

Zscaler Identity Protection™



AT-A-GLANCE

Zscaler Identity Protection Benefits:

REDUCE IDENTITY ATTACK SURFACE

Get visibility into identity misconfigurations that enable adversaries to escalate privileges and move laterally.

DETECT IDENTITY ATTACKS

Stop stealthy identity threats like DCSync, DCShadow, and kerberoasting that bypass existing defenses.

MITIGATE IDENTITY RISK

Measure and monitor your identity attack surface posture using risk scores generated by the identity security assessment.

What is Zscaler Identity Protection?

Zscaler Identity Protection provides visibility into misconfiguration and vulnerabilities in on-prem Active Directory, Entra, and hybrid identity stores to reduce your attack surface and detects identity-based attacks that abuse privileges, on-device credentials, and risky entitlements to move laterally.

Monitor your Active Directory for any misconfigurations or vulnerabilities that expose you to privilege escalation and lateral movement risks with Zscaler Identity Protection. It secures your identities and offers extensive visibility into the identity attack surface to deliver real-time notifications on identity-based assaults. You can now detect and stop identity-based attacks such as stolen credentials, multi-factor authentication bypasses, and privilege escalation techniques.

Why Zscaler ITDR?



NO ADDITIONAL AGENTS / VMS REQUIRED

Built into the Zscaler Client Connector, Zscaler Identity Protection unlocks new capabilities and protections out-of-the-box.



INTEGRATED WITH ACCESS POLICY

The Zscaler Zero Trust Exchange can dynamically apply access policy controls to block compromised users when an identity attack is detected.



SOC INTEGRATIONS

Strengthen investigation and response with Integrations that include EDRs like CrowdStrike, Microsoft Defender, VMware CarbonBlack, and all leading SIEMs.

Key Capabilities

...❖ UNCOVER ISSUES THAT ALLOW ATTACKERS TO GAIN THE UPPER HAND

Discover risky configurations like GPP password exposure, unconstrained delegation, and stale passwords that open up new attack paths.

...❖ BUILD STRONG IDENTITY HYGIENE WITH REMEDIATION GUIDANCE

Understand the issue, impact, and who is affected. Leverage step-by-step remediation guidance along with video tutorials, scripts, and commands.

...❖ GET ALERTS WHEN CONFIGURATION CHANGES INTRODUCE RISK

Identity systems are in constant flux with configuration and permission changes. Monitor in real-time and get alerted to new risks and issues.

...❖ STOP PRIVILEGE ESCALATION WITH IDENTITY THREAT DETECTION

Not all misconfigurations can be remediated. Detect and stop attacks like DCSync, DCShadow, kerberoasting, and more in case of a compromise.

...❖ REDUCE THE SCOPE OF YOUR CREDENTIAL ATTACK SURFACE

Find insecurely stored credentials across your endpoint fleet, get visibility into which of those already compromised or easily cracked, and scrub them with one click.

Use Cases

IDENTITY ATTACK SURFACE VISIBILITY

- Risk score for identity posture quantification and tracking
- Discover top identity issues and riskiest users/hosts
- MITRE ATT&CK mapping for visibility into security blind spots

IDENTITY HYGIENE MANAGEMENT

- Identify new misconfigurations as they emerge
- Real-time alerting for new risks in your identity store
- Ready-made guidance, commands, and scripts for remediation

IDENTITY THREAT DETECTION AND RESPONSE

- Detect attacks against your identity store
- Stop kerberoasting, DCSync, LDAP enumeration, and more
- Built-in containment using zero trust access policy

Visit our [webpage](#) to learn more about Zscaler Identity Protection.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at [zscaler.com](#) or follow us on Twitter [@zscaler](#).

© 2025 Zscaler, Inc. All rights reserved. Zscaler™ 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.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

[zscaler.com](#)



**Zero Trust
Everywhere**