proofpoint.

SOLUTION BRIEF

Securing life sciences organizations with Proofpoint

Protect intellectual property, AI agents, and employees to ensure resilient innovation

Overview

Life sciences organizations are operating in an era where research and development is digital, distributed, and accelerated by AI. Drug discovery, clinical trials, manufacturing, regulatory engagement, and global partnerships now rely on cloud platforms, collaborative research ecosystems, automation workflows, and AI-driven analytics. While this transformation accelerates innovation, it also expands the attack surface dramatically.

Threat actors understand that biopharma companies hold some of the world's most valuable data including intellectual property (IP), clinical trial results, and sensitive patient information. Increasingly, they are launching identity-driven attacks, social engineering campaigns, ransomware, and insider-driven data exfiltration to steal research, disrupt production, or extort organizations.

Proofpoint helps pharmaceutical manufacturers, biotechnology firms, contract research organizations (CROs), and life sciences innovators protect their researchers, executives, partners, AI agents, and data.

Our integrated human and agent-centric cybersecurity platform reduces breach risk, safeguards intellectual property and regulated data, and enables secure collaboration across the global life sciences ecosystem.

Hurting the healers

Cyberattacks on biopharma companies can have many harmful effects, including:

- Loss of competitive advantage and research investment
- Regulatory fines (HIPAA, GDPR, FDA, EMA, and other global mandates)
- Clinical trial disruption or delays in drug approval
- Manufacturing downtime
- Reputational damage and shareholder impact

This solution set is part of Proofpoint's integrated human-centric security platform, securing people and data in the agentic workspace.

Cybersecurity challenges

As life sciences firms modernize their operations and adopt AI-enabled research environments, they face several escalating risks.

Protecting intellectual property across distributed research ecosystems

Research data moves constantly between internal teams, academic institutions, CROs, regulators, and global partners. Sensitive IP now resides in cloud repositories, collaboration platforms, data lakes, and AI pipelines. Without visibility into who or what is accessing that data, exposure risk increases significantly.

Securing clinical trial and patient data

Clinical research requires the collection and analysis of protected health information (PHI) and personally identifiable information (PII). Data breaches can trigger regulatory penalties and undermine trust with research participants and oversight bodies. Healthcare privacy regulations intersect with global data residency and research compliance obligations, creating complex governance requirements.

Stopping impersonation and account takeover attacks

Attackers frequently impersonate executives, researchers, vendors, and regulators to:

- Divert financial transactions
- Steal research data
- Inject malicious files into supply chains
- Compromise trusted communications

Shared mailboxes, service accounts, and automation workflows are particularly attractive targets.

Managing insider and third-party risk

The life sciences ecosystem includes employees, contractors, researchers, lab technicians, external collaborators, and third-party manufacturers. High turnover, joint ventures, and cross-border collaboration increase the risk of accidental or malicious data exposure.

Securing AI-enabled research and automation

AI-driven drug discovery and automated analytics pipelines introduce non-human identities, APIs, and agents that operate at scale. Traditional perimeter controls cannot distinguish between legitimate research activity and compromised or abusive access.

A human and agent-centric approach to life sciences security

Life sciences innovation now depends on both humans and digital agents. Researchers, scientists, regulatory teams, and executives initiate innovation. But many actions are executed by:

- Shared mailboxes and service accounts
- Cloud identities and APIs
- AI-driven research workflows
- Automated analytics pipelines
- Manufacturing and laboratory systems

Modern attacks do not target infrastructure alone. They exploit trusted humans and trusted agents.

Traditional perimeter-based security tools cannot detect when compromised credentials, malicious insiders, or abused automation are being used to exfiltrate IP.

Proofpoint secures this environment by correlating identity, behavior, and data access across people and agents. This closes the blind spots that attackers actively exploit and protects the full research and innovation lifecycle.

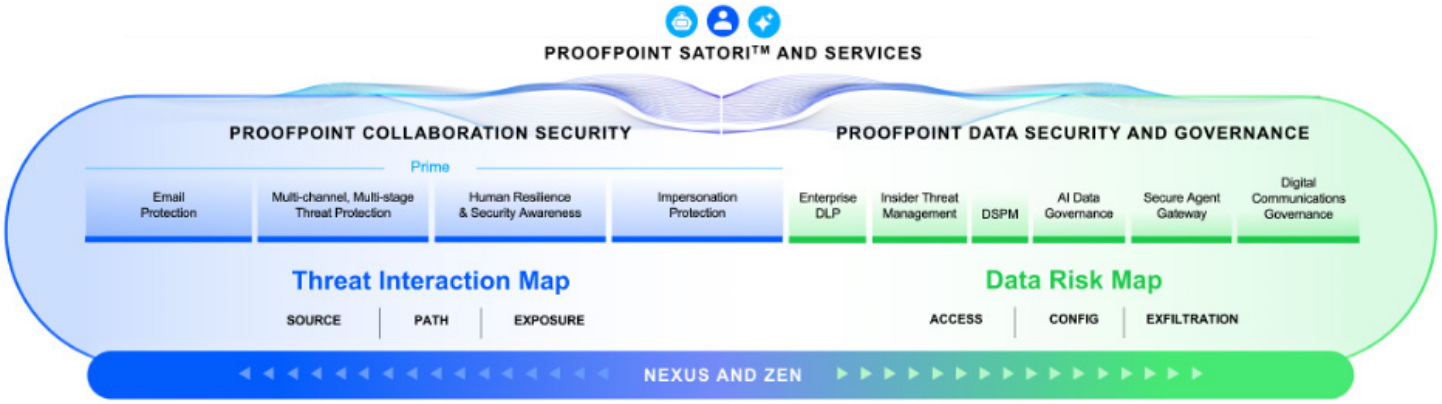


Figure 1. Proofpoint solutions secure the full ecosystem of people, AI agents, and data.

Products

- Proofpoint Collaboration Security Prime
- Proofpoint Secure Email Relay
- Proofpoint Data Loss Protection (DLP)
- Proofpoint Adaptive Email DLP
- Proofpoint Data Security Posture Management (DSPM)
- Proofpoint Satori
- Proofpoint Account Takeover Protection
- Proofpoint Insider Threat Management
- Proofpoint Communications Governance
- Proofpoint ZenGuide

How Proofpoint can help

Trusted by 67% of Fortune 500 healthcare companies, Proofpoint delivers an integrated platform that secures humans, agents, and data together.

Protect against ransomware, phishing, and advanced threats

Proofpoint Collaboration Security Prime provides end-to-end protection across email, collaboration platforms, cloud applications, web channels, and social platforms.

Powered by Proofpoint Nexus®, it uses advanced AI, behavioral analysis, and threat intelligence to:

- Stop phishing and business email compromise (BEC)
- Block ransomware delivery
- Prevent credential harvesting
- Detect supplier and regulator impersonation
- Protect executives and highly targeted researchers

It defends across the full attack lifecycle—from pre-delivery to time-of-click and post-delivery response.

Secure critical research and system-generated communications

Biopharma companies rely heavily on automated and application-generated communications sent from clinical, research, or business applications.

Proofpoint Secure Email Relay enables secure, authenticated, high-volume application-generated email delivery. It:

- Enables DMARC-compliant delivery from research and enterprise platforms
- Protects system-generated email from spoofing and lookalike domain abuse
- Reduces risk from compromised or misconfigured application accounts
- Extends agent-centric security to non-human senders

Protect intellectual property and sensitive data

Proofpoint Data Loss Prevention (DLP) solutions prevent accidental and malicious data loss across email, endpoints, and cloud services.

Proofpoint Adaptive Email DLP uses behavioral AI to detect abnormal sharing patterns and prevent misdirected research data.

Proofpoint Data Security Posture Management (DSPM) identifies:

- Where sensitive IP and clinical data reside
- Which humans and agents can access it
- Where excessive or risky permissions exist

This enables organizations to reduce exposure and securely adopt AI innovation.

Proofpoint Satori™ extends DSPM with real-time data access governance across cloud data stores, analytics platforms, and AI pipelines.

With Satori, pharmaceutical organizations can:
- Discover and classify sensitive research and patient data
- Enforce least-privilege access across researchers and AI agents
- Detect anomalous data access in real time
- Apply policy-based controls to protect IP while enabling collaboration

Detect identity compromise and insider threats

Proofpoint Account Takeover Protection and **Insider Threat Management** detect suspicious activity across both human and non-human identities. They identify:
- Credential compromise
- Privilege escalation
- Lateral movement
- Data exfiltration attempts

By correlating identity, behavior, and data movement, Proofpoint enables earlier detection and faster response—before research or manufacturing operations are disrupted.

Maintain compliance and audit readiness

Life sciences organizations operate in heavily regulated environments.

Proofpoint Digital Communications Governance solutions help:
- Capture and retain regulated communications
- Support e-discovery and investigations
- Meet global regulatory requirements
- Maintain defensible audit trails

This ensures compliance without slowing innovation.

Reduce risk through behavior change

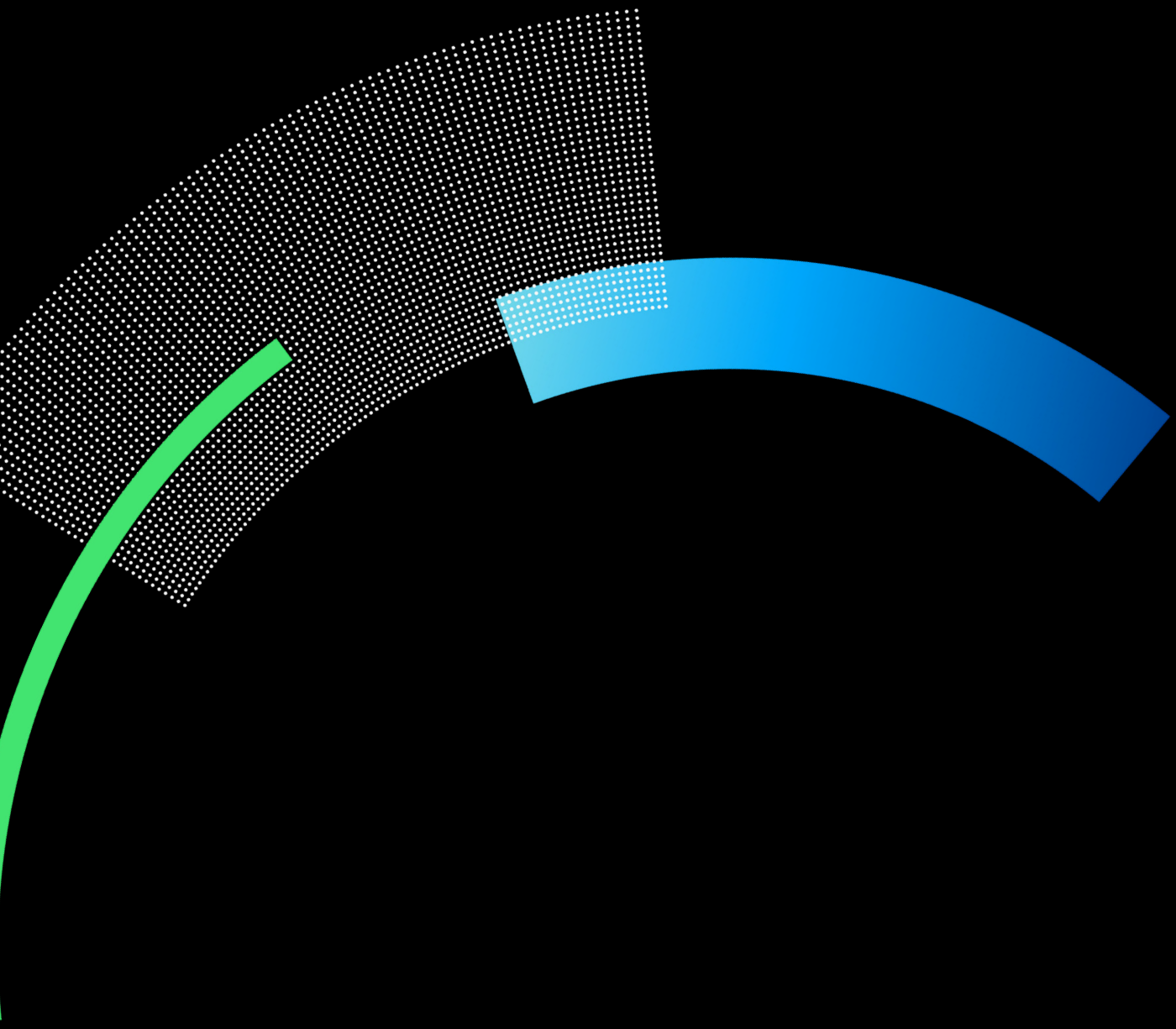
Proofpoint ZenGuide™ delivers role-based, risk-driven security awareness training that's tailored to researchers, executives, regulatory teams, and manufacturing personnel. It reinforces secure behavior using real-world pharmaceutical threat scenarios—without disrupting critical research workflows.

Conclusion

Proofpoint has always protected people. Now our human and agent-centric security platform extends that protection across researchers, executives, collaborators, AI agents, and automation workflows.

With Proofpoint, life sciences organizations can:
- Reduce breach risk
- Protect intellectual property and clinical data
- Maintain regulatory compliance
- Enable secure global collaboration
- Accelerate innovation with confidence

In a world where innovation is digital and threats are identity-driven, Proofpoint delivers the security foundation that life sciences organizations need to protect discovery, safeguard patients, and preserve their competitive advantage.



proofpoint.

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com.

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM →