How Fairfax County Simplified and Amplified its Security Strategy with Zscaler Workload Segmentation

Fairfax County

Location: Virginia, USA

Industry: State and Local Governments

Customer Size: 12,000 government employees

Fairfax County is located in Northern Virginia and employs more than 12,000 government employees. Founded in 1742, Fairfax County is the most populous county in the Commonwealth of Virginia with more than 1.1 million citizens—approximately 13 percent of Virginia's population. With a mission to "protect and enrich our quality of life for people, neighborhoods, and diverse communities," Fairfax County is responsible for overseeing elections, tax collection, public education, social services, law enforcement, fire and rescue, transportation, and parks and recreation.

The imperative to reimagine security strategy to minimize complexity

With cyberattacks on the rise, especially those targeting the government sector, Fairfax County recognized the need to reimagine its security strategy. It had hundreds of applications in the data center and in Azure that needed to be protected, and the county wanted to reduce its network attack surface and decrease the risk of breaches by protecting east-west traffic inside the data center.

The next generation firewalls (NGFWs) it was using to protect its data were becoming suboptimal, with hundreds of applications resulting in thousands of policies and creating unnecessary complexity. With a small, centralized IT team, Fairfax County needed to minimize complexity with a **zero trust solution** that was easy and seamless to deploy, monitor, and manage.

CHALLENGE

- Stop lateral movement of threats, while reducing firewall-induced complexity, to expand the existing zero trust approach

SOLUTION

- Zscaler™ Workload Segmentation
- Zscaler Zero Trust Exchange™ platform
- Zscaler Internet Access™ (ZIA™)
- Zscaler Private Access™ (ZPA™)
- Zscaler Cloud DLP

OUTCOMES

- Protected all 2,000 production systems on premises and in the cloud
- Simplified policy creation, monitoring, and enforcement
- Eliminated tedious troubleshooting tasks enabling IT to focus on business-critical needs
- Gained visibility into application communications
- Reduced burdens on lean IT staff, enabling it to effectively manage multiple products and projects simultaneously

Securing east-west traffic through microsegmentation

"Our main issue was the east-west traffic," explained Gulzar Khan, IT Program Manager for Fairfax County. "We had deployed over 150 VLANs, but still close to 80 percent of our traffic was east-west traffic. So we wanted to find a solution to protect that east-west traffic and minimize the impact if there's an instance of compromise."

Microsegmentation, when done correctly, prevents the lateral movement of threats across flat networks inside cloud and data center environments and originated as a way to moderate traffic between servers in the same network segment. It has evolved to include intra-segment traffic so that server A can talk to server B or application A can communicate with host B, and so on, as long as the identity of the requesting resource (server/application/host/user) matches the permission configured for that resource.

But historically, microsegmentation has been a cumbersome and complex process because firewalls have been used to create the microsegments. As segments get smaller, the firewall rules become impossibly complex. Furthermore, every application is different and organizations have to learn the nuances of every application and build custom policy sets, which introduces complexity and can take months. Fairfax County started looking for a solution that could help to address its security concerns and reduce complexity while also being deployed quickly and easily.

Gaining AI-enabled automation with Zscaler Workload Segmentation

Fairfax County found the solution in **Zscaler Workload Segmentation**, which runs seamlessly independently or as part of the **Zscaler Zero Trust Exchange platform**. The County favored Workload Segmentation because it's not an evolution of a firewall. Rather, it's a purpose-built solution engineered to dramatically simplify microsegmentation by using the identity of software and machines and by automating the entire policy lifecycle with machine learning. Additionally, Workload Segmentation protects applications in both Azure public cloud and on-premises physical servers, increases visibility into application communications, deploys easily, and simplifies creation of segments and policies.

Although it had previously established a zero trust network access (ZTNA) approach with **Zscaler Internet Access (ZIA)**, **Zscaler Private Access (ZPA)** and **Cloud Data Loss Prevention (DLP)**, Fairfax County conducted a comprehensive market evaluation. Ultimately, expanding its Zscaler Zero Trust Exchange platform proved the right solution.

"We looked at multiple products and eventually decided to go with Zscaler Workload Segmentation," Khan said. "We selected the solution because it had superior machine learning capabilities that were much better than other products that we tested.

> "The Zscaler team assisted us with understanding the policy creation process, mapping between servers, and troubleshooting any issues. They were very knowledgeable and helpful."
>
> **– Gulzar Khan**
> IT Program Manager
> **Fairfax County**

©2021 Zscaler, Inc. All rights reserved.

Once the agent was installed, machine learning helped us discover all the processes running on our systems, and when we deployed the whole segment, it identified communication between systems within, coming into, and going out of the segment. It was very helpful for us to learn more about our applications."

Simplified policy creation, monitoring, and management through machine learning

Based on the cryptographic identities of all software and machines communicating on your networks, **Workload Segmentation** eliminates risk by building policy recommendations using patented machine learning technology. Identity-based microsegmentation significantly reduces the number of policies required to protect a segment -- what previously took 100s of policies can now be protected with as few as 7 policies. All software updates are captured instantly, eliminating the need for manual policy creation and management.

"We liked the machine learning aspect of Workload Segmentation, but we also liked the policy creation process for its simplicity," Khan said. "It's basically a few clicks—once a segment is created, you just click on auto-segmentation and that will begin a policy creation process. Once you create a policy, the next step is to troubleshoot any blocks. Overall it was a pretty simple process."

Streamlined agent-based deployment and bypassing automatic host segment creation

Though Khan said he is very selective about **agent-based solutions** because they can be complicated and take extra time and effort to deploy, Workload Segmentation's agent-based deployment allowed for more flexibility and easier management. Fairfax County's workloads are distributed between the cloud and physical servers, and Workload Segmentation was able to streamline deployment regardless of workload location.

"We can deploy these agents to all these distributed workloads for easy management," Khan said. "That was a big plus for us."

One of the benefits of working with Zscaler is that organizations have the freedom to choose and customize their solution based on the organization—teams can be as hands-on or hands-off as they choose. In Fairfax County's case, the team wanted to use their own knowledge to create their own host segments.

"Once the agent was deployed, our next process was to start setting up host segments," Khan said. "Zscaler Workload Segmentation automatically creates host segments, but we decided to use our knowledge and our environment to create our own host segments. Once we were done with the host segments, we let the system run for a couple weeks to discover all the traffic—ingoing, outgoing, and traffic within the segment."

> "The Zscaler Workload Segmentation policy creation process is super simple. It's basically a few clicks."
>
> **– Gulzar Khan**
> IT Program Manager
> **Fairfax County**

©2021 Zscaler, Inc. All rights reserved.

After that, the IT team started working sessions with Zscaler's Workload Segmentation team. Khan explained that these working sessions helped the team understand the policy creation process and mapping between servers and learn how to troubleshoot any potential issues with those policies.

Charting a path for the future

Fairfax County is in the final stages of setting up host segments, though there is still much to learn and accomplish to finalize the Workload Segmentation implementation.

"We are not done yet. We are still in the process of troubleshooting and going over all our host segments," Khan said. "We are still working to understand all those host segments and get policies in place. Eventually, once we are comfortable with all those learnings and processes, then we'll engage the application teams so we can start enforcing, testing, and verifying those policies. We've made pretty good progress and we're close to completion."

The ultimate goal, however, is to get rid of legacy technology and ensure their network is secure. "Our goal is starting to sunset those firewalls," Khan said. "Firewall rules have caused multiple problems and we've had to spend a lot of time troubleshooting them."

> "We can deploy these agents to all these workloads for easy management. That was a big plus for us."
>
> – **Gulzar Khan**
> IT Program Manager
> **Fairfax County**

Achieving goals securely and broadening horizons

Fairfax County, Virginia, has a mission to protect and enrich quality of life for people, neighborhoods, and diverse communities, but it needed the right security solution to protect these initiatives. Zscaler Workload Segmentation allowed the county to protect its sensitive data, both in the data center and in the cloud, while lessening the burden on the IT team, increasing visibility, and reducing complexity.

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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

©**2021 Zscaler, Inc. All rights reserved.** Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, and ZPA™ are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners. V.031820

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com