Forcepoint

Solution Brief

# Comprehensive SaaS Security for the Modern Enterprise

## Challenge

- Organizations struggle to implement consistent data protection across SaaS, cloud, and devices
- The growing complexity of global data regulations increases the difficulty of maintaining compliance and avoiding penalties
- Siloed tools and remote work practices contribute to the increasing complexity of workflows and difficulty of tracking sensitive data throughout the organization

## Solution

- Forcepoint offers a unified platform for SaaS data security powered by native AI
- Extend existing DLP policies to secure SaaS apps with just a few clicks
- Automate detection of data risk and facilitate rapid remediation and permissions management

## Outcome

- Enjoy a stronger data security posture allowing you to exercise effective governance and maintain regulatory compliance
- Minimize the risk of costly data breaches and streamline security workflows
- Achieve secure, flexible SaaS use across all devices to protect workers and data wherever they reside

## The SaaS Reality

Software-as-a-Service (SaaS) applications are now the core of enterprise productivity and collaboration. Yet the rapid pace of SaaS adoption, combined with remote work, Bring Your Own Device (BYOD) and generative AI, has created a sprawling and complex data environment. Sensitive information moves constantly between SaaS platforms, personal devices, cloud storage and third-party tools, often without consistent oversight.

To meet today's challenges, organizations need more than just visibility. They need **unified governance and the ability to extend data protection policies seamlessly into every SaaS application**, ensuring the same level of control in the cloud as in on-prem and endpoint environments.

## The SaaS Security Challenge

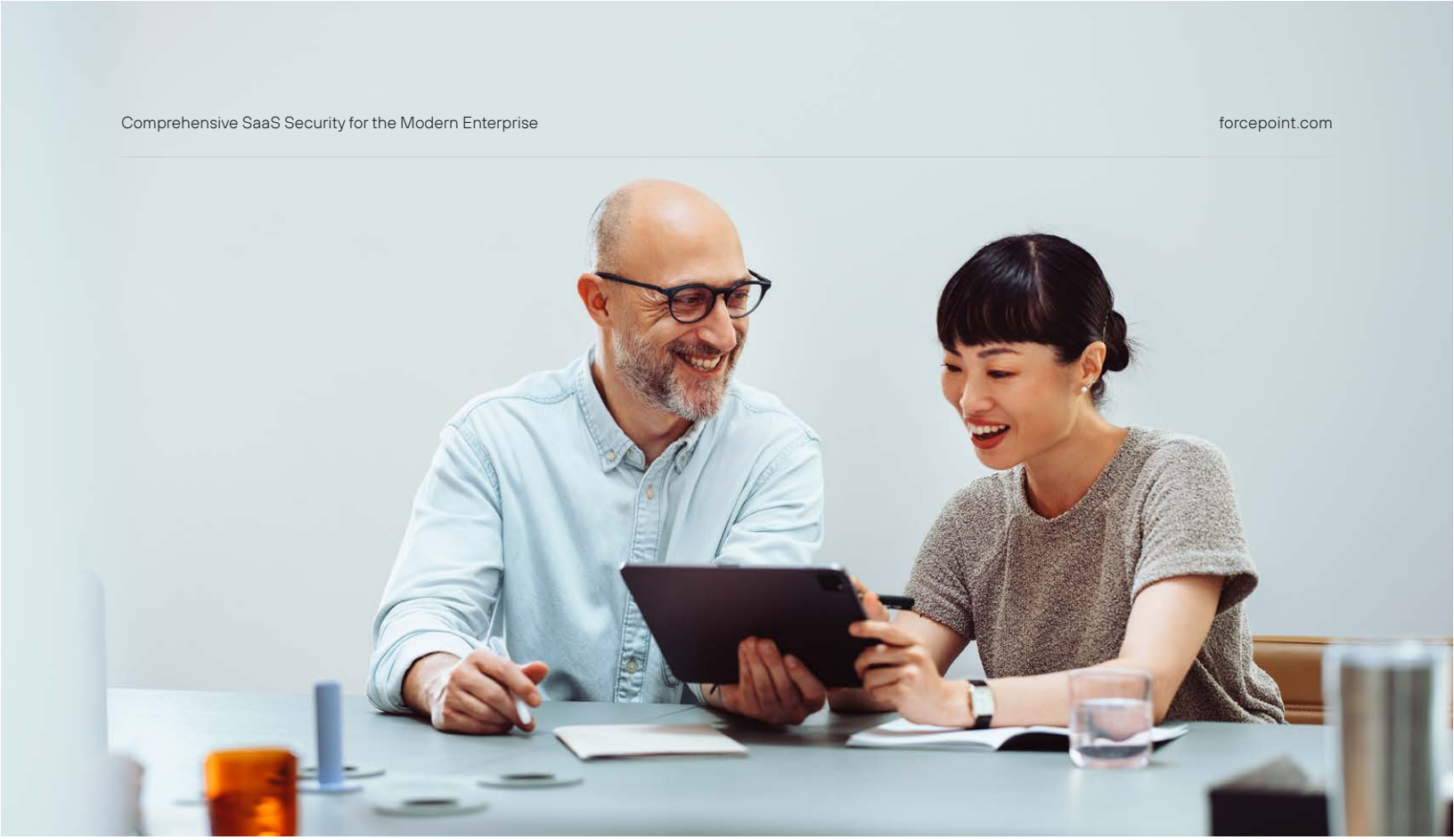
Organizations face mounting pressure to:

- → **Protect sensitive data consistently** across SaaS, cloud, endpoints and web
- → **Maintain compliance** with global and industry regulations and standards such as GDPR, HIPAA and PCI DSS
- → **Secure remote work and BYOD** without hindering productivity
- → **Reduce operational complexity** caused by siloed tools and policies

Without a unified approach to policy enforcement, including the extension of Data Loss Prevention policies into SaaS, security teams risk inconsistent protection, compliance gaps and increased exposure to data breaches.

## The Forcepoint Solution for Securing SaaS

Forcepoint addresses this challenge with a unified platform that delivers comprehensive visibility and control to secure sensitive data across SaaS, endpoints, web and email. Many solutions on the market have gaps and redundancies, lack the ability to automatically and accurately classify and understand data, only cover a few channels or have immature protection on critical channels such as endpoints. Forcepoint unites high-speed discovery, AI-native classification, prioritization and remediation with the industry's leading Data Loss Prevention (DLP) capabilities from the endpoint to the cloud and everywhere in between.



## Key Use Cases for Comprehensive SaaS Security

### 1. Extend DLP Policies to SaaS

Apply the same proven data protection rules used for email, web and endpoints directly to SaaS applications.

- → Enforce consistent classification and protection across all channels
- → Reduce policy duplication and eliminate configuration drift

### 2. Consistent Data Discovery and Classification

Identify and classify both structured and unstructured data within SaaS platforms using a unified taxonomy.

- → Enable accurate, multilingual classification across global operations
- → Ensure policy enforcement aligns with data sensitivity and compliance requirements

### 3. Automated Data Exposure Remediation

Continuously detect risky sharing or overexposure in SaaS files.

- → Identify public links, unauthorized access and excessive permissions
- → Automatically revoke unsafe access to reduce the window of risk

### 4. Compliance Readiness and Audit Support

Simplify compliance across hybrid environments.

- → Align policy enforcement with global regulations using pre-defined templates
- → Maintain centralized logs of all user activity, sharing events and policy actions for audits

### 5. Secure BYOD and Remote Access

Protect SaaS data without requiring agents or proxies.

- → Apply policies within SaaS apps for both managed and unmanaged devices
- → Enable frictionless access while maintaining consistent data protection

## Core Principles of Comprehensive SaaS Security

- → **Unified Policy Enforcement:** One set of DLP policies applied across SaaS, endpoints, web and cloud
- → **Continuous Visibility:** Real-time monitoring of data activity in SaaS environments
- → **Risk-Adaptive Protection:** Dynamic controls based on data sensitivity, user role and context
- → **Consistent User Experience:** Security that protects without slowing workflows
- → **Audit-Ready Operations:** Centralized evidence and reporting across all channels

## Business Benefits

- → **Accelerate SaaS adoption** without sacrificing security or compliance
- → **Strengthen governance** by extending DLP policies into cloud and SaaS environments
- → **Reduce complexity** by eliminating policy silos and redundant tools
- → **Lower breach risk** through faster detection, remediation, and prevention
- → **Enable innovation** by allowing teams to use SaaS tools securely from any device

**forcepoint.com/contact**