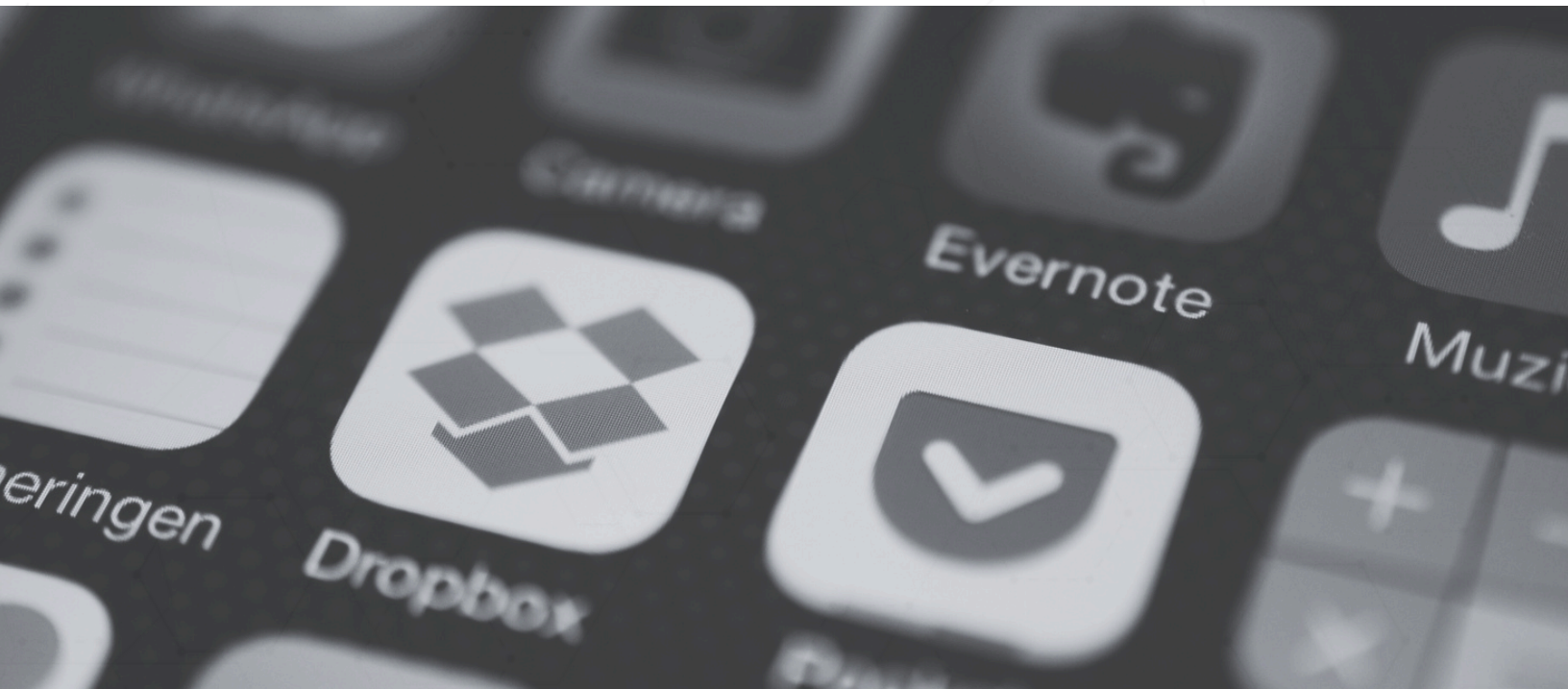




SaaS Security Essentials: Protecting Your Apps Made Simple

A quick guide to securing your SaaS stack with SSO, MFA, and zero trust principles



888-286-4816

NextPerimeter.com

YOU CAN'T PROTECT THE THINGS THAT YOU CAN'T SEE

Modern businesses rely on SaaS apps like Microsoft 365, Dropbox, and Salesforce to run efficiently. But without the right safeguards, these tools can leave your data exposed to breaches and misconfigurations - which is why [SaaS Security](#) should be an essential part of your IT and cybersecurity strategy.

WHY SAAS SECURITY IS ESSENTIAL

Did You Know?

Ninety-nine percent of SaaS security breaches result from misconfigurations or compromised accounts. Additionally, Shadow IT introduces vulnerabilities by allowing unapproved and unmonitored applications to enter your environment.

What's at Risk?

SaaS applications often store critical business information, making them a prime target for cyber threats. Misconfigured apps can also lead to compliance violations and substantial fines. Beyond regulatory risks, a single data breach can severely damage your brand's reputation, eroding customer trust and business credibility.

The Solution

Implementing [Single Sign-On](#) (SSO), [Multi-Factor Authentication](#) (MFA), and [Zero Trust](#) principles provides a foundational approach to securing your SaaS apps and protecting your business.

3 STEPS TO SAAS SECURITY

Step 1: Enable Single Sign-On (SSO)

What It Does

SSO centralizes user authentication across all SaaS applications, reducing the number of passwords employees need to manage while giving IT full visibility into SaaS usage.

Benefits

By simplifying access, SSO enhances both security and productivity. Employees face fewer login hassles, while IT teams gain stronger, centralized control over user permissions and application access.

Step 2: Add Multi-Factor Authentication (MFA)

What It Does

MFA adds a critical layer of security by requiring a second authentication factor, such as a mobile app code or biometric scan, making it significantly harder for attackers to gain unauthorized access.

Benefits

MFA prevents account takeovers and helps businesses meet compliance standards required in industries like healthcare and finance, reducing the risk of credential-based breaches.

Step 3: Apply Zero Trust Principles

What It Does

Zero Trust security models verify every user, device, and login attempt before granting access. This approach ensures that only trusted devices and locations can connect to business-critical SaaS applications.

Benefits

Zero Trust delivers dynamic, adaptive security tailored to real-time risk factors, offering greater peace of mind for IT teams and business leaders alike.

HOW IT WORKS WITH NEXT PERIMETER

The Next Perimeter Advantage

Our platform seamlessly integrates with your existing tools to secure SaaS applications without adding complexity.

Identity Protection

Every login is safeguarded with AI-powered monitoring and automated threat detection. Next Perimeter also enables seamless SSO and passwordless authentication for corporate-managed devices.

Device Compliance

By ensuring that only secure, managed devices can access critical applications, Next Perimeter integrates with Microsoft Intune, Google Workspace, and other enterprise platforms to enhance security.

Visibility and Reporting

Centralized dashboards provide clear insights into application usage and potential threats. Additionally, regular security reports help businesses stay proactive in addressing risks and compliance requirements.

LEARN MORE ABOUT SAAS SECURITY



Visit NextPerimeter.com to explore how *SaaS Security* can protect your business from potential breaches.

We're Here to Help



Phone

888-286-4816

Email

sales@nextperimeter.com

Website

NextPerimeter.com



About Us

Next Perimeter simplifies IT and security for growing businesses by eliminating complexity, boosting productivity, and ensuring seamless, secure experiences.

We streamline onboarding to get new hires up and running on day one, replace outdated systems with cloud-first, zero-trust solutions, and deliver unified IT and security services that protect your business while enabling smarter work.