



# Zscaler Deployment at Scale: Transforming Enterprise Security with Tanium Integration

Thank you for downloading this Tanium resource. Carahsoft is the official government distributor for Tanium cybersecurity solutions available via GSA, NASA SEWP V, CMAS, and other contract vehicles.

To learn how to take the next step toward acquiring Tanium's solutions, please check out the following resources and information:



For additional resources:  
[carah.io/taniumresources](https://carah.io/taniumresources)



For upcoming events:  
[carah.io/taniumevents](https://carah.io/taniumevents)



For additional Tanium solutions:  
[carah.io/taniumsolutions](https://carah.io/taniumsolutions)



For additional cybersecurity solutions:  
[carah.io/cybersecurity](https://carah.io/cybersecurity)



To set up a meeting:  
[tanium@carahsoft.com](mailto:tanium@carahsoft.com)  
703-673-3560



To purchase, check out the contract vehicles available for procurement:  
[carah.io/taniumcontracts](https://carah.io/taniumcontracts)

# Zscaler Deployment at Scale

Transforming Enterprise Security with Tanium Integration

## Executive Summary

In today's distributed workforce environment, organizations face unprecedented challenges in securing remote and hybrid work models. Traditional network perimeter security is no longer sufficient as users access corporate resources from anywhere, using any device. Zscaler's Zero Trust Exchange provides cloud-native security, but deploying and managing security agents across tens of thousands of endpoints presents significant operational challenges.

**55,000**

Government Agency devices secured in under 30 days

Tanium's partnership with Zscaler demonstrates how enterprise-grade endpoint management can accelerate Zero Trust adoption, delivering measurable ROI through rapid deployment, comprehensive visibility, and automated operations at unprecedented scale.

## The Enterprise Security Challenge

Modern enterprises struggle with several critical security deployment challenges:

### Scale & Speed Requirements

Organizations need to deploy security solutions across thousands of endpoints rapidly while maintaining business continuity and user productivity.

### Operational Complexity

Managing multiple security tools across diverse environments creates operational overhead and increases the risk of security gaps.

### Visibility & Compliance

Organizations require real-time visibility into security posture and compliance status across their entire endpoint ecosystem.

### ROI Pressure

Security investments must demonstrate clear business value through faster deployment, reduced operational costs, and improved security outcomes.

## Solution: Zscaler + Tanium Integration

The integration of Zscaler Client Connector (ZCC) with Tanium's endpoint management platform addresses these challenges through a comprehensive approach that combines Zero Trust security with enterprise-scale deployment capabilities.

### Key Integration Capabilities

#### Scale & Speed Requirements

Tanium empowers Zscaler customers to rapidly deploy ZCC agents across their environments using pre-built packages from the Deploy Gallery. Organizations can seamlessly expand coverage to new user groups while ensuring consistent delivery and monitoring deployment success with actionable insights.

#### Automated Deployment Intelligence

The Deploy Package Gallery continuously monitors Zscaler for new ZCC versions and automatically makes them available for deployment, ensuring timely updates to existing endpoints and automated installation on new or unprotected devices.

#### Smart, Rules-Based Rollouts

Deployment Automation enables organizations to define rules and criteria for progressive rollouts, utilize ring-based deployment strategies for controlled updates, and maintain full visibility into deployment status at every stage.

#### Comprehensive Health Monitoring

Tanium Reporting and Sensors provide deep visibility into the ZCC lifecycle, identifying devices where ZCC is missing or misconfigured, monitoring agent health and compliance, and pushing configuration updates to ensure Zscaler protection is always active and effective.



## Proven Results: Government Agency Case Study

The Government Agency's successful deployment demonstrates the power of the Zscaler–Tanium integration at government scale:

**55k**

Devices Deployed

**<30**

Days to Complete

**100%**

Deployment Success

**24/7**

Monitoring Coverage

### Business Impact

This deployment enabled the Government Agency to achieve rapid Zero Trust implementation across their critical infrastructure while maintaining operational continuity. The combination of Tanium's deployment capabilities with Zscaler's security platform delivered measurable improvements in security posture, operational efficiency, and compliance readiness.

## Strategic Value Proposition

The Zscaler–Tanium integration delivers strategic value across multiple dimensions:

- ✓ **Accelerated Time-to-Value:** Reduce deployment timelines from months to weeks through automated, intelligent rollouts
- ✓ **Operational Excellence:** Minimize IT overhead through automated monitoring, updates, and configuration management
- ✓ **Risk Mitigation:** Ensure consistent security coverage with real-time visibility and automated remediation
- ✓ **Scalable Architecture:** Support enterprise growth with proven capability to manage tens of thousands of endpoints
- ✓ **Cost Optimization:** Reduce operational costs through automation while maximizing security investment ROI

## Proven Results: Government Agency Case Study

The integration of Zscaler and Tanium represents a fundamental shift in how enterprises approach Zero Trust security deployment. By combining Zscaler's industry-leading Zero Trust platform with Tanium's proven endpoint management capabilities, organizations can overcome traditional deployment barriers and achieve security transformation at unprecedented speed and scale.

This partnership enables organizations to deploy, manage, and maintain ZCC agents with unmatched speed, precision, and control, all while reducing operational overhead and maximizing security posture. The result is a comprehensive solution that addresses the full lifecycle of Zero Trust security implementation, from initial deployment through ongoing management and optimization.