

# Midwestern State Protects its More Than 30 Departments with Zscaler

## State also centralized and simplified its IT operations

As a large midwestern state was consolidating its network operations, the leadership team recognized the opportunity to adopt a modern, managed services approach for IT across the state. Its goals were to improve efficiency, reduce the time to deploy new tools and services, and strengthen and standardize cybersecurity, which is a top priority for every public sector organization.

### The challenge: Complexity equals risk

Previously, each statewide department was responsible for its network connectivity and IT infrastructure. Each department deployed different policies and security levels, all managed by various groups. The complexity of all these systems significantly increased the risk of a cyberattack.

As the state consolidated IT systems, the Department of Administration (DOA) assumed responsibility for the network, shifting to a modern “as-a-service” approach. The team created a service library, enabling departments to opt-in and quickly deploy proven, trusted IT tools and services.

### Wanted: Enterprise-grade web security

In conjunction with these efforts, the state wanted an adaptive, enterprise-grade web security solution it could deploy as a shared service. It needed to reduce costs as it had multiple appliances deployed across departments, which were expensive to manage and operate. And, it needed to improve redundancy and move away from a single dedicated gateway for web traffic.

After extensive evaluation using a matrix comparison, testing, and pilot implementation, the state selected the Zscaler Web Business Bundle, adding the solutions to its IT service catalog. The suite provides the web security stack as-a-service for all users, on and off the network, at more than

800 local and remote sites. The solution includes authentication, real-time cloud security updates, URL filters, advanced threat protection, anti-spyware tools, cloud application visibility, and cloud and social media controls—all designed to protect employees from malicious web content.

### Why Zscaler?

Zscaler provides global controls and more granular local policy controls, enabling individual agencies to define policies based on unique requirements. And with its improved inspection capabilities, the state was now able to inspect all SSL traffic. In addition, the solution includes built-in disaster recovery and business continuity with automated failover to additional Zscaler data centers.

Because the suite is deployed as a shared service, the state achieves elastic scalability. It also pays for what it uses, as it needs it, with no massive upfront investment.

### Simplified management, reduced costs, scalable security

The state’s IT leaders took an incremental approach as they deployed the Zscaler suite. The initial rollout went well, encouraging other departments to opt in. The team can deploy components to new departments instantaneously. Today, more than 90 percent of all users are protected, regardless of location or the device they use to connect.

The “as-a-service” approach helps the state manage costs in several ways. First, as the number of users increases, the price per user decreases. In addition, the implementation has reduced management time and associated costs by using a single product suite, and reduced the need for onsite server and appliance administration at remote sites.

## IT takes a village

The state’s IT leaders said involving all the agencies and departments in the evaluation process was important. The matrix comparison of the solution options was also useful. As IT teams in other states consider options, this team recommends careful consideration of the network needs— including routing, egress and ingress, and remote and local office access.

The team believes its opt-in philosophy helped drive adoption success. It did not dictate use. Instead, it demonstrated the value of each implementation – a carrot-vs.-stick approach that proved highly effective.

## Additional value

The selection of Zscaler was largely due to its recent Microsoft Office 365 deployment. The state decided to move to Office 365 for many of the same reasons it later chose Zscaler—increased efficiency, cost reductions, simplification, and operational reductions and improvements. But based on an independent study conducted by Microsoft, the state experienced a more than 20-percent performance improvement to its Office 365 investment due to the peering agreement and arrangement that Zscaler holds with Microsoft. Along with the performance increase, the state also takes advantage of the Zscaler One-Click O365 configuration and maintenance, which eliminates all operational efforts required to maintain updates, port configurations, and performance enhancements required by Office 365 customers.

## What’s next?

The state continues to explore additional protection for itself and its users, including exploring zero trust options to reduce the risks from unmanaged devices and lateral access.

The shared service model and successful implementations to date have created a consistent, scalable web security infrastructure across all state agencies. This has resulted in highly productive team members with access to mission-critical applications regardless of location or device, and a platform that enables continued evolution of the state’s IT infrastructure and cybersecurity defenses.

### About Zscaler

Zscaler enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100-percent cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multitenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at [zscaler.com](https://www.zscaler.com) or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

## WINS

### Office 365 performance improvements

– The state experienced a more than 20-percent performance improvement to its O365 investment due to the peering agreement and arrangement that Zscaler holds with Microsoft.

### Increased user protection

– More than 90 percent of all users are now protected, regardless of location or the device they use to connect.

### Checking all the boxes

– Zscaler met all of the state’s project requirements – reduce costs, improve redundancy, and improve inspection capabilities, allowing the state to inspect all SSL traffic.

### More productive employees

– The consistent, scalable web security infrastructure across all state agencies resulted in highly productive team members with access to mission-critical applications regardless of location or device.

