.

proofpoint.

Zen

Control points and contextual user guidance

Proofpoint's Zen™ is the enforcement and user guidance layer of the Proofpoint architecture. It enforces security policies right where users are working. The control points in the Zen suite convert intelligence into real-time protection and policy-aligned coaching. This helps users to make safer decisions without slowing them down.

Key components of the Zen suite

Zen for Outlook empowers users as frontline defenders by embedding security tools in their email workflows. Using real-time threat intelligence from Nexus, it shows users inline warnings when they receive suspicious emails and allows easy reporting. It provides smart nudges for risky behaviors and alerts for sensitive data in outbound emails.

ZenWeb is a lightweight extension for Chromium-based browsers that secures web activities across SaaS, file-sharing and generative AI tools and protects users against phishing sites. Using live detections from Nexus threat models, it provides real-time threat detection and prevention without disrupting user productivity.

Zen Endpoint DLP/Insider Threat Management provides device-level protection against data loss and insider threats by monitoring user behavior at the endpoint. Monitors USB usage, clipboard activity, file sync operations and app behavior. Captures screenshots of suspicious user actions and timelines of user activities.

Zen Cloud API Connectors extends security to cloud-based SaaS platforms such as Microsoft 365, Google Drive, Slack and Box. Monitors file uploads and detects unusual behavior such as excessive sharing. Also enables custom workflows in Okta and security orchestration, automation and response (SOAR) tools.

Zen Communications Connectors captures communications in regulated platforms, such as Microsoft Teams, Zoom and Slack, for archiving and supervision. Ingests messages from various channels into a unified archive format and integrates with supervision tools for human resources and legal workflows.

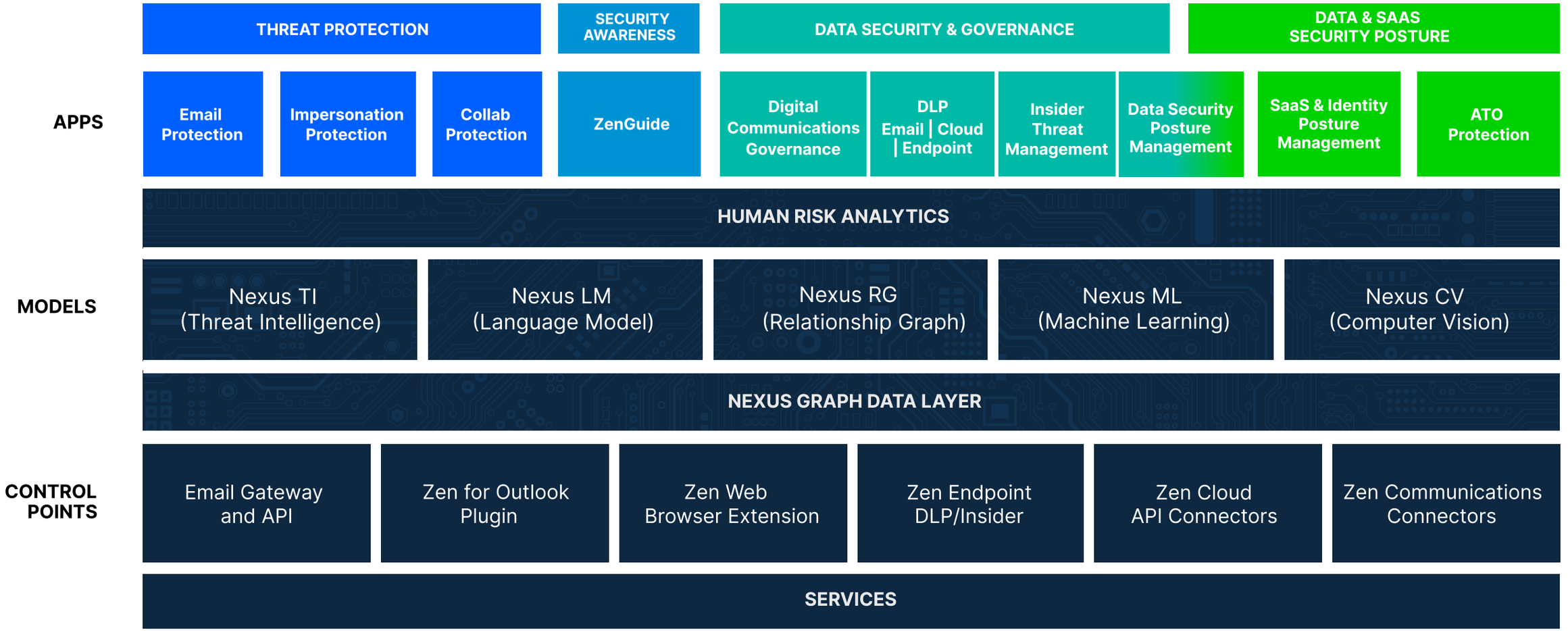


Figure 2: The Proofpoint human-centric security platform is built on a multilayered architecture. Proofpoint products (in our key solution areas of Threat Protection, Security Awareness, Data Security & Governance, and Data & SaaS Security Posture) directly use the capabilities of our core Nexus and Zen technologies

Threat Protection Workbench

Rapid investigation and automated remediation

When a threat is detected or a policy violation is flagged, speed and clarity become critical. For security operations center (SOC) teams, multiple consoles, excessive clicks and dependencies on other teams slow down response times and increase the risks of successful attacks.

Proofpoint Threat Protection Workbench is the investigation and automation layer of the Proofpoint architecture. By providing an intuitive, centralized console, it streamlines threat investigations and remediation. It enables security teams to triage, analyze and respond to threats without the delays caused by tool switching or fragmented data.

Security teams use Threat Protection Workbench to process abuse mailbox submissions, escalate signals about high-risk users and investigate threat campaigns. By correlating threat intelligence from Nexus with user behavior and policy triggers, Threat Protection Workbench delivers high-fidelity alerts rather than unwanted noise.

Threat Protection Workbench example use cases

- Automated responses for account takeover investigations
- Click-path visualizations for targeted users
- Summarization of complex multichannel threats

All of these capabilities reduce analyst workload and threat dwell time. To respond to threats, analysts can trigger playbooks directly or use APIs to escalate them to other, integrated components in their broader security stacks.

Conclusion

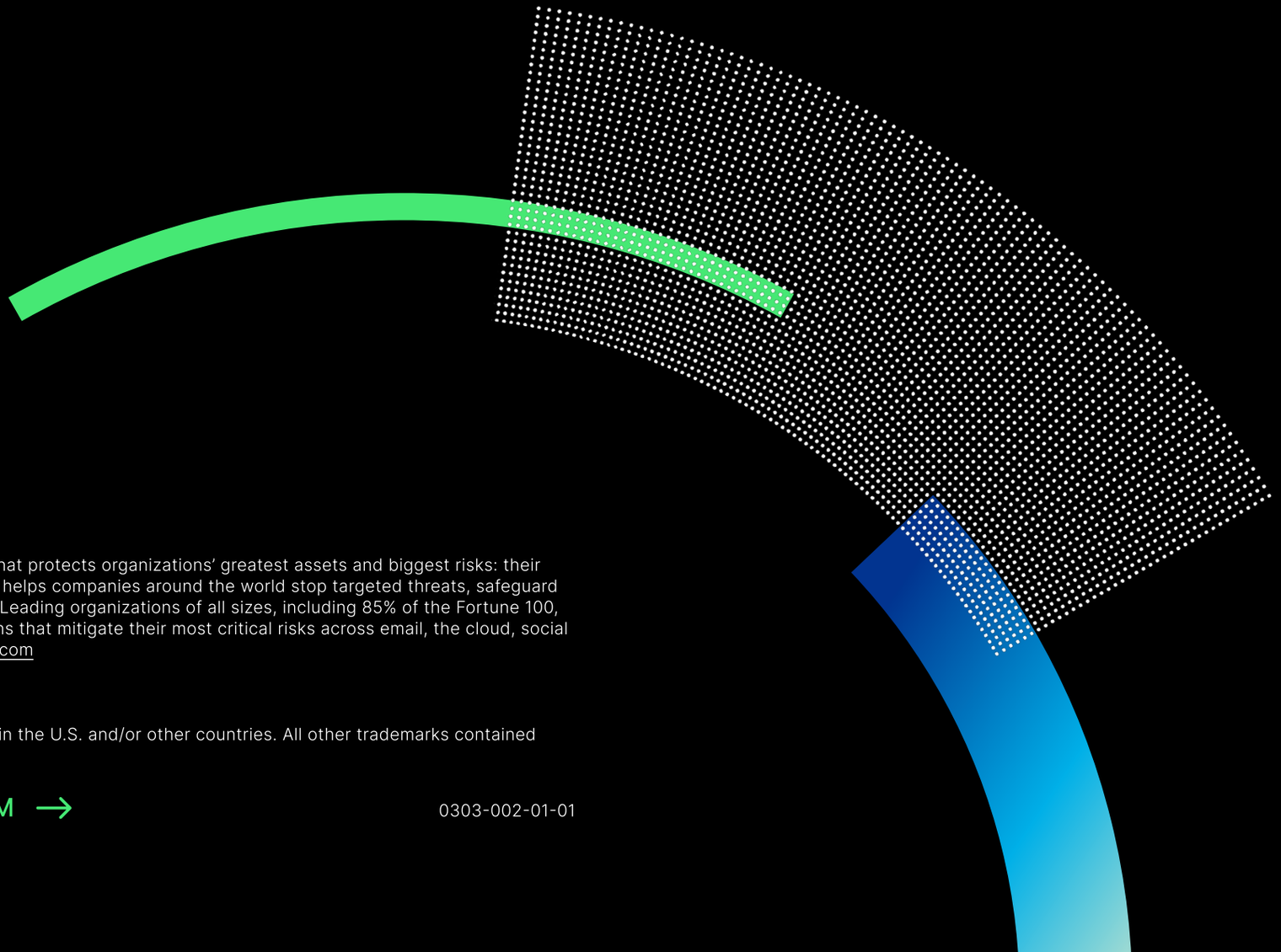
A purpose-built architecture for human-centric security

The nature of cyber risk has changed. Threats don't just target systems — they target people. And the complexity of the digital workspace has outpaced the defenses built to protect it. As users move fluidly between email, browsers, collaboration tools and cloud applications, the old security model — one built around static perimeters and one-size-fits-all controls — can no longer keep up.

Proofpoint's platform solves this challenge by aligning security architecture with the way people work. Through Nexus, organizations get AI-driven visibility into human-centric threats, built on unmatched threat intelligence and behavioral analysis. With Zen, our platform protects and coaches users in the moment, without friction. And with Workbench, security teams respond faster, with clearer insights and less operational overhead.

This is not theoretical. Our platform is a proven, production-scale architecture that reduces risk and builds long-term resilience. Organizations can protect today's workflows and prepare for the next evolution in human-centric risk.

By combining world-class detection, embedded behavioral controls and fast, integrated response, we can help your organization reduce risk where it matters most: at the intersection of people, data and threat.



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

DISCOVER THE PROOFPOINT PLATFORM →

0303-002-01-01