Which cyber solutions does your agency use?

Many agencies are adopting some or all of the building blocks of a zero trust strategy. Those components include:

- **Device visibility:** Knowing what devices are on the network (whether that device is personal or agency-furnished)
- **User visibility:** Knowing who is on the network at every moment

In response to this shift, many cyber experts recommend a zero-trust approach to network access, which applies security measures at the endpoint level to ensure organizations are secure from the latest threats.

**The Threat of Insecure or Unknown Devices**

The threat of insecure or unknown devices attaching to the network, along with a host of breaches due to stolen credentials, has stretched reliance on perimeter-based security beyond the breaking point. Network administrators must adopt a zero-trust approach to network access and intent-based segmentation.

**The Benefit of Zero Trust**

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."

36% of respondents said all or nearly all of their agencies' employees are always on site. Only 22% of employees working outside the office at least occasionally will go up either significantly or somewhat.

**The Move to a More Distributed Workforce**

The move to a more distributed workforce predated the COVID-19 pandemic, which forced many government employees to work remotely. Only 22% of employees working outside the office at least occasionally will go up either significantly or somewhat.

**The Widespread Adoption of Cloud**

With the widespread adoption of cloud, mobility and related technologies, 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 and intent-based segmentation.

**The Building Blocks of a Zero Trust Network Access**

- **Device visibility:** Knowing what devices are on the network (whether that device is personal or agency-furnished)
- **User visibility:** Knowing who is on the network at every moment
- **Endpoint and device protection:** Ensuring that only authorized devices can access network resources
- **Authentication:** Authenticating both the users and the requesting device
- **Least privilege:** Granting the least privilege needed to accomplish the task at hand and data needed to accomplish the requested activity
- **Dynamic control:** Leveraging tools for dynamic intent-based segmentation, allowing users to access only the resources needed to do their jobs
- **Network visibility:** Ensuring that only authorized devices can access network resources
- **Security state:** Scanning of endpoint activity before allowing them to access network resources
- **Traffic monitoring:** Scanning of endpoint behavior before allowing them to access network resources
- **Key capabilities include:**
  - Integrated micro-segmentation
  - Dynamic intent-based segmentation
  - Flexible and granular access control
  - Intent-based network segmentation
  - Dynamic control

**A Blueprint for Success**

Zero trust is not a technology but a strategy that integrates numerous technologies and policies. It is foundational to implementing a zero-trust strategy.

**Understanding Zero Trust Security**

Organizations need to create detailed end-user asset management policies in partnership with their agencies' IT leadership to ensure that the right network access is granted. Some 28% of executive IT level respondents said their IT leaders probably understand the concept of zero trust security: 39% said they don't even know if their IT leaders understand it.

But there is a need for more education about zero trust in government. 71% of respondents said their IT leaders probably have a very clear or somewhat clear picture of zero trust. Only 16% said very well or fairly well said their IT leaders probably had never heard of it.

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:

- **Device visibility:** Knowing what devices are on the network (whether that device is personal or agency-furnished)
- **User visibility:** Knowing who is on the network at every moment

Here is how agencies are doing:

- **Device visibility:** 71% Network administrators said most employees work on site, but many work from remote offices or work from remote offices
- **User visibility:** 72% End user visibility: 63% of respondents said all or nearly all of their agencies' employees are always on site

**Solutions for Zero Trust Network Access**

The Zero Trust Network Access solution offers the necessary security to see and control devices and users across the entire network. With proactive protection, Fortinet solutions offer the necessary security to see and control devices and users across the entire network. The solution includes:

- **Device visibility:** 76% of respondents said most employees work on site, but many work from remote offices or work from remote offices
- **User visibility:** 69% of respondents said all or nearly all of their agencies' employees are always on site

Learn more at www.fortinetfederal.com