FEDInsider

DATASHEET

How To Best Achieve Microsegmentation for State, Local & Educational Institutions

Breaking systems and networks down into tiny little pieces using microsegmentation can be a huge boon for Cybersecurity SLED defenders

Government agencies at all levels are adopting Zero Trust to better protect their networks from cyber threats. Part of that process includes implementing microsegmentation to reduce the attack surface and prevent lateral movement from an adversary. If each microsegment has its own security policies and is only accessible to authorized users and devices, a bad actor will have serious trouble moving throughout the network.

Thought leaders from agencies and industry spoke at a recent FedInsider webinar to discuss how they're implementing microsegmentation and its role in deploying a Zero Trust framework.

Breaking It Down: Zero Trust and Microsegmentation

A Zero Trust architecture eliminates implicit trust within an IT system, restricting access to network applications on a need to basis only, and strengthening user authentication to ensure an adversary can't move about a network if they gain access. That's where microsegmentation comes in.

"Microsegmentation offers, from an IT perspective, breaking your infrastructure into many tiny pieces and locking it down such that if there is a breach, the threat actors cannot move from there and demand a ransom," said Dan Petrillo, director of product marketing for the Zero Trust Security portfolio at Akamai.

The best microsegmentation solutions track the flow of traffic in a network, and remove the ability for traffic to connect if it can't be relied on – eliminating further implicit trust.

And realizing the benefits of Zero Trust doesn't just happen at the end of the implementation journey, Petrillo said. "We are seeing a lot of state and local governments, even if they have a five year roadmap towards achieving Zero Trust, getting drastic gains in risk reduction in the first months, weeks or even days of starting their Zero Trust journey," he said.

Zero Trust at the State and Local Level

Adopting a risk-based approach to security is the key to securing state and local networks, and can be a foundational approach to implementing Zero Trust.

David Morgan, information systems security manager for the Texas Department of Public Safety, said that risk-based approaches help to identify what critical assets and services an entity has, and once those are assessed, organizations can then create a list of priorities. "Using Zero Trust as a framework, this can dovetail in there and help provide that support," Morgan said. Having a risk-based framework can also drive continuous improvement.

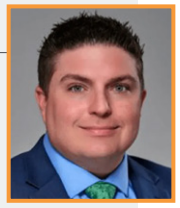
Michael Farrar, chief information officer for the City of Westerville, Ohio, said his town is also on a cloud and Zero Trust journey. "About 75% of all of our applications are now cloud-based, and we have access to everything through the cloud there," Farrar said. Much of this process has been ensuring access to city resources out in the field via various workforce devices.

"We're working on building out those environments to have access to the right resources at the right place at the right time for our staff to deliver the services for our citizens," he said. And to build a trusted network, Westerville created an internal Cyber Command,

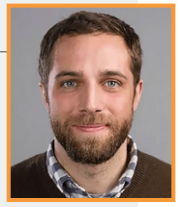
Featured Experts

- **David Morgan**
  IS Security Manger,
  Texas Dept of Public Safety

- **Michael Farrar**
  Chief Information Officer,
  City of Westerville, Ohio



- **Dan Petrillo**
  Director of Product Marketing, Zero Trust Portfolio, Akamai



comprised of a group of people from directors to receptionists in different departments who are designated as first adopters and security champions. "When we have something come out, we communicate through that so their local team can go to them to get information, and they can help pass that around," Farrar said.

The city was also challenged with legacy systems that were unable to be moved to the cloud, but Farrar's team was able to leverage modern technology to build out virtual desktop environments for those legacy systems. "That allows us to wrap around a level of security so that we can go ahead and continue to move forward with our Zero Trust environment and strategy," he said.

And the key to implementing Zero Trust at the state and local level, Petrillo said, is to do so in stages, otherwise "it is too daunting, and you try to boil the ocean." Tie Zero Trust initiatives to specific use cases to get agency buy-in and measure value first. Use cases will eventually follow one after the other, making strides towards full Zero Trust deployment and powerful milestones.

Advancing Zero Trust with Microsegmentation

"One of the most powerful things about microsegmentation when done right is it allows you to work with one control claim despite all the different types of technologies we have to protect," Petrillo said.

Connected devices, hybrid cloud infrastructures, Kubernetes and virtual machines all work together and collaborate, and adversaries can typically move laterally through these assets if they're not protected correctly or use various disparate security tools and control points.

Microsegmentation is software-defined, using either agents or agent technologies, and the data it collects all gets fed into one interface. It provides strong visibility into an environment and how everything is communicating, so users can understand the dependencies and begin to enforce policy against implicit trust where needed.

"Once you have this visibility and an understanding of how your network is operating, it becomes a lot less daunting to enforce these grand policies that are going to affect a lot of assets," Petrillo said. Plus, software-defined projects don't require re-architecture or downtime, and users can start to enforce policies gradually so business can operate as usual.

Taking Microsegmentation to Government

Morgan strongly recommends adopting microsegmentation at the state and local level. For Texas, Morgan said they have the tools and talent to support microsegmentation, which can reduce the attack surface, "so that one shot does not take out the whole network." This helps contain breaches so that single attack attempts don't paralyze the entire state network.

Considering local governments tend to have limited resources, isolating critical systems and identifying and prioritizing the protection of crown jewels allows a locality to continue functioning even if there is a breach.

Farrar said one of the main reasons Westerville wanted microsegmentation was to slow down attacks, detect suspicious activity as soon as possible and to completely isolate their environments to protect its crown jewel assets.

By adopting microsegmentation, Farrar said they've seen real benefits and were able to have a much clearer understanding of the city's network, what assets communicate with each other, and where those communications are going. "It gave us that clear visibility into what we really needed to protect. And it gives us the opportunity to protect infrastructure like a castle and moat, with another castle and moat inside that, and then another one inside that and so on, giving us lots of barriers and extra layers of protection."

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
www.FedInsider.com
@FedInsiderNews
@FedInsider
Linkedin.com/company/FedInsider

Akamai

Akamai Technologies
11111 Sunset Hills Road, Suite 250
Reston, VA 20190

(617) 444-3000
Info@Akamai.com
www.Akamai.com
@AkamaiTechnologies
@Akamai
Linkedin.com/company/Akamai-Technologies