



Zscaler ITDR™

Bringing identity-first security to zero trust

Zscaler ITDR (Identity Threat Detection and Response) detects and defends against identity-based attacks such as credential theft and privilege abuse, Active Directory assaults, and risky entitlements.

Identity is the New Attack Surface

Cyber Attackers are now using sophisticated methods to target identities and identity systems. With identity-based attacks on the rise, today's businesses require the ability to detect when attackers exploit, misuse, or steal enterprise identities. Legacy threat detection techniques and identity systems are often ineffective as they weren't built to handle identity-based threats. Zscaler ITDR mitigates the risk of cyberthreats that target identities and identity infrastructure (on-prem Active Directory).

Zscaler ITDR

Monitor your Active Directory for any misconfigurations or vulnerabilities that expose you to privilege escalation and lateral movement risks with Zscaler ITDR. 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.

Benefits

- **Detect Identity threats in Real-time:** Identity systems are in constant flux with configuration and permission changes. Monitor in real time and get alerted on new vulnerabilities, risks, and issues.
- **Reduce Identity Attack Surface:** Get visibility and remediate identity misconfigurations and risky permissions that create exposure.
- **Mitigate the Risk of an Identity Attack:** Discover risky configurations such as GPP password exposure, unconstrained delegation, and stale passwords that open new attack paths.
- **Accelerate Investigation & Response:** Help security teams prioritize investigation on alerts based on risk scores generated by identity assessments.
- **Streamline Remediation:** Security teams can now leverage Zscaler ITDR step-by-step remediation guidance along with video tutorials, scripts, and commands to speed up response.
- **Deploy Easily:** No additional VMs required. Use the same Zscaler client connector to provide an additional layer of security to thwart identity-based threats.

5/10

Organizations suffer an Active Directory Attack

Source: EMA

80%

Of modern attacks are identity-driven

Source: CrowdStrike

90%

Of Mandiant IR engagements involve AD

Source: Dark Reading

How does it work?

Zscaler ITDR takes a low-touch and operationally simple approach to identity security. It's built into Zscaler Client Connector, a unified agent that securely brokers connections between users and applications/resources.

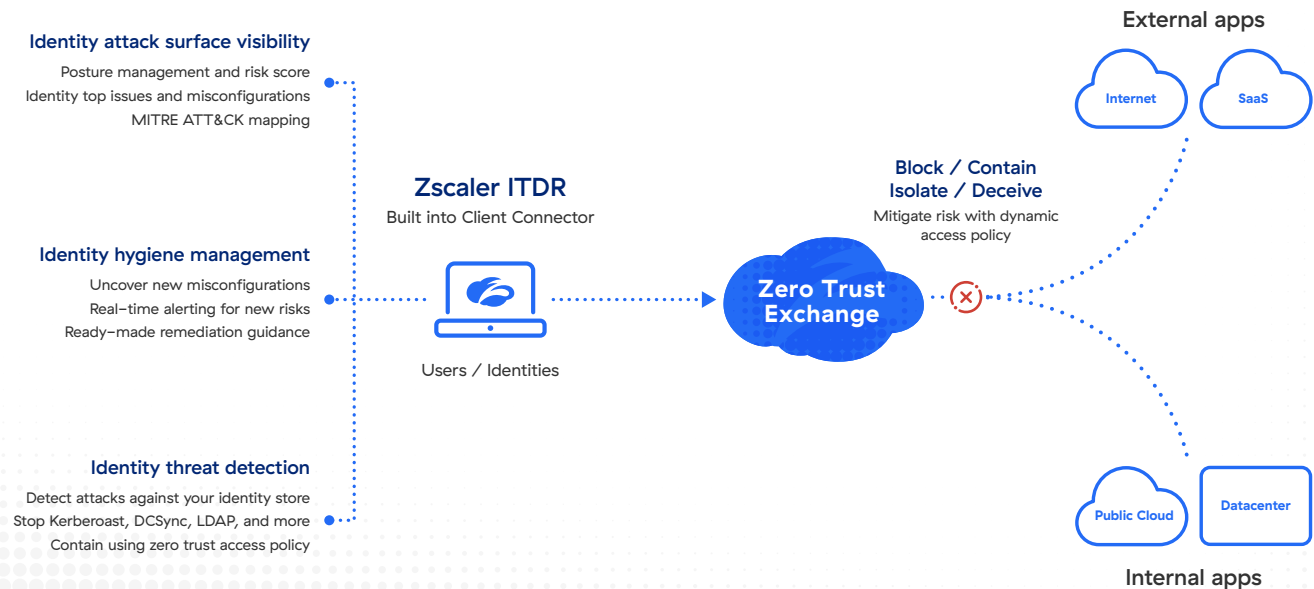
Zscaler ITDR consists of three capabilities:

- Identity Attack Surface Visibility
- Identity Change Detection
- Identity Threat Detection

Attack Surface Visibility

Zscaler ITDR audits the Active Directory by running LDAP queries to build a map of schema, users, computers, OUs, and other objects in your identity store. It then runs checks against these objects to find misconfigurations and vulnerabilities that exist in your Active Directory.

- For assessing the Active Directory, Zscaler ITDR needs to run on a Client Connector installed on a domain-joined Windows machine.
- The security team sets up a scan by specifying the Active Directory domain they wish to access and selecting the Client Connector installed machine from which to run the scan.
- Depending on the size of the Active Directory, it takes anywhere between 15 and 30 minutes to complete the assessment.
- Once the assessment is complete, the results are available to view in the dashboard.
- The assessment includes a domain risk score, focus areas to prioritize remediation, a list of the riskiest users and computers, a basic analysis of severity and risk categorizations, MITRE ATT&CK kill chain mapping, and a complete list of misconfigurations discovered.



For each misconfiguration, the solution provides the following:

- Risk categorization
- Severity
- Remediation effort
- MITRE ATT&CK ID and tactic
- Explanation of the issue
- Potential impact
- List of users, computers, and objects affected
- Remediation guidance
- Video tutorials
- Scripts
- Commands

Identity Change Detection

Once an assessment has been configured, security teams get the ability to turn on change detection for the Active Directory domain. Change detection surface configurations that affect the security posture of Active Directory in near real-time, allowing security teams and directory admins to quickly respond.

- Zscaler ITDR runs a series of high-priority configuration checks against Active Directory.
- The scope of these checks targets the discovery of issues that have the highest possibility of abuse by adversaries.
- These checks run every 15 minutes from the Client Connector installed endpoint for the given domain.
- Changes are marked as having a good or bad impact.
- A good impact indicates that an issue has been resolved.
- A bad impact indicates a potential issue has been introduced.

Real-time Identity Threat Detection

Zscaler ITDR has a threat detection capability that alerts SOC teams and threat hunters of malicious activities directed toward potentially malicious misuse and theft of identities.

Identity Threat Detection can be turned on as an endpoint policy on designated Client Connector installed machines.

- Security teams enable the threat detection policy which enables monitoring events on the system and analyzes for patterns to identify indicators of the chosen threat vectors.
- Available detectors include DCSync, DCShadow, kerberoasting, session enumeration, privileged account access, LDAP enumeration, and more.
- Security teams can choose to turn on all or a combination of detectors on designated endpoints.
- If a pattern is noticed, Client Connector signals to Zscaler ITDR that a threat has been detected.
- The platform enriches the threat signal with information relevant to the user to perform an investigation
- The security team can configure orchestration capabilities in Zscaler ITDR to take automated actions from alerting to forwarding to remediation.

Key Use Cases

Identity Attack Surface Visibility

Continuous assessment of your Active Directory provides a unified risk score, a list of misconfigurations and vulnerabilities, and remediation guidance to fix those issues.

- Unified risk score for identity posture quantification and tracking
- Real-time view of top identity issues and riskiest users/hosts
- MITRE ATT&CK mapping for visibility into security blindspots

Identity Hygiene Management

Get alerts and notifications in real time as new risks are introduced to your Active Directory. Gain real-time visibility into risk configuration and permission changes.

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

Identity Threat Detection and Response

Real-time threat detection for top identity attacks

- Detect attacks against your identity store
- Detections include kerberoast, DCSync, and LDAP enumeration
- Built-in containment using zero trust access policy

Key Differentiators

Built into Client Connector

Built into the Zscaler Client Connector, Zscaler ITDR unlocks new capabilities and protections out-of-the-box. The same endpoint client that securely connects users to the internet and application now provides additional security capabilities and mitigates the risk of identity attacks.

Integrated with the Zero Trust Exchange

Zscaler Identity integrates seamlessly with the Zscaler Zero Trust Exchange platform for better threat detection and response for identity-based threats. The Zero Trust Exchange can dynamically apply access policy controls to block compromised users when an identity attack is detected.

Seamless Integrations

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

Harden Your Security Posture with Zscaler ITDR

Defend Against Identity Threats

Gaining visibility on identities is essential to detecting identity-based threats. Zscaler ITDR provides deep visibility into identity-based incidents and anomalies across your IT environment, so you can thwart identity-based attacks before they occur.

Detect Active Directory Attacks

Active Directories are popular targets for identity attacks. Zscaler ITDR continuously monitors AD/Azure AD for vulnerabilities and misconfigurations or risky configurations.

Prevent Credential Misuse/Theft

Attackers use stolen credentials and attack Active Directory to escalate privileges to move laterally. Zscaler ITDR helps to detect credential exploits and prevent credential theft or misuse.

Stop Lateral Movement

Zscaler ITDR identifies misconfigurations and credential exposures that create attack paths for lateral movement. Stop attackers who have gotten past perimeter-based defenses and are attempting to move laterally through your environment.

Zscaler ITDR unlocks powerful new capabilities that extend what your zero trust program is capable of without adding additional operational or resource overhead.



Experience your world, secured.™

About Zscaler

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 SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @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.