

# People-Centric Compliance

## Satisfy Record-Keeping, Supervision and E-Discovery Requirements in the Digital Workplace

### PRODUCTS

- Proofpoint Content Capture
- Proofpoint Content Patrol
- Proofpoint Compliance Gateway
- Proofpoint Enterprise Archive
- Proofpoint E-Discovery Analytics
- Proofpoint Intelligent Supervision
- Proofpoint NexusAI for Compliance

### KEY BENEFITS

- Detect misconduct in seconds across an array of popular e-communication platforms
- Significantly reduce review time in investigations
- Manage user data in a unified, compliant way
- Stay ahead of all compliance mandates and corporate policies
- Protect your people end to end

The new virtual-first economy has turned to hundreds of new instant messaging and cloud collaboration platforms to interact and get things done. Eighty-four percent of the American workforce began working remotely in 2020. That means 84% of the workforce are now building relationships and interacting on platforms such as Microsoft Teams, Slack and Zoom.

Organizations are now being exposed to the highest levels of unmanageable risks and threats. For IT, compliance, legal and security teams, that means they must focus on protecting their most important asset—their people. Organizations can trust Proofpoint to help mitigate corporate and regulatory risks by leveraging an end-to-end people-centric compliance solution. We unify, manage, store, investigate and supervise communications.

### PEOPLE MATTER MOST IN THE SHIFT TO VIRTUAL-FIRST

Digital transformation is not a paradigm shift anymore. It's already here—and it's all about your people. Your employees are using at least six to 10 ways to communicate in a single day. The work-from-home shift has only further accelerated the use of more digital platforms to connect and interact. Internal communication and project collaboration happen online. Clients and prospects expect to engage with your teams on social media. It's critical that you capture, manage, supervise and retain this content accordingly. It's especially important to do so if your company is regulated, litigious or simply has corporate policies requiring more visibility. For regulatory and legal reasons, you also need the ability to search retained content during litigation and audits. If you're like many organizations, limited resources and legacy technologies make it difficult for you to be effective at getting your job done.

Here are a few steps to follow to have efficient people-centric compliance:

## STEP 1: CAPTURE COMMUNICATIONS—EMAIL AND BEYOND

You need to capture and manage real-time, non-persistent communications content to understand what's going on in your organization. Also, you may need to deliver it to your downstream destinations, such as an archive or supervision system. You probably have a solution for email.

But how do you handle other content sources? Many firms have leveraged IT resources to build connections between new content sources, such as Microsoft Teams or Slack, and their downstream services. But these one-off connections are less than ideal. They often fail to capture key information while requiring constant in-house resources to maintain upkeep. What's more, they often format information differently from source to source. This makes it hard for your team to follow the context of all forms of conversation happening at the same time.

### Content Capture

Content Capture securely captures content from a wide variety of new, popular communication sources and can help deliver it to your downstream services. It captures content with full fidelity and conversational context, making it easier for your teams to find, manage and review. It unifies all content in a single platform for you. And it monitors content sources for updates and ensure your connections are always up to date.

In 2020 alone, Microsoft Teams reached 115 million daily users, Zoom reached 300 million meeting participants<sup>1</sup> and Slack had 12 million daily active users.<sup>2</sup>

## STEP 2: STRATEGICALLY MANAGE AND CONTROL COMMUNICATIONS

In some industries, like financial services or others that are highly litigious, you must prohibit or remediate communications that violate compliance regulations and other laws. Doing so can protect your people and organization from fines and legal challenges. If your firm is growing or simply distributed, intelligence-driven technologies can help you protect your people.

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

<sup>1</sup> Owen Hughes (*TechRepublic*). "Watch out Zoom: Microsoft Teams now has more than 115 million daily users." October 2020.

<sup>2</sup> David Curry (*Business of Apps*). "Slack Revenue and Usage Statistics (2020)." March 2021.

A better approach is strategically managing communications and corporate data. This approach allows you to focus your resources on pinpointing real risks. It can also help you act fast, especially on social media and other public channels. Remediating compliance violations quickly is critical—before they "go viral" and garner unwanted attention.

### Content Patrol

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

## STEP 3: RETAIN MODERN COMMUNICATIONS IN FULL FIDELITY—AND GET PROOF OF RECORD

You need to retain communications in a secure, accessible and searchable archive. Legacy on-premises solutions struggle to keep up with cloud-based communications. And search speeds are often very slow. This can make it a challenge to respond to audit or e-discovery requests in a timely manner. What's more, you need to ensure your records are complete and present proof in case of an audit.

### Compliance Gateway

Compliance Gateway ensures that your content is properly transported and retained when it needs to reside in an immutable data store or archive. It has a built-in feedback loop to confirm that the archive successfully processed each message from your content sources captured. If not, it resends the data. You can also use the Compliance Gateway to filter and route content to multiple destinations.

### Enterprise Archive

Enterprise Archive is a modern, cloud-native archiving solution that helps customers meet long-term business and regulatory information-retention needs. It supports email and a wide variety of digital communication platforms, such as instant messaging and collaboration and social media. Enterprise Archive provides built-in high-performance search, litigation hold and export to address all of your basic e-discovery needs.

## STEP 4: ANALYZE, SUPERVISE AND SURVEILLE INTELLIGENTLY

A variety of regulatory mandates require organizations to supervise and surveil employees within specific industries and functions. From a supervisory perspective, FINRA 3110, SEC 206(7), IIROC NI 31-103 and CFTC are just a few of the relevant rules.

### E-Discovery Analytics

E-Discovery Analytics works with Enterprise Archive, offering advanced features to help streamline your e-discovery workflow and reduce related costs. With case management, your teams can collaborate and track case progress seamlessly. It easily orchestrates your response to e-discovery requests and internal investigations. Intuitive and advanced visualization tools enable you to easily uncover insights from search results at any time.

### Intelligent Supervision

Intelligent Supervision also works with Enterprise Archive. It helps customers monitor and review digital communications and email to ensure corporate and regulatory compliance. With the Compliance Risk Dashboard, you can take advantage of a people-centric approach to identify major compliance risks and violation trends over time. And you also get selective drill down for deeper insights. You can use advanced filtering, sampling and detection to reduce the “noise” you don’t want.

### NexusAI for Compliance

NexusAI for Compliance is built on our machine learning infrastructure. It provides an out-of-the-box detection model to find risks of market abuse, employee misconduct and false information sharing. These models have been trained by countless reviewer decisions to eliminate low-value or non-relevant content. It helps customers streamline supervision processes and save money.

## LEARN MORE

For more information, visit [proofpoint.com/us/product-family/information-archive-and-compliance](https://proofpoint.com/us/product-family/information-archive-and-compliance).

### ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) 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 more than half of the Fortune 1000, 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](https://www.proofpoint.com).

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. [Proofpoint.com](https://www.proofpoint.com)