Zscaler ITDR™

Zscaler ITDR 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 ITDR?

With the rapid adoption of zero trust, attackers are targeting users and identities as the point of entry and using that access to escalate privileges and move laterally. Zscaler ITDR provides continuous visibility into identity misconfigurations and risky permissions. It augments this visibility with guidance in the form of video tutorials, scripts, and commands to remediate these issues and reduce your internal attack surface.

In addition to preventive capabilities Zscaler ITDR also provides high-fidelity detections for identity-based attacks like stolen credentials, multi-factor authentication bypasses, and privilege escalation techniques that usually pass through existing defenses in cases of identity compromise.

Why Zscaler ITDR?

No additional agents / VMs required
Built into the Zscaler Client Connector, Zscaler ITDR 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.

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 ITDR.

zscaler™ | 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**.

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