Proofpoint Digital Communications Governance

A smarter way to govern communications amid digital sprawl

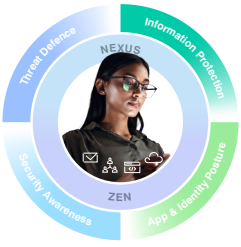
Products

- Proofpoint Capture
- Proofpoint Patrol
- Proofpoint Track
- Proofpoint Archive
- Proofpoint Discover
- Proofpoint Supervision
- Proofpoint Automate

Key Benefits

- Intelligently detect misconduct in seconds across an array of popular digital communications platforms
- Significantly reduce review time in investigations
- Deploy in private cloud or native public cloud for greater flexibility
- Manage user data in a unified, compliant way
- Accelerate data migration with robust, high-speed data ingestion and analysis to save time and costs
- Stay ahead of all compliance mandates and corporate policies

This solution set is part of Proofpoint's integrated human-centric security platform, mitigating the four key areas of people-based risks.



The virtual-first, nomadic economy has brought a sharp rise in the use of mobile and instant messaging tools as well as cloud collaboration platforms. Today's workers rely on these tools to interact and get things done on the go. Now, more than ever, they are building relationships and interacting on established platforms, such as Microsoft Teams, Slack and Zoom, as well as hundreds of newer ones that continue to crop up.

Microsoft Teams, for example, has reached 320 million monthly active users.[1] Slack users reportedly send 1.5 billion messages on the service each week.[2] In this age of digital communications sprawl, it's not surprising that about 41% of recently surveyed data leaders struggle with more than a thousand data sources. More than a third of these leaders want to improve data privacy and security and automate their data management and governance.[3]

Companies are now exposed to the highest levels of risks and threats across their digital communications stacks. They also face problems with communications sprawl. For IT, compliance, legal and security teams, that means they must focus on protecting their most important asset—their people.

Proofpoint can help. We provide a digital communications governance platform based on artificial intelligence (AI) that helps you unify, manage, store, investigate and supervise a vast array of digital communications. With Proofpoint Digital Communications Governance, you can build the corporate and regulatory compliance protection you need.

1 Microsoft. *Microsoft Fiscal Year 2024 First Quarter Earnings Conference Call*. October 2023.
2 David Curry (Business of Apps). 'Slack Revenue and Usage Statistics (2024)'. January 2024.
3 CDO Magazine Bureau. *Why CDOs Need AI-Powered Data Management to Accelerate AI Readiness in 2024*. March 2024.

People matter most in the shift to virtual first

Digital transformation is no longer an emerging paradigm shift. It's already here. It's all about your people, how they communicate and the tools that they use. Your employees use at least six ways to communicate each day. The move to working from home has seen the adoption of more and more digital platforms for workers to connect and interact.

Internal communication and project collaboration now happen online. Clients and prospects also expect to engage with your teams on social media. You must be able to capture, manage, supervise and retain this content. This is especially important if your company is regulated or litigious or has corporate policies that need extra visibility.

For regulatory and legal reasons, you must also be able to search retained content during litigation and audits. If your company has limited resources and legacy technologies that can't keep up with the modern workplace, your people might not be as effective at their jobs as they should be.

Proofpoint offers a compelling digital communications governance portfolio that can help you build and maintain an efficient security and compliance strategy. Our approach centres on protecting people and defending data. For highly litigious or highly regulated organisations in particular, the strategy has the following steps:

1. Capturing communications
2. Strategically managing the communications
3. Retaining communications in full fidelity and getting proof of record
4. Intelligently analysing, supervising and surveilling communications

Reliable communications capture across diverse channels

To understand what's happening in your organisation, you must be able to capture and manage non-persistent communications content in real time. You may also need to deliver this content downstream destination, such as an archive or supervision system.

You might have a solution for email. But how do you handle other content sources? Many firms use IT resources to build connections between content sources, such as Microsoft Teams or Slack, and their downstream services.

But these types of custom connections are not ideal. They often fail to capture key information and require constant in-house resources to maintain. What's more, they often format information differently from source to source. This makes it hard for your team to follow the contexts of all conversations that are happening at the same time.

Proofpoint Capture

Proofpoint Capture securely collects content from a wide range of new and popular communication sources. It can also help to deliver this content to your downstream services. It captures content with full fidelity and context. This makes it easy for your teams to find, manage and review the information they need. Capture unifies all content in a single platform. It also monitors content sources for updates and ensures that your connections are always up to date.

Communications management and control

In industries such as financial services and other, highly litigious ones, you must block or remediate communications that break compliance regulations. Doing so can protect your people and company from fines and legal challenges. If your firm is growing or is distributed, intelligence-driven technologies can also help you protect your people.

With human analysis and random sampling alone, you're likely to miss the issues that need most attention. And you will spend valuable resources reviewing those that are lower risk.

A better approach is to strategically manage communications and data. This lets you focus on pinpointing real risks. It can also help you act fast, especially on social media and other public channels. Quickly remediating compliance violations is critical. You must deal with these before they go viral and get your company unwanted attention.

Proofpoint Patrol

Proofpoint Patrol helps you meet rules for social media monitoring, control and remediation. Patrol gives you a complete, real-time view of the social presence of your employees and your brand. It uses machine learning and natural language processing to accurately classify content on monitored accounts. When it detects a compliance violation from your employee or corporate accounts, it notifies you before it becomes a problem. You can even set it to remove problematic content.

Retain communications in full fidelity

You need to retain modern communications in a secure, accessible and searchable archive. You must also be able to get proof of record. Legacy on-premises solutions struggle to keep up with cloud-based communications. Their search speeds tend to be very slow, often without expected service-level agreements. This can make it a challenge to quickly respond to audit or e-discovery requests. What's more, in case of an audit, you need to ensure that your records are complete and be able to present proof.

Proofpoint Track

Proofpoint Track helps to ensure your content is transported and retained in an immutable data store or archive for compliant record-keeping and investigation. It has a built-in feedback loop to confirm that the archive successfully processed each captured message from your content sources. If the process was not successful, it resends the data. You can also use Track to filter content and route it to multiple destinations.

Proofpoint Archive

Proofpoint Archive is an intelligent, cloud-native archiving solution that helps you meet your long-term business and regulatory information-retention needs. It supports storing email as well as content from digital communication platforms, such as instant messaging, collaboration and social media. Archive provides high-performance search, litigation hold and export. These features address all of your essential e-discovery needs.

FedRAMP authorisation

The Federal Risk and Authorization Management Program (FedRAMP) standardises security requirements for the adoption and use of cloud services by the US federal government. Federal agencies rely on FedRAMP to help ensure that vendor cloud services properly secure and protect federal information. Proofpoint Archive is authorised for the FedRAMP Moderate security impact level.

PCI DSS compliance

At a fundamental level, the Payment Card Industry Data Security Standard (PCI DSS) provides baseline requirements for protecting payment account data. If you store payment account data long term, you need a PCI DSS-compliant archive. Proofpoint Archive has PCI DSS compliance. For further PCI DSS validation, you can request our Attestation of Compliance (AoC) and Responsibility Matrix.

Reduce investigation times from days to seconds

Litigious companies in healthcare, pharmaceuticals, retail and other business-to-consumer industries struggle with e-discovery and investigations. This is due to a lack of timely insights to drive effective decisions. Companies face high fines and other negative outcomes if they cannot promptly produce relevant evidence during litigation.

Proofpoint Discover

Proofpoint Discover complements Proofpoint Archive, which offers financially backed service-level agreements for both archive search performance and archive system availability. Discover has advanced features that help streamline your e-discovery workflow and reduce related costs.

With case-management features, your teams can collaborate and track case progress. Discover orchestrates your response to e-discovery requests and internal investigations. Intuitive and advanced visualisation tools help you easily gain insights from search results.

Prevent large fines from non-compliance

Many regulatory mandates require companies to supervise and surveille employees in specific industries and functions. For financial services firms in North America, FINRA 3110, SEC 206(7), IIROC NI 31-103 and CFTC are some of the relevant rules. In Europe, regulations include FCA in the United Kingdom and ESMA and MiF ID II in the European Union. Non-compliance can result in significant fines and other penalties.

Proofpoint Supervision

Proofpoint Supervision also complements Proofpoint Archive. It helps you monitor and review digital communications and email for corporate and regulatory compliance. With its Compliance Risk Dashboard, you get an intelligent approach to identifying major compliance risks and violation trends over time. You also get selective drill-downs for deeper insights. You can use advanced filtering, sampling and detection to reduce noise in your results. This helps you understand why your policies identify content as potentially risky.

Proofpoint Automate

Proofpoint Automate is built on our machine-learning infrastructure. It provides out-of-the-box detection models to find risks of market abuse, employee misconduct and false information sharing. The models have been trained on countless reviewer decisions to eliminate low-value or nonrelevant content. Automate can help reduce false positives by up to 84% compared with legacy systems. It helps you streamline supervision processes and save money.

For more information, visit www.proofpoint.com/us/products/digital-communications-governance.

Learn more at proofpoint.com