DoIT

Illinois Department of
Innovation & Technology

The Zero Trust League Superheroes of Cybersecurity

Cybersecurity

State of Illinois
Adam Ford
Chief Information Security Officer
Adam.Ford@illinois.gov

Initiation Date: December 2021
End Date: May 2023

Executive Summary

Information Technology is full of buzz words, marketing hype and jargon. Ten years ago, which of these categories the term “cloud” fit into was largely dependent on who was using the term. Jokes like “cloud, someone else’s computer” summoned easy laughs during group presentations. But as in a good superhero movie, the whispers of cloud grew and echoed across the landscape and technology heroes began to understand the new powers, and responsibilities, that cloud computing truly offered. During the COVID-19 pandemic, states, including Illinois, rapidly adopted cloud technologies to solve new problems and deliver critical services to residents. Long forgotten are the easy jokes.

Following a similar, but slightly delayed trajectory, is the concept of zero trust security computing. Despite being described by NIST SP 1800-35, zero trust is still often used as a buzz word on marketing materials. As was the case with cloud computing, advocates of a zero trust architecture have watched their “hero” rise from a joke to a real-world solution to an ever, more hostile cyber threat landscape. Organizations able to harness and begin the journey to a zero trust security architecture are finding themselves able to solve problems faster, with more transparency and more security.

The zero trust implementation at the State of Illinois requires all users to be authenticated, authorized, and continuously validated before being granted access to applications and data. The Department of Innovation & Technology (DoIT) has been working to improve security technology capabilities that enable zero trust architectures. In the past two years, DoIT has rapidly implemented projects and programs to harden security and build the foundation for moving to zero trust in Illinois. By embracing modern security platforms, working diligently to improve the quality of the information available to make security decisions and setting zero trust architecture as a cybersecurity NorthStar, the State of Illinois has begun to leverage zero trust technologies to accelerate modernization and provide more secure, more user-friendly solutions.

Idea

When the State of Illinois adopted an “assumed breach” mindset in 2021 due to the increasing frequency and severity of cybersecurity attacks such as SolarWinds and Colonial Pipeline, one of our largest constraints was our legacy approach to internet filtering. The State had operated an internet filtering system for more than ten years which relied upon network routing and firewalling to ensure that users from each customer agency were directed to the specific web proxy servers configured for their agency. This dependency constrained Illinois from simplifying our technology operating model and required expansive use of network virtualization, multiple firewalls and network-address based server environments.

Moving to a zero trust architecture was critical for the State of Illinois, like other states, to be able to effectively defend against increasingly complex cybersecurity attacks. Additionally, Illinois needed to be able to simplify its operating environment to make more efficient use of scarce employee and fiscal resources. Technology business practices which require large amounts of expertise and staff time create cyber risks through their very existence. Working harder not smarter, spreading our workplace thin and continuing to support complex legacy topologies keeps states focused on technology as an end rather than operating technology to drive resident services.

Zero trust architecture is one of the rare cybersecurity concepts that not only improves security but also improves user experience and increases our agility and ability to meet the technology needs of the next ten years, not the last ten years.

By adopting a zero trust technology to remove the State of Illinois' dependence on network-based security to address internet filtering, the State positioned itself into a rapid transition posture that enabled us to simplify our networking environment, improve the access control to agency applications, and monitor user activity for malicious behavior. It also positioned us to implement increasingly mature context-based Multifactor Authentication (MFA) and other security controls based upon risks and the criticality of the system being accessed.

Implementation

Implementation of zero trust architecture is like starting up an official group of superheroes. The Incredible Hulk had been smashing for a long time before being asked to join the Avengers. Professor X ran a school for mutants before founding the X-Men. Zero trust combines, refines, and repurposes many technologies and processes already underway. Like many states, Illinois had been operating Microsoft Active Directory/Azure Active Directory to organize, catalog, distribute software and assign policies to the computers our users rely on. In 2020, we implemented OKTA SSO to provide a centralized user interface to multiple on-premise and cloud-hosted applications which leveraged MFA and risk-based access techniques. Also in 2020, we migrated from an on-premise SIEM to Splunk cloud, which combined security and operational log management capabilities and reporting. Some of the Avengers were already assembling.

We were lacking a solution that could help us get to user-based internet filtering without relying on the network-based security approaches that had driven our designs for the previous 15 years. We were in the same place that a lot of large organizations get to; our best and most reliable product (network-based security) just didn't meet the needs of the modern world. Like a landline telephone, or the telegraph before it, network-based security was keeping us stuck at home when we really wanted to be out with the other superheroes, saving the day. So, we asked for help, from other states, from consultation services, and from industry. How was the rest of the world addressing internet filtering without relying on network-based security?

The answers we got back were surprising and discouraging. The rest of the world was moving to a model that relied upon a desktop client to direct user internet traffic to (GASP!) the cloud where the filtering and security services that we had built our environment on were performed. We would be bypassing 15 years of blood (paper cuts), sweat (sitting on the vent side of a switch is hot), and tears (no explanation needed) by going around the network security appliances we'd come to know and love. Humor aside, building a consensus from our technicians, architects, and key users required many whiteboard sessions, Webexes, and meetings. It also required intense and honest discussion about the assumptions we had made about how complex our environment needed to be to meet our users' needs. The technicians and engineers who support the State of Illinois are the real heroes in our story and as in most good superhero movies, the decision to join the Zero Trust League required a lot of soul-searching. Change is always hard, and radical change is incredibly hard. Moving from network-based security to true zero trust architecture is like sending your kids to college and selling the home you raised them in.

After the soul-searching, the Illinois team got to work on the implementation. A plan was built to get the Zscaler Client Connector deployed to each of our agency workstations and schedules were built. As agency communications were prepared, DoIT made one other key decision related to the rollout of Zscaler that impacted the rollout. In the legacy network-based security design, each agency was able to leverage customized block and permit lists based upon categories and URLs. While this sounds quite reasonable, the approach implemented in 2008 had turned into an unwieldy villain due to the modernization of websites. DoIT security and operations teams were spending a substantial amount of staff time working with end users to make available access to sites that had been miscategorized. The decision was made to simplify and standardize the internet filter approach to focus on sites that were harmful rather than operating a complicated environment to manage employee time abuse. Reporting using Splunk and native tools was provided to customer agencies to do their own employee management, but the DoIT team was focused on protecting the data and systems of the state of Illinois. Superman can absolutely call balls and strikes better than any MLB umpire, but he has more important things to do.

2000-2020

- Implemented and operationalized Microsoft Active Directory

2020

- Converted from on-premise SIEM to Splunk Cloud
- Implemented Okta and synced AD accounts with OKTA

2021

- Accelerated adoption of OKTA SSO for on-premise and cloud-based applications
- Conducted internal and external evaluations of solutions to replace network security-based internet filtering
- Began procurement process for Zscaler Internet Access (ZIA) solution

2022

- Testing of ZIA was successful, and rollout began to approximately 50 agencies, boards, and commissions across the state.
- Conversion of internet filtering from unique to standardized implemented on legacy solution as well as new solution

2023

- April 2023: ZIA rollout completed for all agencies
- April 2023: Zscaler (ZPA) rollout began with all agencies with possible access to federal tax information, which replaced our current VPN access and required all users to authenticate with their OKTA account before gaining access remotely
- May 2023: ZIA rollout complete

Impact

Implementation of ZIA at the State of Illinois has had significant impact on security operations and technical agility and has fostered a shared vision of what the network of the future looks like at DoIT. Assumptions have been challenged and restrictions overcome. The soul-searching part of our story has helped employee morale because it involved personal engagement between so many team members to envision a future that was radically different from the past.

The number of user generated tickets related to internet access problems has plummeted from over **90%** of Security Operations Center (SOC) tickets pre-ZIA and now make up around **10%** of tickets. This reduction in ticket volume allowed the SOC to focus on improving detection and response in other key security areas **(WHAM!)**.

User experience was also greatly improved. Our legacy filtering technology had been designed for a simpler internet 15 years ago and was ill-equipped to address the complicated web sites of 2023. This meant that portions of web pages would be blocked, and the SOC had to often bypass filtering on sites to get users working again. This environment was frustrating to our users and bypassing security controls as a regular solution to any problem is greatly undesirable.

As noted in the timeline above, DoIT had already experienced a radical acceleration in our ability to transform our technology environment. During the month of April 2023, DoIT was able to convert 12,000 remote users from a legacy VPN solution to a more user-friendly, secure, remote access solution by implementing Zscaler ZPA. From initiation to completion, this migration took three weeks. The change allowed users to leverage the already familiar OKTA MFA solution that they use for ZIA and many other applications rather than needing to learn another MFA approach. Consistency in user experience with MFA made it easier for DoIT to expand MFA adoption. The migration was able to be accomplished because it was built on the zero trust foundations laid prior to April 2023 **(BAM!!).**

Beyond the operational and security improvements, this project has emboldened the superhero technologists at DoIT to see our environment in a new way. As problem solvers, many of them had felt boxed in by the complicated network-based security configurations that had been built and maintained. Implementation of ZIA challenged them to not just think outside of the box but to fly out of the box and be empowered to drive radical changes to our environment (**KAPLOOEY!!!).**

The project has been a success by reducing support requirements, improving user experience, and unlocking our users from network security dependencies. DoIT plans to expand deployment of ZPA to all devices which will allow for the disassembly of the complicated and difficult to manage legacy network-based security stack. With several of the key building blocks already in place to accelerate into zero trust, Illinois is positioned to rapidly take advantage of improvements in our data governance and classification practices. Improvements within identity and access management, asset management and application management can be integrated rapidly into authorization decisions (**SLAM-DUNK!!!!)**.