JOINT SOLUTION BRIEF

zscaler™ + torq

Powerful collaboration and remediation across the Zscaler suite.

INTEGRATION HIGHLIGHTS

- Automatically detect and respond to Zscaler alerts in real time using Torq's autonomous security operations platform.
- Simplify and secure temporary access to blocked content with structured, auditable workflows.
- Correlate and act on data across Zscaler, EDR, and identity platforms to accelerate investigation and remediation.

The Market Challenge

Today's enterprise environments are increasingly distributed and complex, with users accessing resources from anywhere, using a wide range of devices and networks. Security operations teams are inundated with a growing number of alerts across fragmented systems—network security, endpoint detection, cloud apps, and more—without a unified way to correlate data and prioritize response. Analysts are forced to manually stitch together context across disparate tools, resulting in alert fatigue, missed threats, and delayed response times.

Compounding the issue is the lack of automation in key workflows such as URL blocking, access approvals, and incident response. Manual processes not only slow down remediation efforts, but they also introduce human error and create compliance gaps. In a world where every second counts, organizations need integrated and intelligent solutions that deliver end-to-end visibility, automated response, and seamless user access control—without the operational drag of switching between disconnected systems.

The Solution

Zscaler and Torq integrate cloud-delivered zero trust access with intelligent hyperautomation to help organizations reduce risk, improve consistency, and accelerate response. By combining Zscaler Internet Access (ZIA) with Torq's autonomous security operations platform, security teams can automate high-impact workflows such as responding to threat alerts, managing temporary access requests, and updating global blacklists—all without switching between tools or relying on manual tasks.

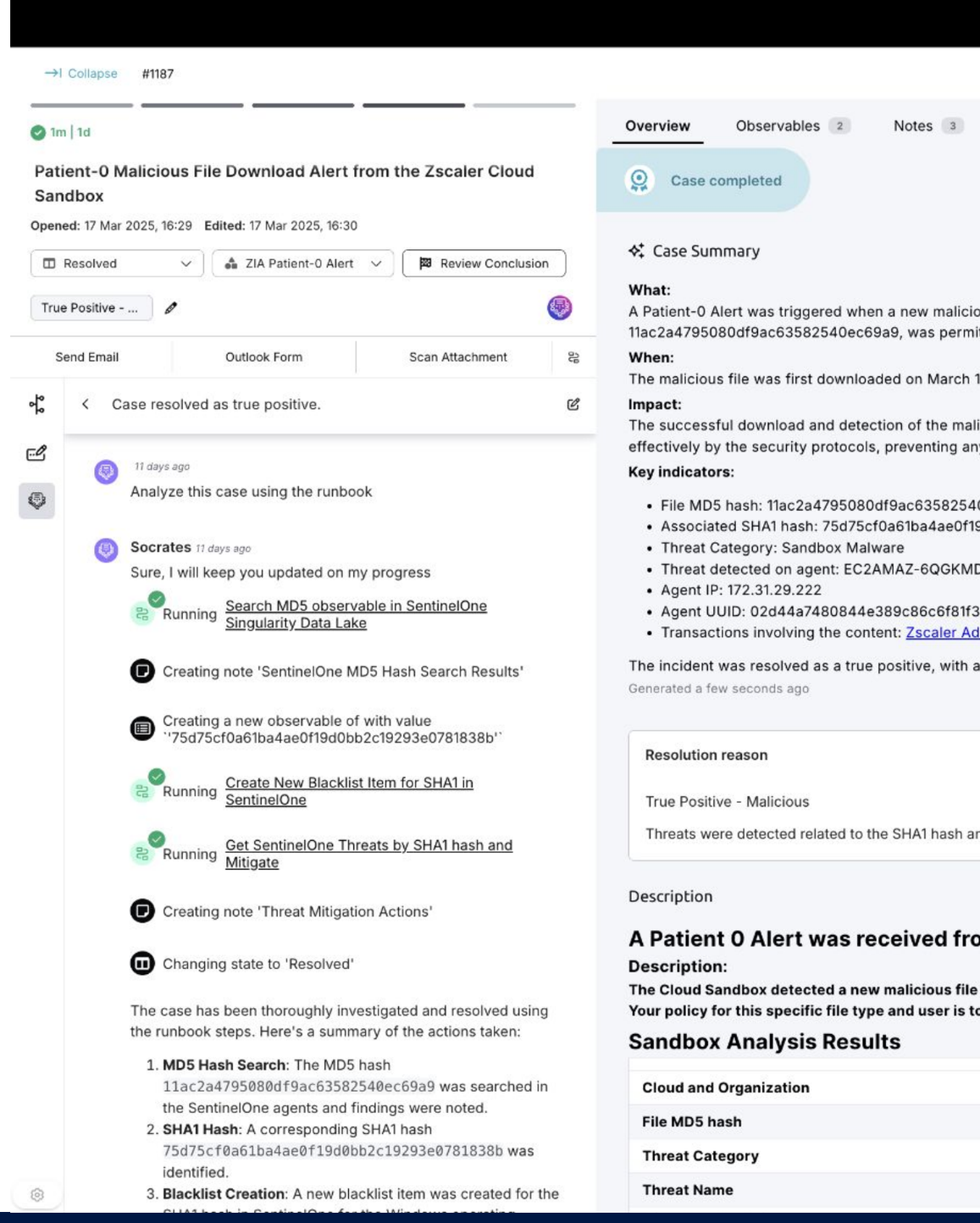
With Torq's event-driven hyperautomation and agentic AI SOC analyst (Socrates), security teams can instantly respond to ZIA "Patient 0" alerts, perform threat hunting across EDR platforms, and enforce time-bound access policies based on real-time context. This seamless integration eliminates bottlenecks, enhances visibility, and enables faster, more accurate decision-making across the entire security stack.

Say goodbye to manual mayhem—Zscaler and Torq deliver real-time, zero trust hyperautomation that hunts, blocks, and protects at machine speed.

Solution Components Deep Dive

Torq adds an AI-driven hyperautomation layer to Zscaler, enabling security teams to build event-driven workflows across ZIA, EDRs, identity systems, and collaboration tools—without writing code. Whether reacting to ZIA "Patient 0" alerts or processing access requests from block pages, Torq captures events, enriches them with context (like file hashes and user data), and triggers hyperautomated actions. These workflows are fully auditable, scalable, and easy to adapt to any security policy.

Powered by Torq's integration framework and agentic AI SOC Analyst, the platform delivers fast, intelligent response and continuous policy enforcement. For example, when ZIA flags a malicious file, Torq Socrates can correlate the hash across EDRs, isolate endpoints, and blacklist the threat autonomously. It also handles time-bound access rules in ZIA—creating and revoking them based on identity, approval, and duration. The result: faster remediation, lower risk, and security actions that align with zero trust by default.



KEY USE CASES

Collaboration Tool Based ZIA Blacklist Management

Security analysts can check, add, or remove URLs from the Zscaler Internet Access (ZIA) global blacklist directly through collaboration tools like Slack. Torq automates the entire process—querying ZIA for URL categorization, prompting for confirmation, and updating the blacklist—reducing response times and eliminating risky manual steps. False positives can be reversed just as easily, making blacklist management faster, safer, and fully auditable.

Automated Response to ZIA "Patient 0" Alerts

When ZIA's sandbox identifies a malicious file post-delivery, Torq springs into action—automatically creating a case, investigating the file hash across EDR platforms, blacklisting the threat, and quarantining infected endpoints. Powered by Socrates, Torq's agentic AI SOC Analyst, this use case transforms a manual, time-consuming incident response into a fully autonomous workflow, dramatically reducing dwell time and preventing lateral spread.

"The integration between Zscaler and Torq gives customers end-to-end visibility and control. Blacklist updates, incident triage, and access approvals can happen automatically with full auditability. Security teams are going from chasing endless alerts to fully automating their response, and threats are mitigated in seconds instead of hours."

Eldad Livni

Co-founder and Chief Innovation Officer, Torq

Zscaler + Torq Benefits

ACTION	DESCRIPTION
Automate Threat Response	Respond to ZIA alerts in real time by triggering end-to-end remediation workflows across your EDR, identity, and network security stack—without analyst intervention.
Streamline Access Approvals	Allow employees to request temporary access to blocked content through a structured, auditable process integrated with ZIA, Slack, and identity providers.
Accelerate Investigation	Correlate alerts and threat indicators across ZIA, EDR, and IAM tools automatically, enabling faster root cause analysis and reducing mean time to resolution (MTTR).
Eliminate Manual Errors	Replace risky, manual steps like URL blacklisting or rule creation with automated, policy-driven workflows that ensure accuracy and consistency every time.
Enforce Zero Trust Policies	Apply context-aware, time-bound access rules based on user identity, risk posture, and approval status—then automatically revoke them when no longer needed.

Conclusion

Zscaler and Torq combine zero trust access with AI-driven security hyperautomation to transform manual, reactive security operations into fast, intelligent, and consistent workflows. By integrating Zscaler Internet Access (ZIA) with Torq's Hyperautomation engine and agentic AI SOC Analyst, organizations can autonomously respond to alerts, enforce time-bound access, and manage blacklist policies—without switching tools or writing code. This unified approach accelerates incident response, improves policy enforcement, and gives security teams the power to scale operations while reducing risk.

Learn more at **www.zscaler.com/partners/technology**

zscaler™ | **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 SASE-based Zero Trust Exchange is the world's largest in line cloud security platform. Learn more at zscaler.com or follow us on X (Twitter) @zscaler.

+1 408.533.0288

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

©2025 Zscaler, Inc. All rights reserved.