Building a Foundation for Zero Trust

With the widespread adoption of cloud, mobility and related technologies, government workforces are becoming more widely distributed - meaning that agencies can no longer rely on perimeter-based defenses to keep their networks secure. In response to this shift, many cyber experts recommend a zero-trust approach to network access, which applies security measures at the level of individual applications, data or systems. Zero trust is not a technology but a strategy that integrates numerous technologies and policies.

GovLoop, Fortinet and Carahsoft surveyed 105 federal, state and local government employees and contractors about the role of zero trust in their agencies.

BUILDING FOR THE FUTURE

The move to a more distributed workforce predated the COVID-19 pandemic, which forced many government employees to work remotely. Only 22% of respondents said all or nearly all of their agencies' employees are always on site. In contrast:

40%

said most employees work on site, but some telework or work from remote offices occasionally

20%

said most employees work on site, but many work remotely occasionally

19%

said employees were scattered across many different offices

And even apart from COVID-19, remote work will become even more common at most agencies in the next 18-24 months, with 67% saying that the number of employees working outside the office at least occasionally will go up either significantly or somewhat.

A WORK IN PROGRESS

Zero trust is beginning to get traction in government agencies. 36% said it's a current component of their agency's cyber strategy, and 13% said "not yet but likely will be in the future."

But there is a need for more education about zero trust in government.

39%

said they didn't know if their agencies were doing zero trust

28%

said they didn't understand the topic at all

19%

had never heard of it

Decisions about enterprise strategies like zero trust are often made at the executive IT level. Asked how well they think their agency's IT leaders understand the concept of zero trust security:

71%

said very well or fairly well

16%

said their IT leaders probably had never heard of it

13%

had never heard of it

THE BUILDING BLOCKS OF ZERO TRUST

Whether they call it zero trust or not, many agencies are adopting some or all of the building blocks of a zero trust strategy. Those components include:

End user visibility:
Knowing who is on the network at all times

Authentication:
Authenticating both the users and devices before allowing them to access network resources

Device visibility:
Knowing what devices are on the network (whether that device is personal or agency-furnished)

Least privilege:
Allowing users to access only those resources needed to do their jobs

Here is how agencies are doing:

71%

have a very clear or somewhat clear picture of network users

72%

have a very clear or somewhat clear picture of connected devices

63%

don't allow employees to connect their personal devices to the network

76%

authenticate users/devices before allowing them access

69%

enforce a "least privilege" policy

A BLUEPRINT FOR SUCCESS

Zero trust encompasses numerous cyber solutions. Here is a look at how some of the most common solutions are being used today.

Which cyber solutions does your agency use?

71% Network access control technology

54% Network micro-segmentation (internal firewalls)

36% Continuous endpoint protection

68% Identity and access management

50% Centralized authentication services

51% Multi-factor authentication

35% Automated scans of endpoint security state

28% Traffic scanning

SOLUTIONS FOR ZERO TRUST NETWORK ACCESS

The threat of insecure or unknown devices attaching to the network, along with a host of breaches due to stolen credentials, has stretched continued reliance on perimeter-based security beyond the breaking point. Network administrators must adopt a zero-trust approach to network access and data protection. Knowing what devices, data, and users are on your network is foundational to implementing a zero-trust strategy.

Fortinet solutions offer the necessary security to see and control devices and users across the entire network. With proactive protection, organizations can ensure their networks are secure from the latest threats. Key capabilities include:

Endpoint and Device Protection
Identify and secure endpoints, devices and user requests to access the network. Integrated endpoint visibility, control, and advanced protection ensure organizations are secure at the enterprise edge, in the network core, and in the cloud.

Visibility
See and identify every device on the network, profile its behavior, and scan for known vulnerabilities. Validate every request for access—checking both the identity of the user and the trusted state of the requesting device.

Dynamic Control
Leverage tools for dynamic control to implement intent-based segmentation, restricting access to that data needed to accomplish the task at hand and granting the least privilege necessary (read, write, or file creation/deletion) to perform the requested activity.

Learn more at www.fortinetfederal.com

FORTINET govloop carahsoft