AppOmni

SOLUTION OVERVIEW

Zero Trust Posture Management (ZTPM) with AppOmni

SAAS-READY ZERO TRUST ARCHITECTURE

The Challenge

Zero Trust (ZT) is a cybersecurity paradigm that states never trust the identity of any user within or outside the network perimeter. It emphasizes the need for continuous verification of all identity and access requests to safeguard data and services. It also stresses the importance of continuously monitoring user behavior for malicious activity.

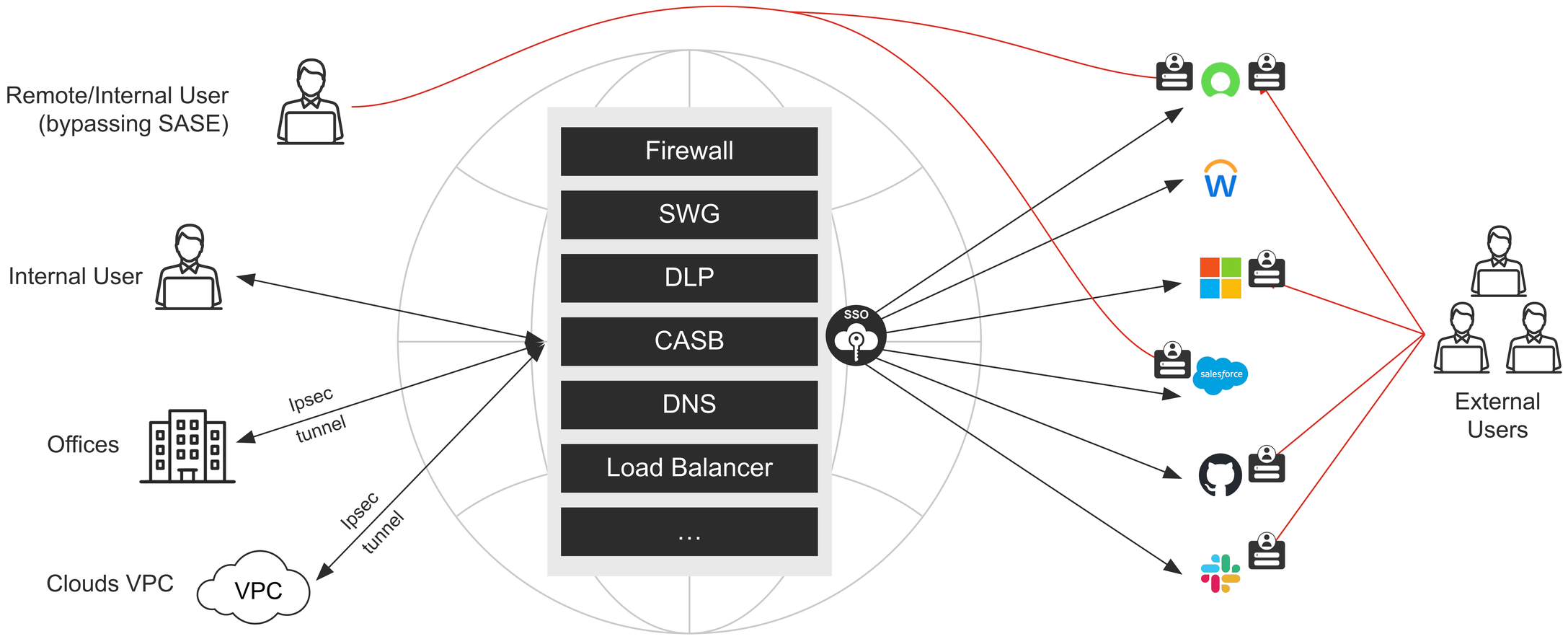
In the context of SaaS applications, traditional ZT implementations via Secure Access Service Edge (SASE) solutions fall short by not addressing SaaS app vulnerabilities such as misconfigurations, unchecked user privileges, and exposed data access.

Neither can these network-centric solutions detect direct SaaS app access for example, by guest users that have been provisioned direct SaaS app access outside of the purview of the SASE solution.

CHALLENGES

- SaaS App Misconfigurations – Uneven SSO and MFA implementation enabling threat actors to compromise SaaS apps without being detected
- Direct SaaS App Access via Side-Loaded Accounts – Out of band SaaS App access cannot be detected by SASE solutions, enabling backdoor access into SaaS Apps
- Inadequate IP Restrictions – SaaS Apps can be accessed from any IP location bypassing SASE controls

The SaaS Security Challenge



The Solution

Zero Trust Posture Management capabilities in the AppOmni Platform bridges a critical gap in network-centric Zero Trust (ZT) architectures by providing deep visibility into the configuration, security posture, and user behaviors within SaaS applications.

ZTPM addresses SaaS misconfigurations, ensures mandatory SSO and MFA configurations are enforced, provides visibility and control across the SaaS estate including all access points, which enables comprehensive SaaS security from a single pane of glass.

SaaS SECURITY BENEFITS

- Enhanced Visibility and Monitoring
- Granular Access Control and Configuration Management
- Robust Identity Access Protection
- Secure Third-party Integrations

AppOmni enables and enforces the following Zero Trust security controls:

Enhanced Visibility and Monitoring:

- Provides context and identity-aware continuous monitoring of user activities and application configurations. It identifies risks stemming from suspicious behavior or misconfigurations and ensures that applications adhere to ZT principles even as they evolve.

Granular Access Control and Configuration Management:

- ZTPM enables detailed oversight and management of user roles, including role-based access control, permissions and entitlements management, data access in complex SaaS deployments, and other key components and capabilities within SaaS platforms. It ensures that access is strictly based on the principle of least privilege and in line with a user’s roles and responsibilities.

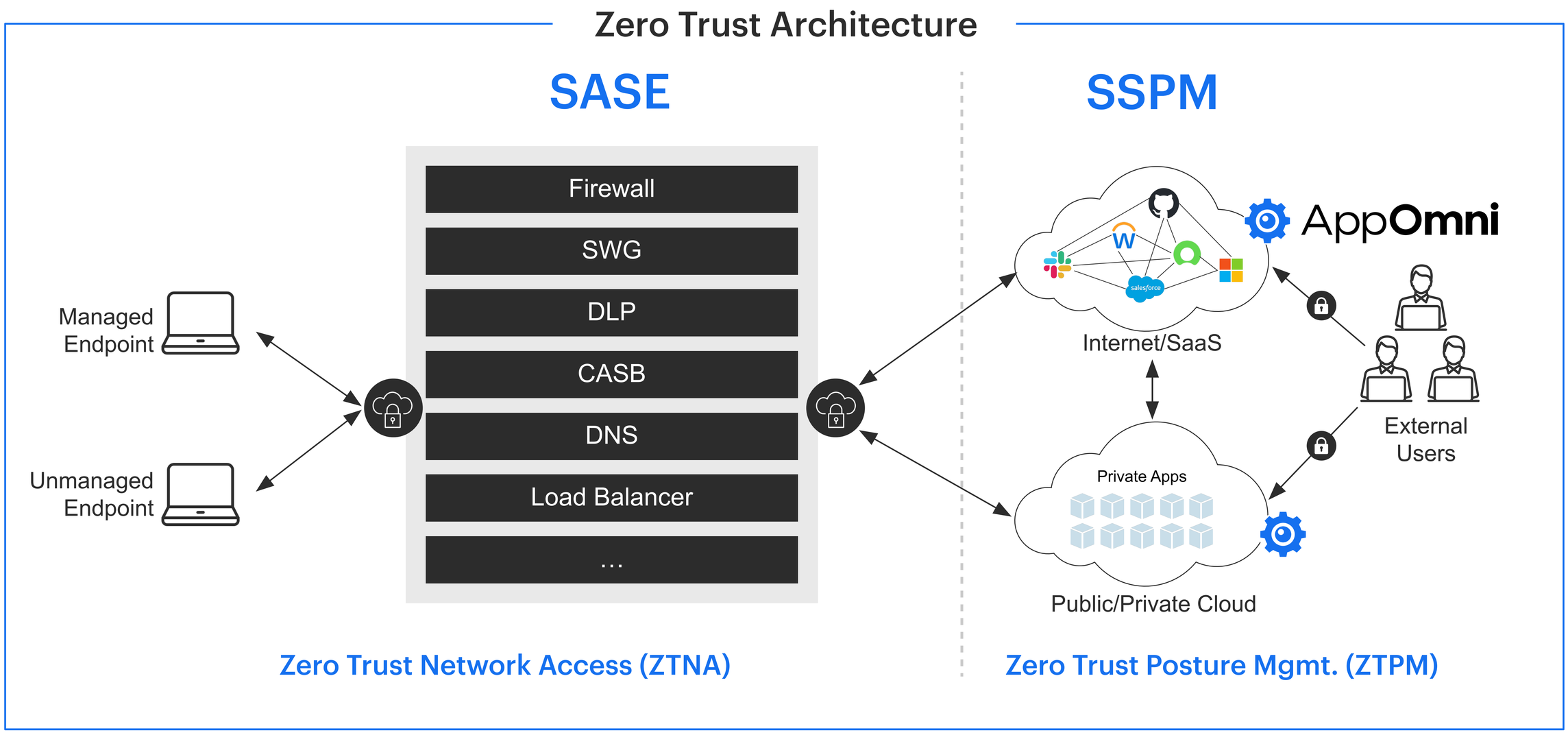
Robust Identity Access Protection:

- Leveraging deep insights into user behavior and application context, ZTPM facilitates robust and dynamic identity and access decisions. For example, it might trigger stronger authentication requirements for users capable of accessing sensitive data within an application and then tailor security measures to the specific context of each access request. These capabilities are critical for making dynamic access decisions within a Zero Trust Architecture (ZTA).

Secure Third-party Integrations:

- Applications often integrate with external services and data sources. ZTPM principles scrutinize these integrations and ensure that they don't introduce vulnerabilities or bypass ZT controls. These actions effectively extend the ZT framework to encompass cloud-to-cloud and third-party interactions.

Closed Loop Zero Trust Solution - SASE & SSPM



Key Features

End-to-End Security

- Zero Trust Posture Management (ZTPM) extends Zero Trust (ZT) through applications by providing visibility into the configuration, security posture, and user behaviors within applications, which are pivotal components of the security and data path in a ZT framework. This capability addresses the gap in ZT's goal of achieving end-to-end security by ensuring that not only the network but also the applications and data accessed through SaaS products are secured under the ZT principles.

Standardizes Least Privilege Access

- ZTPM enhances the implementation of least privilege access within applications and SaaS systems, a core requirement of a ZTA. It does so by offering deep visibility and control over enterprise SaaS resource configurations and data authorizations. This granularity in visibility and control makes the application of least privilege more meaningful and effective than traditional, coarse-grained access controls, such as group memberships, thus preventing unauthorized access to sensitive data.

Granular Access Decisions

- The goal of ZT to make access decisions as granular as possible is supported by ZTPM through its comprehensive visibility and configuration analysis capabilities within applications. ZTPM enables organizations to apply access controls and policies at the finest level of detail, thereby aligning with the ZT principle of granting access based on explicit permissions and the precise requirements of the user's role and the context of the access request.

Dynamic Policy Enforcement

- ZTPM contributes to dynamic policy enforcement by providing a ZTA with insights into a user's data access, behaviors, and permissions within applications. This information allows a ZTA to adapt access controls and security measures in real-time, based on the ongoing assessment of risk and the need for access, thus ensuring that security policies remain effective and responsive to changing conditions.

Continuous Monitoring and Feedback Loop

- By offering continuous monitoring capabilities of both users and applications, ZTPM enables a ZTA to maintain a feedback loop that informs security policy adjustments and actions. This capability allows for real-time, context-aware responses to detected security events or anomalies, such as terminating suspicious sessions, requiring step-up authentication, or implementing other remedial actions.

Extension of Zero Trust Principles

- ZTPM extends the application of Zero Trust principles to third-party and cloud-to-cloud integrations, as well as non-corporate users, thereby broadening the scope of a ZTA to encompass all entities interacting with the organization's resources, not just internal users.

Configuration Assurance

- Ensuring that applications are configured to prevent bypasses of a ZTA that would allow direct access to applications or data exposures to external entities is crucial for the integrity of ZT strategies. AppOmni's ZTPM plays a vital role in this aspect by analyzing and ensuring that applications and their configurations do not allow users to bypass security controls, such as SSO, MFA or IP restrictions, thus maintaining the effectiveness of the ZTA.

About AppOmni

AppOmni is the pioneer of SaaS Security Posture Management (SSPM) enabling customers to achieve secure productivity with their SaaS applications. With AppOmni, security teams and SaaS application owners quickly secure their mission-critical and sensitive data from attackers and insider threats. The AppOmni platform constantly scans SaaS APIs, configurations, and ingested audit logs to deliver complete data access visibility, secure identities and SaaS-to-SaaS connections, detect threats, prioritize insights, and simplify compliance reporting. The AppOmni SSPM solution provides the most robust and comprehensive ZTPM capability on the market, enhancing and closing the loop on Zero Trust.

Learn more at appomni.com