Zscaler AppProtection

Fortify Private Application Security to Stop Critical Threats

Reduce web-based threats with inline inspection

Inspects HTTP/S traffic to private applications and mitigates web application risks, including those in OWASP Top 10 such as SQL injection and Server Side Request Forgery (SSRF).

Identify and detect Active Directory attacks

Enhance your Active Directory security by inspecting traffic and detecting behaviors related to Active Directory attacks, such as kerberoasting and user enumeration.

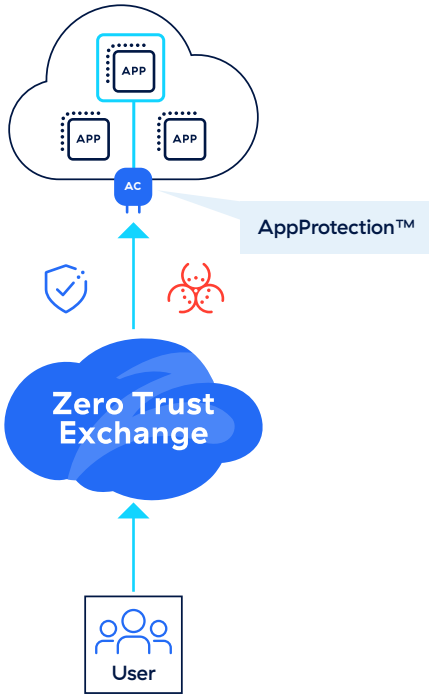
Prevent zero-day attacks and browser-based vulnerabilities

Automatically apply virtual patches against the latest CVEs identified by Zscaler ThreatLabz and secure third-party access.

The migration of private applications to the cloud and the rise of remote work have dispersed users, applications, and data worldwide. The internet has become an extension of the corporate network, making traditional "castle and moat" security architectures insufficient for protecting today's enterprises. There's a need for robust security solutions that must address vulnerabilities such as misconfigurations, insecure designs, and unpatched components, with a particular focus on mitigating web application and API risks, as highlighted in the OWASP Top 10.

Moreover, vulnerabilities in core network services such as Active Directory, LDAP, and SMB, prone to attacks like kerberoasting and injections, are driving the need for advanced monitoring, enhanced encryption, and stringent access controls. The rise in critical CVEs and zero-day attacks further compels organizations to prioritize real-time threat detection and proactive security strategies.

Zscaler AppProtection, an integral component of Zscaler Private Access™ (ZPA), ensures robust security for private applications by guarding against web and identity-based threats through comprehensive inline application layer (Layer 7) inspection. This advanced solution identifies and blocks malicious traffic aimed at exploiting vulnerabilities or altering application logic. By consolidating inspection capabilities into ZPA, it significantly reduces the risks associated with misconfigurations and incompatibilities. Additionally, Zscaler AppProtection strengthens security measures, enhances threat detection, and aligns with the MITRE ATT&CK framework, all while protecting against the latest CVEs with timely signatures and virtual patching, courtesy of the Zscaler ThreatLabz team.



Use Cases

Protect private apps from third-party web threats

In addition to ZPA providing secure access to private applications for third parties, such as contractors, partners, and agencies, it is crucial to ensure that private applications are protected against web-based risks and to report any suspicious browser-based activities.

AppProtection, an integral component of ZPA, secures private applications from web-based threats, including those listed in the OWASP Top 10, such as SQL injection, cross-site scripting, server-side request forgery, and remote code execution. It continuously monitors app traffic for any malicious activities.

AppProtection also aligns with the MITRE ATT&CK framework, providing protection against third party web threats using techniques such as Trusted Relationship (T1199), Browser Session Hijacking (T1185), and Web Service (T1102), among others.

Detailed visibility into user logging paths during VPN replacement

VPN replacement is one of the key use cases to consider when adopting a zero trust environment. ZPA is the industry's first AI-powered ZTNA solution. During this transition, it is critical to have visibility into the details specific to domain and path access for all users of web applications and APIs.

AppProtection can monitor the logging details of every user accessing a private application. It provides detailed visibility into every transaction of a user and the response code. This information can help detect any malicious activity.

Protect against web and identity threats and maintain compliance throughout M&A

During a M&A, AppProtection can help secure private applications in two specific areas. First, it can inspect and monitor all users accessing applications for any web threats, including the OWASP Top 10 risks. Second, it can ensure protection against Active Directory attacks such as kerberoasting, LDAP, and SMB enumeration, while also safeguarding against malicious insiders. This level of protection is crucial when integrating multiple networks and applications that have different credentials and authentication systems.

Product Benefits

Powerful built-in application protection identifies potentially malicious traffic aimed at private apps and prevents attempts to exploit vulnerabilities or abuse application logic. Admins can customize protection against any threat or vulnerability and implement business-specific security policies using our easily customizable rule sets.

Reduce web-based threats with inline traffic inspection

Inline traffic inspection analyzes every HTTP/S transaction between users and private apps, providing visibility into the application layer (L7), which is not achievable with traditional network security controls at layer 4 (L4).

Protect against OWASP Top 10 risks

OWASP Top 10 protection offers comprehensive coverage against the most common types of web attacks, including SQL injection, cross-site scripting, server-side request forgery, and remote code execution.

Identify and detect Active Directory attacks

Enhance Active Directory security by inspecting and detecting suspicious activity related to kerberoasting, LDAP, and SMB enumeration.

Detect and respond to latest CVEs by virtual patching

Zero-day threat defense uses predefined signatures from the Zscaler ThreatLabz research team to protect against the latest security threats.

Detect and report suspicious browser-based activity

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.

Integrated for effortless deployment

Management from the ZPA console lets you achieve easy deployment and scalability, with no new components to install in your environment.

Align with the MITRE ATT&CK framework

The MITRE ATT&CK® framework is a globally-accessible knowledge base of adversary tactics and techniques, that helps security teams assess their defense strategies by understanding attack behaviors. AppProtection aligns with this framework to evaluate your organization's security posture and assess cyber attack risks.

For more information on MITRE ATT&CK framework, visit: https://attack.mitre.org/

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com