DoIT
Illinois Department of
Innovation & Technology

When the Cicadas Fade, Security Concerns Still Remain

Cybersecurity

State of Illinois
Jason Bowen
Chief Information Security Officer
Jason.Bowen@illinois.gov

Initiation Date: 03.01.2022
End Date: 01.15.2023

EXECUTIVE SUMMARY

The State of Illinois has been actively modernizing its internet access system, moving away from siloed legacy infrastructure and toward a more secure and centralized environment. This transition has been a key success story for the Illinois Department of Innovation & Technology (DoIT). The adoption of the Zscaler platform across State agencies has allowed Illinois to embrace a cloud first strategy, enhancing user experience, improving performance, optimizing network cost savings, and enhancing the security posture. This implementation enables significant progress towards Zero Trust Architecture. With this system, DoIT has streamlined response to potential concerns in the environment, protected against advanced phishing attacks, and enabled a zero-trust policy across network access.

Transitioning to Zscaler Internet Access (ZIA) for Secure Internet and Security as a Service solution is part of a comprehensive security enhancement program. Its goal is to advance IT security, operations, and end user efficiency by maturing cyber capabilities while preparing and planning for the future of cybersecurity throughout the State's environment.

IDEA

Prior to this initiative, the State faced numerous obstacles with over 60 internet gateways resulting in several challenges. Administration of these disparate systems required changes to be made in each system, making it inefficient and prone to errors. Lack of centralized blocking capabilities hindered DoIT's ability to quickly respond to security threats. Furthermore, performance was often subpar, and usage data was scattered across multiple consoles, making it challenging to gather comprehensive insights. The costs associated with maintaining these legacy systems were also increasing. Finally, the "allow" and "block" lists were ad hoc, inconsistent, and not informed by wider cybersecurity awareness.

Implementing ZIA helped remove hardcoded proxy settings in applications and servers, thus routing internet traffic at the firewall, simplifying both the application and server configuration maintenance. ZIA implementation enabled sunsetting of the 63 web gateways and standardized and centralized operations support for internet virus protection.

This initiative is crucial because it streamlines administration, enhances incident response capabilities, improves performance, centralizes usage data, reduces costs, and establishes a more robust and uniform approach to cybersecurity. The adoption of a centralized internet gateway solution not only addresses the existing problems but also sets the foundation for a more standardized, efficient, and secure internet infrastructure in the State's environment.

IMPLEMENTATION

After evaluating several products, DoIT concluded that implementing ZIA would be the ideal solution. ZIA offers several benefits to the enterprise, including the ability to prevent cyberthreats and data loss using Artificial Intelligence (AI). This AI technology leverages real-time updates from 500 trillion daily threat signals, sourced from the Zscaler's global security cloud.

By implementing ZIA, DoIT has modernized its platform and provided administrators with a unified console, reducing the administrative burden, and creating a central location for incident response. As a cloud-based solution, it has streamlined architecture and increased internet access speed in a secure manner. It has also eliminated the need to route all traffic back to the State's infrastructure. However, rolling out a project of this magnitude to 66,000 end users could be disruptive. To ensure a seamless transition, DoIT's team of professionals developed a detailed rollout plan with an agency-by-agency approach. DoIT prioritized reviews and buy-in from each agency and conducted thorough testing in each environment.

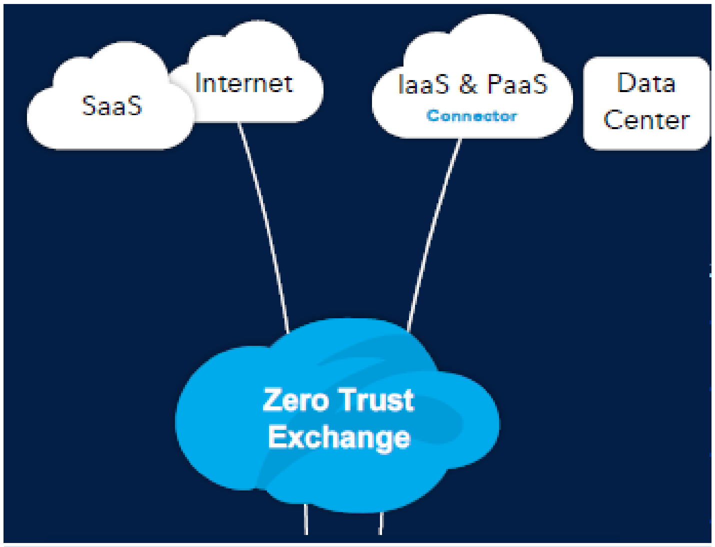
Here is a high-level overview of the project plan:

Phase 1: Design

- Complete design
- Document design
- Design migration strategy
- Design test strategy

Phase 2: Build and Test

- Build
- Configure traffic forwarding
- Configure authentication
- Configure policy structure
- Configure reporting
- Test
- Internal IT testing
- Test key applications
- Test business process



Secure Transformation with Zero Trust Exchange

Phase 3: Traffic Roll Out

- Per agency pilots
- Select users, 1 site, up to 10 users
- Production
- Rollout to multiple sites and mobile users

Phase 4: Legacy Gateway Decommissioning

- Per agency test and decommission

Phase 5: The implementation of the plan centered around an Agile-Lite methodology that utilized:

- Training agency IT Champions
- Functional applications testers
- Rollout to state agency staff
- Technical staff that migrated from the project (Dev) to the Security Operations Center (Ops)

By following this phased deployment plan and addressing the unique challenges of the State's environment, the DoIT security team aimed to provide a seamless transition to the new platform. The rollout to over 65 agencies was completed in approximately 10 months.

DoIT's implementation of ZIA has significantly improved the provision and management of uniform and secure internet access in the following ways:

- Security monitoring tools and phishing reports inform a universal response. The teams can dynamically, if a host or set of hosts are deemed too high a security risk, block and/or route traffic. This protects the environment from bad actors.
- Enterprise policies are consistently and uniformly applied enterprise wide.
- DoIT can provide a more consistent experience to its wide customer base.
- Multifactor/Multidevice Authentication was implemented for all remote IDs and devices accessing the State network remotely.
- Configurations are now informed by the global cybersecurity community and shared information.

Additionally, ZIA has enhanced DoIT's Security Operations Center (SOC) by providing access to web insight logs, which allows analysts to prioritize detections based on threat severity and scores. The SOC can now manage and report on time-to-investigate and time-to-respond, optimizing workflows and investigations. ZIA logs are ingested into the Security Information and Event Management (SIEM) tool for all malware and advanced threat detections within the ZIA security engines. ZIA also offers advanced C2 (command and control) detection capabilities through automation and machine learning, protecting against malicious use of multiple C2 profiles utilized by threat actors.

The implementation of ZIA has significantly enhanced the security and stability of DoIT's architecture. Administrators now have the capability to utilize pre-defined cloud firewall and DNS control, which enables the implementation of industry best practices and the delivery of high-security protections. This includes the ability to block unwanted DNS tunnels, malicious domains and IPs, as well as disrupt botnets.

This program can automatically remove higher risk newly registered, newly activated, and newly observed domains before malicious attackers can gain access to the State's environment. This helps to proactively safeguard the State's systems against potential threats.

The implementation of ZIA has provided improved visibility into endpoints, allowing for the identification and removal of orphaned credentials. This includes outdated credentials such as usernames and passwords, authentication tokens, connection strings, and password hashes that may be present in files, registry memory, cache, configuration files, credential managers, and browsers. By reducing the State's internal attack surfaces through credential cleanup, DoIT is better equipped to deter the efforts of attackers and identify potential lateral movement paths.

ZIA complements the State's existing suite of tools, such as Active Directory and Okta. It can monitor for risks such as changes to permissions, to flag potential threats, and enrich identity profiles with metadata and context from Okta. They can also take built in response actions on identities, such as suspending, clearing user sessions, or deactivating the user via Okta.

Overall, the implementation of ZIA has greatly strengthened DoIT's technical architecture, ensuring a more secure and consistent experience for their customers.

IMPACT

Through the deployment of ZIA, DoIT's Security team has transformed the cybersecurity landscape, providing enhanced protection, improving network performance, simplifying operations, and delivering a scalable solution. State employees rely on being able to access their state resources quickly, securely, and confidently.

ZIA ensures that those connections are made in a way that provides us the ability to protect those resources, trust that they are operating securely and quickly in order to provide the residents of Illinois with the best service possible. Through the deployment of ZIA, DoIT has been able to increase their visibility through the ZIA analytics map. The security posture of this data provides a view into DoIT's data not available before:

- Over 60,000 users and devices are utilizing this tool meaning the core of DoIT's infrastructure is more secure from internet intrusions than ever before.
- API connections feed directly into security applications, allowing DoIT to collect, filter, and monitor activity on the network more efficiently.
- This system monitors over 1.2PB of traffic through three Zscaler DCs, and SSL inspects over 3.5 million threats every quarter, ensuring systems are accessing the internet securely.
- Zscaler ensures secure private application access processing 16.9K users and over 1.08 billion transactions.
- Administrators gain a more enhanced digital experience as ZIA monitors over 60,000 users in nearly 40 geographical locations who are accessing 13 applications with 309 software solutions.

This project exemplifies DoIT's commitment to leveraging innovative technologies to address critical challenges and provide secure and efficient services to our customers. DoIT believes that the ZIA project showcases the State's "whole of state" concept, DoIT's leadership in cybersecurity, and the team's dedication to leveraging technology for the benefit of Illinois residents. Here's what a user is saying:

"The implementation of the Zscaler Internet Access solution for DOC proved to be difficult but was accomplished with the creative collaboration between the business area staff, technical staff and vendor technical staff.

The primary issue resolved with the policy that correctional officers are not allowed to carry cell phones into our facilities; and incoming calls are routed through a central switchboard. This precluded the use of smartphones or desk phones. Solution was reached with the use of security question and answer; with a future solution of Yubikeys for the state correctional officers.

Some creative configuration solutions to support inmate access to training (GED and job skills materials) allowed secure usage of the DOC devices in the facilities. The solution provided for the rotation of the correctional officers to the correctional cell blocks, allowing correctional officers to securely access multiple devices in a correctional facility.

The project methodology used allowed for agile response to issues exposed during each of the 20 rollout waves; that covered the State of Illinois Administration 68 Agency/Board/Commission organizations with over 65,000 devices/ID's. This effort allowed us to sunset 18 Internet Virus Servers (appliances) running the previous internet virus solution, replaced by the Zscaler ZIA cloud services. Additionally, this effort consolidated 124 security policies specific to our organizations into seven Enterprise Zscaler Groups."

- Jerald Setnicky, Deputy Chief Information Officer, Illinois Department of Corrections, 10,380 Devices/ID's

Looking ahead, DoIT will focus on implementing a comprehensive maintenance strategy that includes regular updates and enhancements to adapt to evolving technology and cybersecurity landscapes. This will enable DoIT to stay ahead of potential threats and ensure the project's long-term success. Further, DoIT will prioritize ongoing training and education for team members to ensure they have the necessary skills and knowledge to effectively manage and maintain the project. By investing in their professional development, DoIT can guarantee a high level of expertise and efficiency in handling any challenges that may arise.