AppOmni

SOLUTION BRIEF

CLOSED LOOP ZERO TRUST ARCHITECTURE:

Cisco Secure Access and AppOmni SaaS Security Posture Management

Introduction

In the evolving landscape of cybersecurity, Zero Trust (ZT) stands out as a foundational principle that asserts no entity should be implicitly trusted, regardless of its position within or outside the network perimeter. This paradigm shift is essential in an era where organizational resources span across diverse environments, from cloud services to remote workforces.

However, realizing a complete Zero Trust architecture demands attention not just at the network and infrastructure levels, but extends deeply into the realm of SaaS applications and platforms. In fact, SaaS stands out as a critical yet neglected component of this new distributed computing reality. To achieve an end-to-end architecture, Zero Trust principles must be applied and enforced along the full path from the user to the applications.

This is where Cisco's Secure Access (SSE), which provides Zero Trust Network Access (ZTNA) and the AppOmni SaaS Security Platform, which provides Zero Trust Posture Management (ZTPM), converge to present a comprehensive Zero Trust architecture across networking and into SaaS.

What Is Zero Trust Posture Management (ZTPM)?

Gartner defines Zero Trust as, "a security paradigm that replaces implicit trust with explicit trusts that are continuously assessed based on identity and context risks". Nowhere is the need to create controls and policies with explicit trust felt more than in the case of SaaS applications which have become the de facto operating system of business. Nearly all SaaS breaches involve some violation of implicit trust models — for example: Person A is in a sales operations role, so she should be able to grant access to Salesforce to guest users; Person B is a test user who should be able to create new

users and grant them privileges (see Midnight Blizzard Breach). What if SaaS security policies can be designed (initial policy implementation), maintained (drift prevention), and monitored (anomalous user behavior detection) to create a security model for SaaS identities (for human and machine identities) that never trusts and always verifies regardless of the location of the user? Such a Zero Trust architecture needs to be implemented using the just-in-time context of the application, data access, users, behavior, and events. It goes beyond network controls and connectivity, giving defenders better mechanisms to prevent, detect, and react to attackers. This is Zero Trust Posture Management (ZTPM) for SaaS applications built on Zero Trust principles.

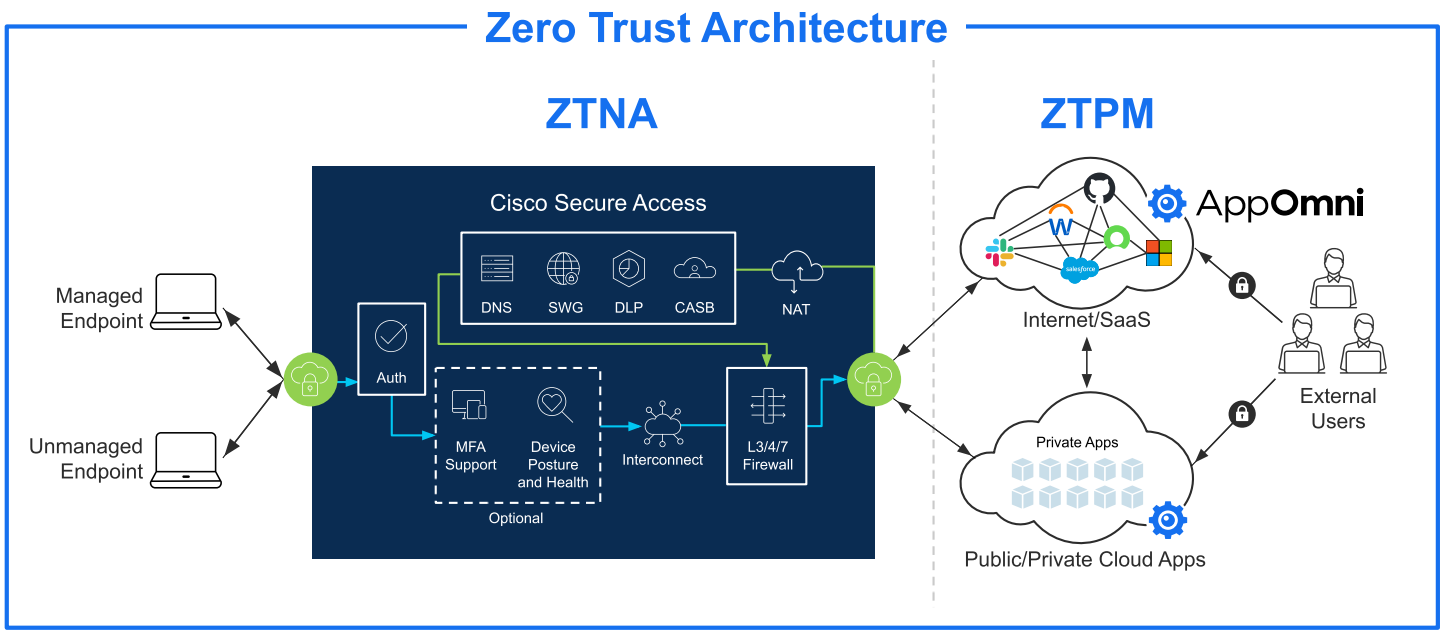
Unified Zero Trust Strategy with AppOmni and Cisco

Cisco Secure Access brings a robust, network-centric approach, merging networking and security functionalities into a singular cloud-based service. It leverages the principles of Zero Trust Network Access (ZTNA) to enforce strict access controls based on user identity and context, a strategy that becomes even more crucial as organizations navigate the challenges of remote work and cloud adoption.

As a complement to the traditional, network-centric ZTNA approach, AppOmni has implemented ZTPM principles for SaaS security to fill a critical void in Zero Trust implementations. AppOmni extends Zero Trust to the application layer regardless of access location, with complete visibility into configurations, security posture, SaaS identities (human and machine), and user behaviors within applications. It ensures the principles of Zero Trust are embedded deeply within the applications that manage and process vital business data.

ZTNA + ZTPM - Extend Zero Trust principles deeply to the applications that manage and process vital business information

Closed Loop Zero Trust Solution - Cisco & AppOmni



Closing the Loop: Zero Trust Posture Management

While Cisco Secure Access provides seamless and managed access to internal and external applications based on identity and device posture, AppOmni extends this security through the application layer.

Key security features include:

- Visibility into data access configuration and least privilege within SaaS applications
- Security coverage for all SaaS identities (human and machine) i.e. external users, anonymous/ guest-users, and third party or cloud-to-cloud applications
- Application and identity-aware threat detection to monitor user behavior of internal and external users
- Continuous security of application posture, configuration drift, and critical application components of SaaS applications
- Identify and mitigate misconfigurations such as side-loaded accounts or misconfigured Single Sign On (SSO) that may allow bypassing of ZTNA controls and protect your users from password attacks and account compromise
- Provides a 'Shared Signals Bridge' to inspect applications configurations and user activities. This creates a continuous feedback mechanism through which security events can be sent to Secure Access, Duo, or other components to support continuous authorization decisions

Continuous visibility into app configurations and activities enables a critical feedback loop in a Zero Trust architecture. This approach uses a user's permissions, data access entitlements, and behaviors to create a continuous authorization loop. This feedback loop facilitates dynamic adjustments to security measures or termination of access based on suspicious activities.

Additionally, AppOmni enhances the integrity of the Zero Trust Network Access (ZTNA) capabilities provided by Cisco Secure Access by identifying potential application misconfigurations that could lead to ZTNA circumvention. By implementing Zero Trust (ZT) principles across their applications, customers can detect unmanaged accounts, inadequate IP restrictions, and other security vulnerabilities. Such proactive identification helps prevent these misconfigurations from undermining ZTNA protections, thereby safeguarding users and data against phishing and other attacks, which ZT architecture aims to mitigate.

Completing the Identity Graph: Cisco Identity Intelligence and AppOmni Identity Fabric

With the continuing adoption of hybrid work increasing the sprawl of systems, applications, and accounts, an identity-centric view of security has become critical. The joint partnership between Cisco and AppOmni addresses this critical challenge head-on by integrating Cisco Identity Intelligence with the application visibility of AppOmni's SaaS Identity Fabric. This partnership provides visibility and control into user entitlements, data access, third-party application connections involving human and machine identities, and application activities/behaviors. This collaboration marks a significant leap forward in creating the most robust, shared picture of Identity security on the market.

Key features include:

- Continuous monitoring of user entitlements and compliance
- Identification of non-SSO accounts and non-human identities (SaaS-to-SaaS, service accounts, etc.) within each SaaS environment
- Integration with IAM tools for automated enforcement and validation of IAM policies
- Best-in-class identity activity monitoring, threat detection, and UEBA for SaaS

Enhancing SASE with SSPM for Comprehensive Security

The integration of Cisco's Secure Access and AppOmni represents a paradigm shift in achieving a comprehensive SaaS security with the combined power of SSE and SSPM. The security perimeter extends beyond traditional network boundaries to include robust SaaS application security, ensuring a seamless, secure experience for both corporate and non-corporate users.

This collaboration ensures:

- End-to-end, proactive security aligned with Zero Trust principles, applied continuously and through your SaaS applications.
- Enhanced visibility and control over SaaS identities, security posture, threats, and cloud-to-cloud connections
- Strong security assurance that your users and accounts are always protected by Secure Access
- Dynamic, responsive security measures applied continuously based on application context.

Conclusion: A Comprehensive Approach to Zero Trust

Together the Cisco SSE and AppOmni SSPM partnership offer customers a unified Zero Trust architecture that ensures comprehensive security across networking and into SaaS.

By embedding Zero Trust principles at every layer of the digital infrastructure, from the network to the application layer, Cisco Secure Access and AppOmni ensure that organizations can navigate the digital landscape with confidence, securing their valuable data and resources against both present and future threats.

Organizations are encouraged to embrace this integrated approach to cybersecurity, leveraging the combined strengths of Cisco's network-centric protections and AppOmni's SaaS-centric security, to achieve a truly robust and dynamic Zero Trust security architecture.

About AppOmni

AppOmni is the pioneer of SaaS Security Posture Management 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. Over 25% of the Fortune 100 and global enterprises across industries trust AppOmni to secure their SaaS applications. AppOmni is recognized by 2024 Great Place To Work, Forbes America's Best Startup Employers 2023, Fortune Cyber60, Strong Performer in the Forrester Wave™ SSPM Q4 2023 Report, and 2023 Company of the Year for Global SSPM by Frost & Sullivan.

Learn more at AppOmni.com and AppOmni on LinkedIn.