Zscaler and Cimcor

Enhancing cybersecurity with real-time integrity monitoring and zero trust access control

Solution Brief

At-A-Glance

- **Change detection:** CimTrak can detect integrity or compliance deviations throughout the environment and provide awareness, forensics, and audit logs for these unexpected changes.
- **Hardening/compliance:** CimTrak can scan systems for secure, hardened configurations and if they meet or beat best practice standards from CIS or DISA.
- **Access management:** Zscaler can manage and restrict which users, systems, and networks have access to within the environment.
- **Security automation:** The integration leverages CimTrak's ability to detect unwanted changes, unexpected changes, threats, or if the systems are in a hardened and compliant state to then automatically enable/disable specific Zscaler policies to change or prevent access to these machines that are no longer in a state of integrity or compliance.
- **Zscaler configuration monitoring:** CimTrak can also audit and log when changes are made in Zscaler; alerting on any policy, user, or configuration deviations. Side-by-side comparisons are offered to show exactly what settings/values were modified.

The Market Challenge

Organizations across all industries are facing an unprecedented array of cybersecurity threats. From sophisticated malware to insider attacks, the potential for system compromise and data breaches has never been higher. Traditional security measures are no longer sufficient to protect against these advanced threats.

Many businesses struggle to detect critical system changes in real-time and are most often going undetected for months, with unrestricted access, leaving them vulnerable to attacks that can spread rapidly across their networks. The consequences of a successful breach can be severe, including data loss and leaks, operational downtime, and significant damage to an organization's reputation and bottom line.

What You Need

Organizations need a security solution that adapts to the dynamic nature of modern IT environments. Real-time change detection and alerts are crucial for identifying potential threats quickly. However, detection alone is insufficient; the ability to rapidly manage and modify access to affected systems is critical. An ideal solution combines real-time incident detection with automated access control, ensuring that compromised or non-compliant systems can be immediately isolated or restricted.

Zscaler and Cimcor: A Powerful Alliance

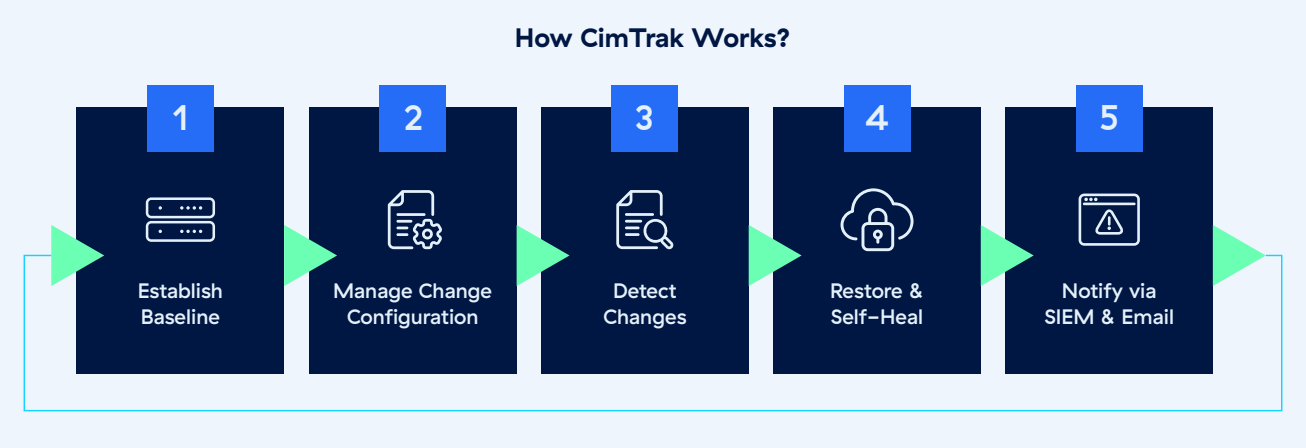
The partnership between Zscaler and Cimcor creates a comprehensive security solution that addresses the complex needs of modern organizations. This integration leverages the use of Cimcor's flagship product, CimTrak, to combine real-time system integrity and security posture monitoring capabilities with Zscaler's sophisticated access control, enabling:

- Immediate detection and response to critical system modifications
- Monitoring and auditing of Zscaler configuration settings
- Dynamic Zscaler policy adjustments based on system integrity
- Rapid quarantine of compromised or non-compliant systems
- Streamlined compliance management and reporting
- Enhanced system hardening through continuous security assessments

By leveraging this integrated solution, organizations can dramatically improve their security posture, minimize the risk of successful cyberattacks, and maintain compliance with industry regulations.

What is CimTrak?

CimTrak is a Next-Gen Integrity Monitoring tool and Benchmarking/Hardening solution that revolutionizes how users understand and manage change within their enterprise. By replacing outdated polling interval checks with true, real-time change detection, CimTrak provides instant alerts with comprehensive forensic details, including the who, what, when, and where of each change. Additionally, CimTrak streamlines system hardening and vulnerability management through continuous compliance scans based on industry-recognized best practices from CIS and DISA. These scans assess your system security settings against modern cybersecurity expectations, ensuring your infrastructure remains secure and compliant.



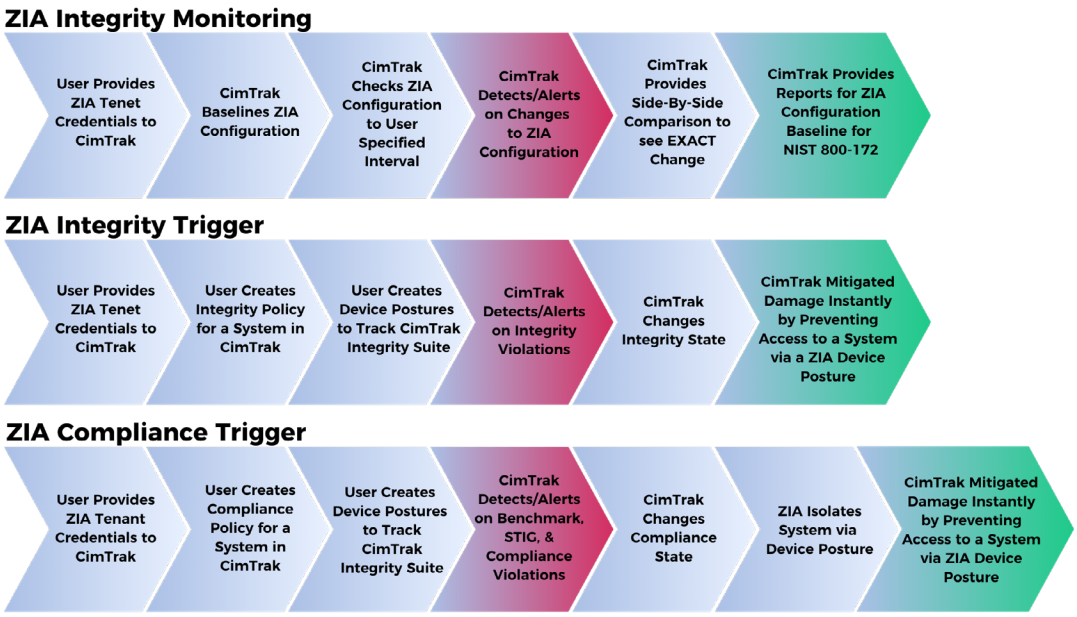
The Solution

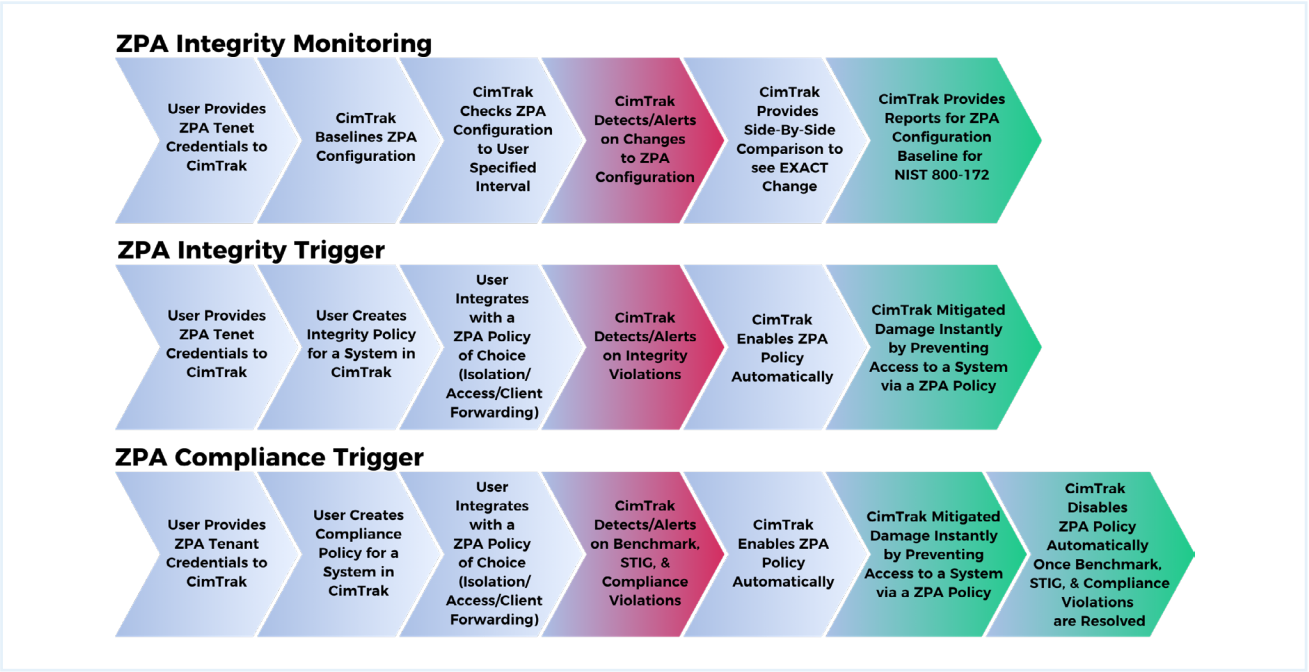
The integration of CimTrak and Zscaler creates a powerful synergy that significantly enhances the protection of your environment. CimTrak's real-time detections and alerts can be used as triggers to initiate automated, targeted policies in Zscaler. This enables swift action in response to critical security events, changes in a system's hardening status, or when the system fails to meet DISA STIGs/CIS Benchmarks. By leveraging CimTrak's immediate awareness of these events, you can take quicker actions within Zscaler, such as locking down specific environments, restricting access to infected cloud applications, isolating suspicious users, and more!

Key Features

- **Change detection:** CimTrak can detect integrity or compliance deviations throughout the environment and provide awareness, forensics, and audit logs for these unexpected changes.
- **Hardening/compliance:** CimTrak can scan systems for secure, hardened configurations and if they meet or beat best practice standards from CIS or DISA.
- **Access management:** Zscaler can manage and restrict which users, systems, and networks have access to within the environment.
- **Security automation:** The integration leverages CimTrak's ability to detect unwanted changes, unexpected changes, threats, or if the systems are in a hardened and compliant state to then automatically enable/disable specific Zscaler policies to change or prevent access to these machines that are no longer in a state of Integrity or Compliance.
- **Zscaler configuration monitoring:** CimTrak can also audit and log when changes are made in Zscaler; alerting on any policy, user, or configuration deviations. Side–by–side comparisons are offered to show exactly what settings/values were modified.

"Together Zscaler and Cimcor help organizations protect their critical IT infrastructure by detecting and mitigating unauthorized changes, ensuring compliance, and ensuring secure access."





Use Case 1

CimTrak + Zscaler Internet Access (ZIA) Integration

Violations of Integrity Triggers

CimTrak's ability to detect files (or other objects) being added, deleted, or modified enables the triggering of policies within Zscaler Internet Access (ZIA). CimTrak can now trigger ZIA rules to isolate a system from joining the ZIA network. By analyzing the system integrity of an endpoint and determining its security posture, this integration allows ZIA to remove that newly compromised system from the network. Whether it's a new threat file being added or a critical configuration file that changed, any CimTrak integrity rules that get violated can enable this automation.

Use Case 2

Violations of System Hardening + Compliance Triggers

With this integration, CimTrak can trigger Zscaler Internet Access rules to isolate a system from joining the ZIA network when a system's integrity is compromised or fails to meet DISA STIGs/CIS Benchmark hardening standards. With this notification from CimTrak, ZIA can remove that newly compromised system from the network and fully isolate it from the entire environment, preventing additional damage beyond that endpoint. If key system–specific security settings have been modified, or if a system is no longer in an acceptable state according to CIS Benchmarks or DISA STIGs, this integration allows you to ensure that only devices in a "trusted state" are allowed to connect to the network.

Use Case 3

Monitoring the Integrity of ZIA + ZPA

CimTrak can also be used to monitor and measure the integrity and deployment of Zscaler's products. There are a myriad of settings in both ZPA and ZIA. This integration provides an audit trail that includes the specific values of each configuration item for ZPA and ZIA. This visibility can help identify when unwanted or unexpected changes are made to ZPA/ZIA. In addition, it will allow the organization to identify when changes are made without following a standard change management process. Furthermore, this unprecedented visibility can also help mitigate the risk associated with malicious activity targeted at Zscaler products and support operational goals and requirements aimed at increasing availability and the establishment of a resilient infrastructure. This capability helps ensure uptime and proper operation of the Zscaler instance.

CimTrak also helps meet several control requirements of NIST SP 800-172 and other compliance mandates by providing a detailed audit trail with the necessary forensics and corrective actions to ensure that Zscaler ZIA & ZPA are configured in a trusted, secure, and, most of all, expected/approved configuration.

Customer Benefits

- **Real-time integrity monitoring:** Continuously monitor critical files, configurations, and systems and instantly detect unauthorized changes.
- **Compliance management:** Demonstrate compliance with industry regulations and standards and pass audits with automated tracking and reporting of changes.
- **Automated access control:** Ensure all modified, compromised, and non-compliant systems are instantly isolated or restricted from access.

Deliver better business results with Zscaler and Cimcor

Together, Zscaler and Cimcor provide a comprehensive security solution that combines real-time incident detection with automated access control, ensuring that compromised or non-compliant systems can be immediately isolated or restricted:

Download our Zscaler and Cimcor Deployment Guide here.

CIMCOR

About Cimcor

Cimcor develops innovative, next-generation compliance and system integrity monitoring software. Its flagship product, the CimTrak Integrity Suite, monitors and protects a wide range of physical, network, cloud, and virtual IT assets in real-time while providing detailed forensic information about all changes. CimTrak helps reduce configuration drift and ensure that all systems are in a secure and hardened state. Securing your infrastructure with CimTrak helps you get compliant and stay that way. For more information, visit https://www.cimcor.com/cimtrak-integrity-suite

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 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**.

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