OBSIDIAN

WHITE PAPER

# Zero Trust in a SaaS World

The importance for healthcare organizations to extend the principles of zero trust to business-critical applications

## The Principles of Zero Trust

The zero trust security framework is predicated on the foundational concept that implicit trust of users and devices in the environment increases the risk of a potential compromise. By eliminating this implicit trust and requiring strict identification and authentication throughout the network, security teams employing zero trust hope to severely limit the opportunities for any attacker looking to gain unauthorized access to sensitive data.

The earliest discussions around zero trust questioned the effectiveness of traditional perimeter security measures, asserting that an attacker who bypassed these would have unfettered access to the corporate network and suggesting instead that every request for access should be logged and verified. Since then, zero trust has evolved from network perimeter security to a more identity-centric model in response to an increasingly mobile workforce and the adoption of cloud services.

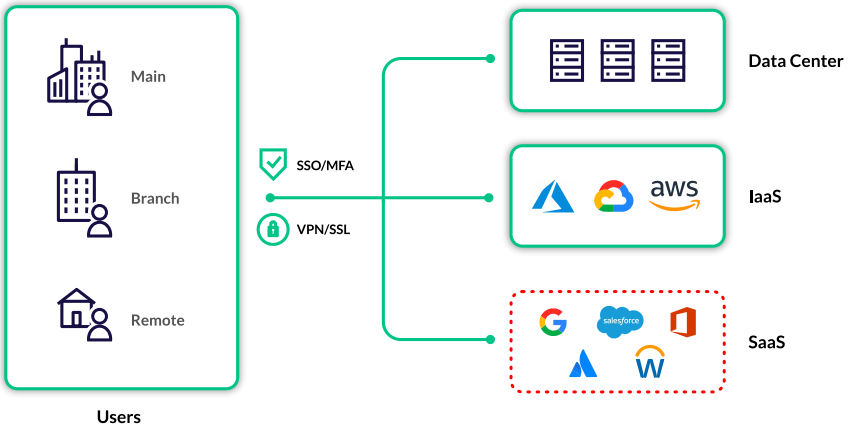
The healthcare industry has likewise undergone a transformation from on-premises network perimeters to more decentralized systems of mobile employees and contractors, internet-connected medical devices, and cloud applications. As attackers target healthcare organizations with greater frequency, many security leaders are turning to a zero trust model to better protect their environments. With applications containing more sensitive data than ever, applying this zero trust framework to SaaS can significantly minimize the risk and impact of a potential compromise—but implementing it requires a deep understanding and continuous verification of every piece of business-critical SaaS applications.

## Bringing Zero Trust to SaaS

Zero trust brings substantial security advantages to an enterprise, as avoiding implicit trust minimizes the likelihood, impact, and time to detect a breach. The zero trust model of security requires that an organization "never trust, always verify" how they connect, access, and use corporate information technology. As per the National Institute of Standards and Technology (NIST 800-207), zero trust requires the implementation of three key tenets:

- Continuous verification of access for every element
- Limiting the impact of a potential breach
- Collection of behavioral data to facilitate faster incident response

Bringing zero trust to your SaaS applications means applying these same principles when designing controls. It is not sufficient to simply rely on single sign-on (SSO) and multi-factor authentication (MFA); these solutions provide initial verification of user access, but do not verify every component of the SaaS environment. Zero trust for SaaS requires a deeper understanding of each application, not relying on the identity provider alone.




## The Interconnected SaaS Environment

Because zero trust requires continuous verification of every element, it is not sufficient to simply validate the connection between a client and the application—there are other sources of risk in the SaaS environment that require monitoring. A zero trust approach to SaaS security starts with a comprehensive understanding of the three core components of an application's architecture: the client connection, the application itself, and other services connected to the application.

### The Client Connection

Understanding the authentication, privileges, and actions of users within and across business-critical applications is absolutely necessary to define the scope of each user's risk. This data must be continuously aggregated and normalized into a single, easily understood format in order to be readily accessible for your security team. This extends the principle of "never trust, always verify" beyond identity providers and into the SaaS applications themselves.

### The Application

Enterprise SaaS applications are inherently unique and complex systems with their own structural vulnerabilities and issues specific to each user environment. Continuous monitoring of the application security posture is an important part of zero trust—this includes both application configurations and privileges granted to users. SaaS security posture management (SSPM) doesn't just mean knowing the state of controls and permissions, but also monitoring the activities associated with each one.

### The Integrations

When SaaS users and administrators integrate third-party applications into core applications to expand functionalities, automate workflows, and enable cross-platform communication, they grant persistent access and permissions to the connection. This can create a serious security risk if left unchecked. Even vetted third-party applications can be compromised, providing a backdoor into the core service. Continuous monitoring and threat detection for integrations is a critical piece of zero trust for SaaS.

## Staying Ahead of Threats

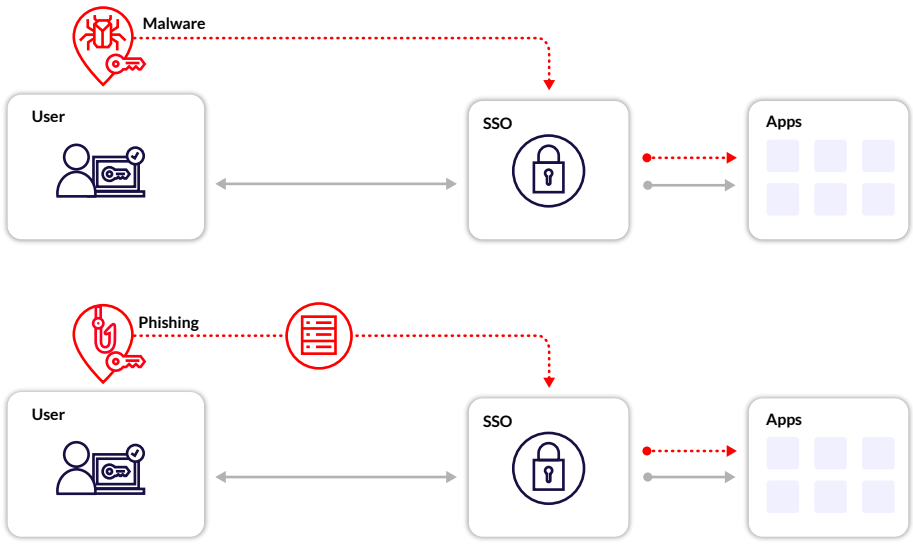
The clients, integrations, and applications in your SaaS environment all introduce some degree of risk and, if left unchecked, can become potential breach entry points. Organizations who don't continuously monitor these connections within the SaaS environment are effectively blind to threats and posture gaps within their core applications, leaving their zero trust architectures incomplete.

The challenge for healthcare organizations is especially significant as attackers look for opportunities to overwhelm security teams. The US Department of Health and Human Services (HHS) reported a 50% increase in healthcare cybersecurity breaches in the first half of 2020, disrupting healthcare organizations preoccupied with the emerging COVID-19 pandemic.

Increasingly sophisticated attackers can use a variety of techniques to bypass identity providers and gain unauthorized access to SaaS environments, including session hijacking and OAuth abuse.

### Session Hijacking

To improve the user experience, SaaS applications provide a session token stored in the browser that identifies the user and allows access without requiring a login each visit. These tokens are nearly impossible to guess, protected with SSL over the network, and encrypted when stored on the endpoint. Once a user has a token, they can revisit the application over a multi-day period without needing to reauthenticate. In the case of an identity provider (IDP) like Okta, Duo, or Microsoft Azure AD, it allows them to authenticate to their authorized applications, generating new application-specific tokens and facilitating frictionless access to all services.



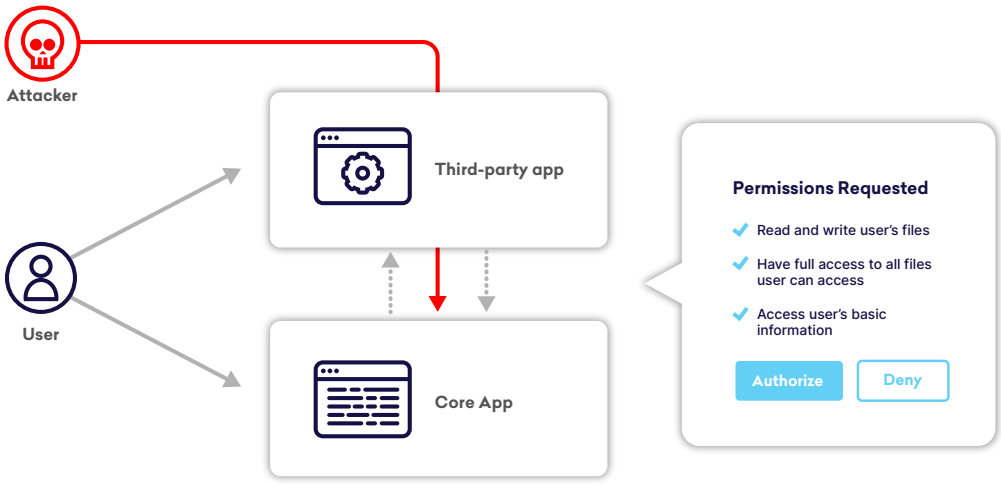
Unfortunately, the convenience provided by long-lived session tokens has created an opening for attackers to exploit. Rather than attempting to steal usernames and passwords, attackers are attempting to establish persistence in the SaaS IDP through malware or a man-in-the-middle attack. Attackers wait for a device to successfully authenticate with MFA before intercepting the session token in transit. They are then able to connect to the IDP as a fully-authenticated user, which allows attackers to connect to every application for which the user has access. This technique can give attackers up to 30 days of full access without ever authenticating.

Bypassing authentication essentially allows attackers to negate any aspect of zero trust present in an organization. This also enables them to avoid the majority of a security team's tooling which is often focused on the source and nature of a login.

A sophisticated instance of token theft can be difficult to manually identify. Security teams must be equipped with a solution that continually analyzes and models user activity to identify potentially subtle anomalies associated with session hijacking in order to facilitate rapid remediation. Ensuring that security personnel have a clear understanding of the user interaction with the identity provider and their activity within and across SaaS applications enables better incident response and reporting.

### OAuth Application Abuse

The interconnectivity of applications provides one of the greatest productivity advantages of SaaS. Users and administrators often integrate services in order to augment and expand the functionality of a core application. Application administrators commonly connect services such as Salesforce and Microsoft 365, while individual users regularly connect enterprise productivity suites like Google Workspace and Microsoft 365 to third-party tools including Grammarly, Evernote, and Asana. These connections are typically made via an OAuth grant, which simply requires a user to click a link authorizing access to the application. Once authorized, the integrations can access the SaaS environment with permissions and data access equivalent to the user.




Sophisticated attackers have adapted their techniques to exploit the benefits of OAuth. Rather than attempting to phish credentials, attackers can send requests containing links that authorize an OAuth application. This act grants attackers the same level of access as a username and password but with long-term persistence and resilience to password resets. Alternatively, attackers can compromise a third-party

application and use existing OAuth connections to access connected applications. Both scenarios avoid MFA protection, customer monitoring, and even the ability to see data being exfiltrated.

Whether a breach occurs through the addition of a malicious connection or the compromise of a trusted one, zero trust for SaaS is only possible with continuous and detailed monitoring of these interconnected services. Security teams need detailed information not only about the activity of every integration, but also on the scope of the permissions they have been granted. This helps define the blast radius of a potential compromise, identify the presence of malicious OAuth applications, ensure that vetted connections are not being abused, and ultimately limit opportunities for lateral movement throughout the SaaS environment.

## Trust Nothing, Verify Everything

The growing interconnectedness of systems within healthcare organizations enables a better, more seamless experience for care providers and greater overall productivity for a distributed workforce of employees and contractors. At the same time, it expands the potential attack surface and creates opportunities for attackers to make lateral movements into connected services after gaining initial access. With cloud services entrusted with so much sensitive business data and patient records, continuous monitoring and verification of everything within and across applications is absolutely vital.

Solutions like SSO and MFA are ubiquitous for their effectiveness in validating access and providing a smooth user experience, but these alone do not offer comprehensive verification of every component in a complex, interconnected SaaS environment. Zero trust for SaaS is predicated on a deep, consolidated understanding of your clients, applications, and integrations—and the connections between them. With this established, your security team is better equipped to identify and mitigate increasingly sophisticated threats to your environment, enabling your healthcare organization to operate smoothly and securely.

### About Obsidian Security

Obsidian Security is the first truly comprehensive threat and posture management solution built for SaaS. Our platform consolidates data across core applications to help your team optimize configurations, reduce over-privilege, and mitigate account compromises and insider threats. Getting started with Obsidian takes just a few minutes—with no agents to deploy or rules to write.