



Zscaler™ Private Access AppProtection

ZPA AppProtection Benefits:

Reduced risk of web-based threats to private applications

Detect malicious content in your private app traffic so you can manage threats before they disrupt your operations.

Protection against the most prevalent application attacks

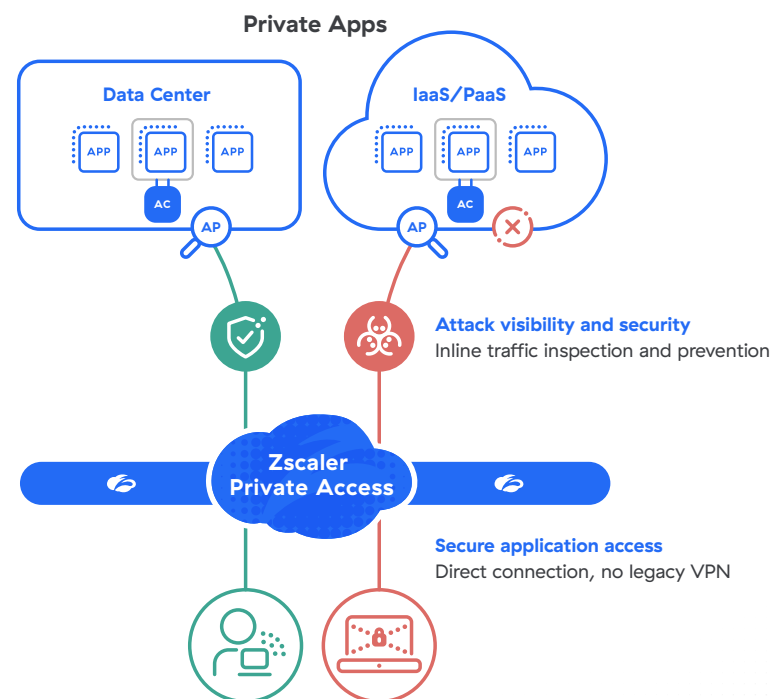
Block the OWASP Top 10 and other known web application security risks such as SQL injection and cross-site scripting.

Visibility over zero-day and known vulnerabilities

Get the latest zero-day signatures from the Zscaler ThreatLabz Research Team and actively patch against known CVEs with custom signatures.

Attackers regularly steal credentials, exploit application vulnerabilities, and bypass security controls to gain access to your network and spread laterally to high-value targets such as databases, file servers, CRM, and ERP systems. Businesses need visibility into malicious traffic destined for their internal applications as well as inline prevention methods to stop attacks that can disrupt their operations.

Zscaler offers powerful application security built into its zero trust network access solution, Zscaler Private Access (ZPA), to protect internal apps and infrastructure against the most prevalent cyberattacks. ZPA's AppProtection service provides high-performance, inline security inspection of the entire application payload to expose threats. It identifies and blocks known web security risks, such as the OWASP Top 10, and emerging zero-day vulnerabilities that can bypass traditional network security controls. With Zscaler's unique zero trust architecture, you get AppProtection as part of an integrated set of security services that is only available with advanced ZTNA solutions.



Use Cases

Application attack visibility

Expose threats with a high-performance security inspection of the entire application layer payload.

OWASP Top 10 defense

Block the most common attack types including:

- SQL injection
- Cross-site scripting
- Environment and port scanners

Zero-day threat protection

Guard your systems against exploits of newly discovered vulnerabilities with the latest signatures written by the Zscaler ThreatLabz Research Team.

High-risk user monitoring

Gain crucial visibility into user activities through detailed diagnostics and dashboards to detect signs of compromise.

Solution Capabilities

- **Powerful built-in application protection** identifies potentially malicious user traffic destined for private apps and prevents attempts to exploit vulnerabilities or abuse application logic. Admins can tailor protection against any threat or vulnerability, or implement business-specific security policies with our easily customizable rulesets.
- **OWASP Top 10 prevention** provides comprehensive coverage for the most common types of attacks used by cybercriminals—including SQL injection, cross-site scripting, environment and port scanners, and cookie poisoning.
- **Positive security controls** reduce your application attack surface by allowing only known good traffic, and enforcing access and inspection policies based on identity and context.
- **Inline traffic inspection** analyzes every HTTP/S transaction between users and private apps, providing visibility into the application layer (L7) not possible with traditional network security controls (L4).
- **Zero-day threat defense** provides predefined signatures from the Zscaler ThreatLabz Research Team to protect against the latest security threats.
- **Browser session protection** identifies high-risk users by examining the number of unique fingerprints generated by user browser activity and flagging users with an abnormally high fingerprint count.
- **Easy deployment and scalability** with one-click activation from the Zscaler Private Access console and no new components to install in your environment.

Visit zscaler.com/zpa to learn more about what Zscaler Private Access can do for you.

 | Experience your world, secured.™

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

© 2023 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.