LEVELBLUE + ZSCALER + SENTINELONE: INTEGRATION BRIEF

LevelBlue Managed Endpoint and Network Security, Powered by Zscaler and SentinelOne

Market Challenges

Today's enterprise technology stacks are complex – with distributed applications, users, and endpoints, an ever-expanding list of IoT devices, and new sanctioned and unsanctioned tools being deployed daily. As attack vectors multiply, from endpoints to networks to the cloud, security teams struggle to secure their valuable assets inside and outside the traditional network perimeter.

The more security controls that security operations teams deploy, the more alerts they get, but too often, the signal is buried in the noise. Security analysts are forced to pivot between tools that do not integrate and fail to connect the dots across the entire technology stack. As a result, security data is collected and analyzed in isolation, without any context or correlation, creating gaps in what security teams can see and detect, leading to longer dwell times. This complexity has necessitated a new approach to securing access—one that provides frictionless security from endpoint to network to application.

Joint Solutions

LevelBlue unifies SentinelOne and Zscaler technologies to provide enterprise security across endpoint, network, and cloud, enabling enhanced end-to-end visibility, accelerated remediation, seamless sandboxing, and secure conditional access. SentinelOne continuously protects, detects, and responds to threats across endpoints, identities, and cloud workloads with unified analytics.

Key Use Cases:

- Comprehensive visibility
- Integration of SentinelOne and Zscaler
- Provides security teams with a holistic understanding of threat context and user attributes
- Allows for quick response to attacks

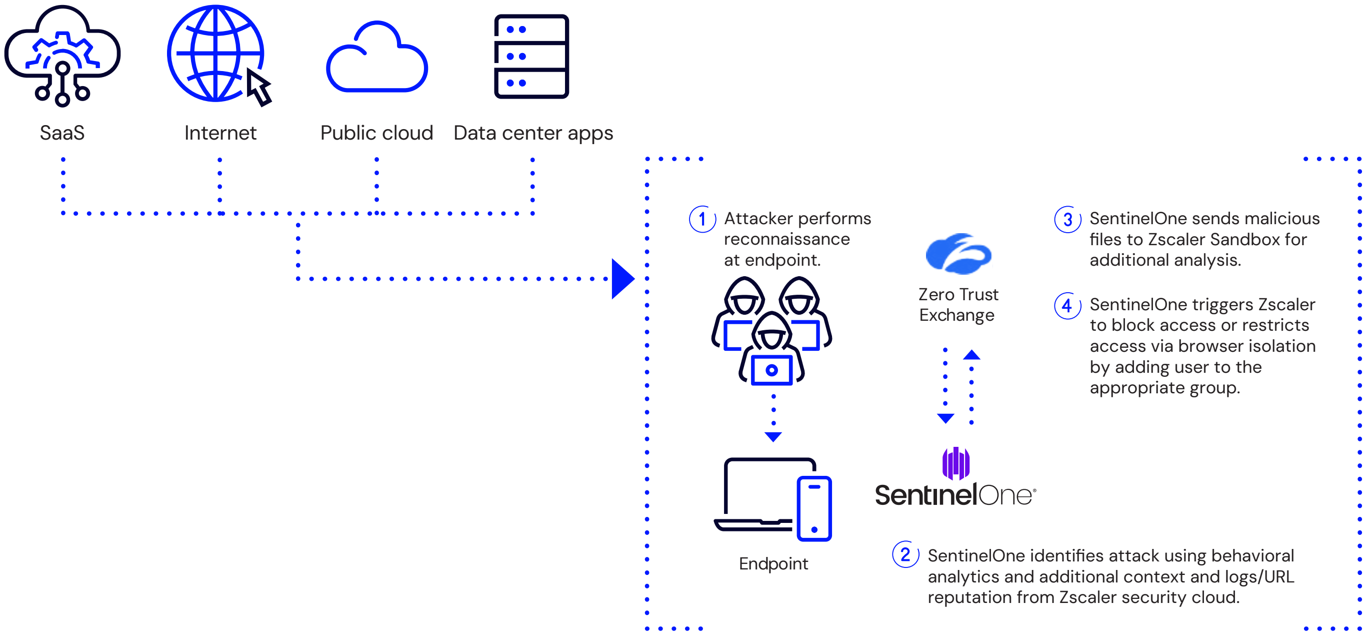
Solution Benefits:

- Efficiently prevent business compromise
- Simplify security operations
- 24/7 monitoring
- Consolidated, fully managed solution

Joint Solution Highlights:

- Zero Trust security with advanced threat protection and End-to-End Visibility
- Threat enrichment with user attributes, URL lookups, and sandbox analysis
- Accelerated investigation and remediation
- Zero Trust conditional access
- Increased visibility
- AI-powered threat detection

Extended Visibility and Accelerated Remediation


SaaS
Internet
Public cloud
Data center apps
1 Attacker performs reconnaissance at endpoint.
Endpoint
Zero Trust Exchange
SentinelOne
3 SentinelOne sends malicious files to Zscaler Sandbox for additional analysis.
4 SentinelOne triggers Zscaler to block access or restricts access via browser isolation by adding user to the appropriate group.
2 SentinelOne identifies attack using behavioral analytics and additional context and logs/URL reputation from Zscaler security cloud.

The Zscaler Zero Trust Exchange provides secure access to internet, SaaS apps, and private apps for all users from any device or location, with inline AI-powered traffic inspection and advanced threat protection.

LevelBlue delivers managed services atop SentinelOne and Zscaler technology to minimize risk across an organization's entire attack surface, at the network, endpoint, and application levels. With proactive monitoring through the LevelBlue SOC, threats are investigated and remediated more efficiently to keep business operations running smoothly.

Accelerated Remediation: SentinelOne and Zscaler enable security analysts to speed up response with policy-driven actions that automatically remediate threats in Zscaler from the SentinelOne console.

Seamless sandboxing: SentinelOne's platform and Zscaler Sandbox offer a seamless sandbox analysis experience to further enrich threats.

Zero Trust Conditional Access: The SentinelOne and Zscaler Zero Trust Exchange integration enables seamless conditional access, ensuring that a trusted identity on a trusted device can directly access authorized corporate applications without exposing the network.

Unparalleled Visibility, Threat Protection, and Automated Response: Zscaler and SentinelOne provide best-in-class Zero Trust access control with unparalleled visibility, threat protection, AI-powered detection, and automated response across endpoints, applications, and cloud workloads.

Continuous Policy Check and Compliance Enforcement: SentinelOne continuously checks policy and enforces compliance at every endpoint security incident.

Managed Security Service Benefits

High-Touch

Onboarding Support and System Setup

24/7

Monitoring

LevelBlue SOC Analysts

Monitor and Manage

Unified Security Strategy

Reduce Costs

Onboarding

- Set up environment including implement console, create users, complete platform integration, and configure policies
- Guidance and recommendations provided throughout agent deployment
- Policy tuning by creating exclusions, filtering or suppressing rules, creating orchestration rules, and changing policies
- Create a Customer Engagement Plan (CEP) and keep it updated to provide a common framework of procedures for investigating and responding to security incidents
- Training of the platform, including an overview of the agents, platforms, integration tools, and demo the management consoles

LevelBlue SOC Management

- Triage alarms to identify actionable security threats, update alarm status, or open investigations
- Investigate threats by gathering additional forensic information, update the severity, and determine remediation steps
- Respond to threats, per the CEP, and remediate threats by taking actions including to isolate, disconnect, or rollback an agent
- Ongoing policy tuning based on recurring false positive exclusions, block lists, or policies can be updated
- Schedule recurring analyst meetings to review recent investigations, outcomes, and any compliance or audit reporting need

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

To learn more, contact your LevelBlue representative.