Government leaders share their views on what is helping or hindering efforts to assess their cybersecurity postures and make progress towards meeting federally mandated zero-trust goals.
Federal agencies have been charged with implementing a comprehensive zero-trust cybersecurity strategy as part of a larger White House Executive Order on Improving the Nation’s Cybersecurity and comparable Defense Department mandates. But agencies face a number of technical and operational challenges in assessing their existing security posture and determining the best paths forward in implementing their zero-trust strategies.

FedScoop surveyed 191 prequalified government leaders to understand what is helping — and hindering — agencies in their efforts to fully assess their cybersecurity posture and develop and manage a zero-trust strategy.

The study also explored how capable agencies appear to be in assessing their overall security posture; the gaps that remain in meeting federally mandated zero-trust security objectives; and what steps they’re taking to close them.
Familiarity with federal zero-trust objectives
Nearly half of all respondents (47%) said they are generally familiar with the core objectives of OMB’s Federal Zero-Trust Strategy or DOD’s latest Zero-Trust Reference Architecture, and roughly 3 in 10 said they are fully familiar.

Maturity in agencies’ zero-trust journey
Using DOD measures of zero-trust maturity — 3 in 10 respondents said their agencies were at the discovery/assessment stage; 1 in 4 had baseline capabilities; 18% had intermediate capabilities; and 17% reported advanced capabilities. Comparing zero trust maturity by agency employee size, a higher share of respondents at midsize agencies had intermediate and advanced capabilities compared to both small and large agencies.

Financing zero-trust work
Budgets
More than half of all respondents said they have a budget line item created for zero-trust work. However, fewer respondents at small agencies said zero-trust has its own budget line.

FY2024 Funding
Zero-trust funding remains uncertain: 6 in 10 respondents who said they were at a “baseline” or “intermediate” maturity level said they were only “moderately confident” that their agency will receive incremental funding for zero-trust work in the FY 2024 budget.

In contrast, 56% of those with “advanced” capabilities said they were “highly confident” they’d receive incremental funding.

Conflicting IT priorities
Respondents also expressed the belief that other high-priority IT projects will suffer in FY 2024 due to the need to reallocate resources to meet zero-trust work, with 43% expressing “moderate concern” and 18% expressing “high concern.”

Who’s leading the effort?
Individual
More than 6 in 10 respondents said their agency has already designated an individual to lead their zero-trust efforts, with the highest portion (70%) of respondents at medium-size agencies compared to small or large agencies.

Office
Of those who said their agency has a designated individual leading zero-trust implementation, that individual most often reports to the CIO’s office at small, medium and large agencies. The CFO’s office was the next most frequently named oversight office, particularly at small agencies.
EXECUTIVE SUMMARY

Realigning existing security programs
Three in 4 respondents are either highly or moderately confident that ongoing security programs can be realigned to meet OMB’s and DOD’s zero-trust goals.

Visibility into gaps
However, 4 in 10 respondents at large agencies, 32% at small agencies and 20% at medium size agencies said their senior leaders do not have visibility into the gaps that must be closed to achieve zero-trust objectives.

Confidence in skills to assess zero-trust pillars
Respondents’ confidence in their agency’s in-house skills to assess the security needs for each pillar of zero-trust varied by pillar and by agency size. Respondents at small agencies said they were highly confident in their “data” skills and least confident in managing “users.” In contrast, respondents at medium and large agencies said they were highly confident in their skills to manage “devices” and least confident with “automation orchestration.”

Value of zero-trust assessments
Nearly 9 in 10 respondents said it would be highly or moderately valuable to conduct a comprehensive zero-trust assessment to identify gaps. Almost as many (8 in 10) believed having a third party makes those assessments would be highly or moderately valuable.

Barriers to implementing zero-trust
4 in 10 respondents said data management was the top staff/skills shortage hindering their agency in implementing zero-trust, followed by those with security engineering skills (39%) and networking modernization skills (38%).

Resources required for zero-trust
When looking at which zero-trust pillars will likely require the most resources to implement, responses naturally varied by agency type, size and zero-trust maturity level. Civilian agency respondents said implementing “user” controls will require the most resources and “automation/orchestration” the least. Defense/intelligence agency respondents see “user” controls as requiring the most resources, but “visibility/analytics” the least.

Implementing “user” controls also topped the list of resource demands at medium-size and large agencies while addressing “network/environment” needs ranked highest at small agencies.

When comparing by zero-trust maturity, those still in the discovery stage said that “data” would require the most resources and “devices” the least. Those at the baseline stage ranked “network/environment” highest and “visibility/analytics” least.

Those at the intermediate stage ranked “user” controls highest and “visibility/analytics” least. While those at advanced levels said their “network/environment” would require the most resources and “automation/orchestration” the least.
WHO WE SURVEYED
FedScoop conducted an online survey of 191 prequalified federal government IT decision-makers. The survey was conducted online in September – October.

Respondent by agency type

<table>
<thead>
<tr>
<th>Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civilian</td>
<td>63%</td>
</tr>
<tr>
<td>Defense/Intelligence</td>
<td>37%</td>
</tr>
</tbody>
</table>

Respondent by agency size

<table>
<thead>
<tr>
<th>Size</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 5,000 employees</td>
<td>32%</td>
</tr>
<tr>
<td>5,000 – 10,000 employees</td>
<td>28%</td>
</tr>
<tr>
<td>More than 10,000 employees</td>
<td>39%</td>
</tr>
</tbody>
</table>

Respondent breakout by job title

<table>
<thead>
<tr>
<th>Title</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-suite</td>
<td>21%</td>
</tr>
<tr>
<td>Chief information, technology and security officials</td>
<td>7%</td>
</tr>
<tr>
<td>IT management</td>
<td>36%</td>
</tr>
<tr>
<td>IT security management/staff</td>
<td>12%</td>
</tr>
<tr>
<td>IT influencer</td>
<td>7%</td>
</tr>
<tr>
<td>Procurement official/staff</td>
<td>14%</td>
</tr>
<tr>
<td>Other (systems engineer, operations management)</td>
<td>3%</td>
</tr>
</tbody>
</table>
How familiar are you with the core objectives of OMB M 22-09 or DOD’s latest zero-trust reference architecture?

- Fully familiar: 39%
- Generally familiar: 47%
- Somewhat familiar: 15%
- Not familiar: 9%
Where would you rate your agency’s maturity in its zero-trust journey?

<table>
<thead>
<tr>
<th>Discovery/Assessment</th>
<th>Baseline</th>
<th>Intermediate</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify Desktop as a Service (DaaS)</td>
<td>Access to DAAS driven by cyber policies</td>
<td>Fine-grain user/device attributes drive access</td>
<td>Cybersecurity policies dynamically determine access + real-time analytics</td>
</tr>
<tr>
<td>Map data flows</td>
<td>Networks segmented</td>
<td>User ID based on federated ID service</td>
<td>Continuous, adaptive authentication &amp; authorization</td>
</tr>
<tr>
<td>Inventory user/devices</td>
<td>Devices are managed &amp; comply with IT policies</td>
<td>Micro-segmentation across majority of the network</td>
<td>User/device ID based on enterprise federated ID service</td>
</tr>
<tr>
<td>Identify privilege accounts</td>
<td>Least privileged access, MFA are in use</td>
<td>Initial DLP/ DRM implementations</td>
<td>Majority of data is ML-tagged</td>
</tr>
<tr>
<td>Log network traffics</td>
<td>Meet encryption requirements</td>
<td>User &amp; entity behavior analytics in use</td>
<td>Advanced analytics supports automation</td>
</tr>
<tr>
<td>Determine security policies, compliance and privilege levels</td>
<td>Begin data classification and tagging of critical data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Base: 191  |  Don’t know 9%
Where would you rate your agency’s maturity in its zero-trust journey?

**Civilian**
- Base: 120
- Don’t know 10%

- Discovery: 18%
- Baseline: 28%
- Intermediate: 29%
- Advanced: 15%

**Defense/Intelligence**
- Base: 71
- Don’t know 8%

- Discovery: 18%
- Baseline: 38%
- Intermediate: 15%
- Advanced: 20%
ZERO-TRUST MATURITY
ALL RESPONDENTS BY AGENCY SIZE

Where would you rate your agency’s maturity in its zero-trust journey?

<table>
<thead>
<tr>
<th>Agency Size</th>
<th>Discovery</th>
<th>Baseline</th>
<th>Intermediate</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 5,000</td>
<td>23%</td>
<td>37%</td>
<td>21%</td>
<td>16%</td>
</tr>
<tr>
<td>employees</td>
<td>employees</td>
<td>employees</td>
<td>employees</td>
<td>employees</td>
</tr>
<tr>
<td>Base: 62</td>
<td>Don’t know 3%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5,000-10,000</td>
<td>15%</td>
<td>31%</td>
<td>28%</td>
<td>19%</td>
</tr>
<tr>
<td>employees</td>
<td>employees</td>
<td>employees</td>
<td>employees</td>
<td>employees</td>
</tr>
<tr>
<td>Base: 54</td>
<td>Don’t know 7%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>More than 10,000</td>
<td>17%</td>
<td>27%</td>
<td>24%</td>
<td>16%</td>
</tr>
<tr>
<td>employees</td>
<td>employees</td>
<td>employees</td>
<td>employees</td>
<td>employees</td>
</tr>
<tr>
<td>Base: 62</td>
<td>Don’t know 16%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
BUDGET LINE FOR ZERO-TRUST
BY AGENCY SIZE

Has your agency created a budget line item for zero-trust work?

- **Less than 5,000 employees**: 52% Yes, 27% No, 21% Don’t Know
  - Base: 62

- **5,000 - 10,000 employees**: 67% Yes, 15% No, 19% Don’t Know
  - Base: 54

- **More than 10,000 employees**: 60% Yes, 19% No, 21% Don’t Know
  - Base: 75
How confident are you that your agency will receive any incremental funding for zero-trust work in the FY 2024 budget?

- **Less than 5,000 employees**
  - Highly confident: 24%
  - Moderately confident: 44%
  - Not very confident: 23%
  - Not at all confident: 10%
  - Don’t know: 2%

- **5,000-10,000 employees**
  - Highly confident: 17%
  - Moderately confident: 50%
  - Not very confident: 20%
  - Not at all confident: 11%
  - Don’t know: 1%

- **More than 10,000 employees**
  - Highly confident: 15%
  - Moderately confident: 39%
  - Not very confident: 33%
  - Not at all confident: 8%
  - Don’t know: 5%
How confident are you that your agency will receive any incremental funding for zero-trust work in the FY 2024 budget?

- **Highly confident**
- **Moderately confident**
- **Not very confident**
- **Not at all confident**

**Discovery**
- Base: 35
- Don’t know: 6%

**Baseline**
- Base: 60
- Don’t know: 3%

**Intermediate**
- Base: 46
- Don’t know: 9%

**Advanced**
- Base: 32
- Don’t know: 8%
CONFLICTING IT PRIORITIES

ALL RESPONDENTS

How concerned are you that other high-priority IT projects will suffer in FY2024 due to the need to reallocate resources to meet OMB’s/DOD’s zero-trust objectives?

The majority of all respondents reported some level of concern for other high-priority IT projects.

However, those concerns varied, depending on where agencies are in their zero-trust maturity.

- **Highly concerned**: 18%
- **Moderately concerned**: 43%
- **Not very concerned**: 26%
- **Not at all concerned**: 9%

Base: 191 | Don’t know 3%
CONFLICTING IT PRIORITIES
BY ZERO-TRUST MATURITY LEVEL

Level of concern that other high-priority IT projects will suffer in FY2024

- Highly concerned
- Moderately concerned
- Not very concerned
- Not at all concerned

Discovery
Base: 35
Don’t know 3%

Baseline
Base: 60
Don’t know 2%

Intermediate
Base: 46
Don’t know 2%

Advanced
Base: 32
WHO IS LEADING ZERO-TRUST WORK
BY AGENCY SIZE

Does your department/agency have a designated individual in place to lead its zero-trust implementation?

- **Less than 5,000 employees**
  - Yes: 61%
  - No: 27%
  - Don’t Know: 11%
  
  Base: 62

- **5,000 - 10,000 employees**
  - Yes: 70%
  - No: 11%
  - Don’t Know: 19%
  
  Base: 54

- **More than 10,000 employees**
  - Yes: 65%
  - No: 12%
  - Don’t Know: 23%
  
  Base: 75
WHERE ZERO-TRUST OFFICE REPORTS
BY AGENCY SIZE

Who does that individual report to?

- CIO’s office
- CFO’s office
- COO’s office
- Other
- Haven’t finalized
- Don’t know

**Less than 5,000 employees**
*Base: 62*
- CIO’s office: 42%
- CFO’s office: 34%
- COO’s office: 11%
- Other: 3%
- Haven’t finalized: 3%
- Don’t know: 8%

**5,000-10,000 employees**
*Base: 54*
- CIO’s office: 45%
- CFO’s office: 16%
- COO’s office: 18%
- Other: 11%
- Haven’t finalized: 11%

**More than 10,000 employees**
*Base: 75*
- CIO’s office: 55%
- CFO’s office: 16%
- COO’s office: 12%
- Other: 4%
- Haven’t finalized: 6%
- Don’t know: 6%
How confident are you that ongoing security programs can be realigned to meet OMB’s and DOD’s zero-trust goals?

- **Highly confident**: 28%
- **Moderately confident**: 48%
- **Not very confident**: 16%
- **Not at all confident**: 3%

Base: 191 | Don’t know 3%
Do you believe your agency’s senior executives have full visibility of the gaps that must be closed to achieve zero-trust objectives?

- **Less than 5,000 employees**: 55% Yes, 32% No, 13% Don’t Know (Base: 62)
- **5,000 - 10,000 employees**: 63% Yes, 20% No, 17% Don’t Know (Base: 54)
- **More than 10,000 employees**: 48% Yes, 39% No, 13% Don’t Know (Base: 75)
How confident are you that your agency has the requisite skills in-house to assess its security needs in each of the primary zero-trust pillars?

- Highly confident
- Moderately confident
- Not very confident
- Not at all confident
- Don’t know

**Less than 5,000 employees**
*Base: 62*

<table>
<thead>
<tr>
<th>Pillar</th>
<th>Highly Confident</th>
<th>Moderately Confident</th>
<th>Not Very Confident</th>
<th>Not At All Confident</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>23%</td>
<td>44%</td>
<td>26%</td>
<td>8%</td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>31%</td>
<td>53%</td>
<td>11%</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>Network/Environment</td>
<td>31%</td>
<td>52%</td>
<td>15%</td>
<td>3%</td>
<td></td>
</tr>
<tr>
<td>Applications/Workload</td>
<td>31%</td>
<td>42%</td>
<td>23%</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>44%</td>
<td>31%</td>
<td>19%</td>
<td>5%</td>
<td>2%</td>
</tr>
<tr>
<td>Visibility/Analytics</td>
<td>24%</td>
<td>44%</td>
<td>24%</td>
<td>6%</td>
<td>2%</td>
</tr>
<tr>
<td>Automation Orchestration</td>
<td>27%</td>
<td>41%</td>
<td>19%</td>
<td>8%</td>
<td>3%</td>
</tr>
</tbody>
</table>
SKILLS TO ASSESS ZERO-TRUST
BY PILLAR AND BY AGENCY SIZE

How confident are you that your agency has the requisite skills in-house to assess its security needs in each of the primary zero-trust pillars?

- **Highly confident**
- **Moderately confident**
- **Not very confident**
- **Not at all confident**
- **Don’t know**

**5,000 - 10,000 employees**
*Base: 54*

<table>
<thead>
<tr>
<th>Pillar</th>
<th>Highly Confident</th>
<th>Moderately Confident</th>
<th>Not Very Confident</th>
<th>Not at All Confident</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>33%</td>
<td>48%</td>
<td>13%</td>
<td>6%</td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>52%</td>
<td>31%</td>
<td>7%</td>
<td>4%</td>
<td>6%</td>
</tr>
<tr>
<td>Network/Environment</td>
<td>41%</td>
<td>33%</td>
<td>17%</td>
<td>2%</td>
<td>7%</td>
</tr>
<tr>
<td>Applications/Workload</td>
<td>39%</td>
<td>31%</td>
<td>15%</td>
<td>6%</td>
<td>9%</td>
</tr>
<tr>
<td>Data</td>
<td>39%</td>
<td>48%</td>
<td>4%</td>
<td>2%</td>
<td>7%</td>
</tr>
<tr>
<td>Visibility/Analytics</td>
<td>35%</td>
<td>35%</td>
<td>17%</td>
<td>6%</td>
<td>7%</td>
</tr>
<tr>
<td>Automation Orchestration</td>
<td>28%</td>
<td>37%</td>
<td>28%</td>
<td>7%</td>
<td></td>
</tr>
</tbody>
</table>
SKILLS TO ASSESS ZERO-TRUST
BY PILLAR AND BY AGENCY SIZE

How confident are you that your agency has the requisite skills in-house to assess its security needs in each of the primary zero-trust pillars?

- Highly confident
- Moderately confident
- Not very confident
- Not at all confident
- Don’t know

More than 10,000 employees
Base: 75

<table>
<thead>
<tr>
<th>SKILLS TO ASSESS ZERO-TRUST</th>
<th>USER</th>
<th>DEVICE</th>
<th>NETWORK/ENVIRONMENT</th>
<th>APPLICATIONS/WORKLOAD</th>
<th>DATA</th>
<th>VISIBILITY/ANALYTICS</th>
<th>AUTOMATION ORCHESTRATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>32%</td>
<td>45%</td>
<td>15%</td>
<td>5%</td>
<td>3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>33.33%</td>
<td>45.33%</td>
<td>12%</td>
<td>5.3%</td>
<td>4%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network/Environment</td>
<td>28%</td>
<td>52%</td>
<td>13%</td>
<td>4%</td>
<td>3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications/Workload</td>
<td>25%</td>
<td>43%</td>
<td>23%</td>
<td>4%</td>
<td>5%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>25%</td>
<td>47%</td>
<td>17%</td>
<td>7%</td>
<td>4%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visibility/Analytics</td>
<td>21%</td>
<td>51%</td>
<td>19%</td>
<td>5%</td>
<td>4%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automation Orchestration</td>
<td>21%</td>
<td>43%</td>
<td>25%</td>
<td>4%</td>
<td>7%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VALUE OF ZERO-TRUST ASSESSMENTS
ALL RESPONDENTS

How valuable would a comprehensive zero-trust assessment be to identify gaps and key focus areas?

- Highly valuable: 43%
- Moderately valuable: 46%
- Not very valuable: 45%

How valuable do you feel this assessment and any subsequent services would be from a third-party vendor or organization?

- Highly valuable: 35%
- Moderately valuable: 13%
- Not very valuable: 7%
- Not at all valuable: 2%
Which shortage of staffing/skills is hindering your agency most in implementing zero-trust? (Select up to 3)

- Data management: 40%
- Engineering security specialist: 39%
- Networking modernization: 38%
- Enterprise architecture: 29%
- Project management: 25%
- DevSecOps: 21%

Base: 191 | Other 7%: IT management, user education, limited staff, IAM and multiplatform integration engineer
Which pillars will likely require the most resources to implement? Please rank each with 1=most resources and 7=least resources.

<table>
<thead>
<tr>
<th>Civilian</th>
<th>Defense/Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User</td>
</tr>
<tr>
<td>Network/environment</td>
<td>Network/environment</td>
</tr>
<tr>
<td>Data</td>
<td>Device</td>
</tr>
<tr>
<td>Applications/workload</td>
<td>Data</td>
</tr>
<tr>
<td>Device</td>
<td>Applications/workload</td>
</tr>
<tr>
<td>Visibility/analytics</td>
<td>Automation/orchestration</td>
</tr>
<tr>
<td>Automation/orchestration</td>
<td>Visibility/analytics</td>
</tr>
</tbody>
</table>
## GREATEST RESOURCE DEMANDS
### BY AGENCY SIZE

Which pillars will likely require the most resources to implement? Please rank each with 1=most resources and 7=least resources.

<table>
<thead>
<tr>
<th>Less than 5,000 employees</th>
<th>5,000-10,000 employees</th>
<th>More than 10,000 employees</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network/environment</strong></td>
<td><strong>User</strong></td>
<td><strong>User</strong></td>
</tr>
<tr>
<td><strong>Applications/workload</strong></td>
<td><strong>Network/environment</strong></td>
<td><strong>Data</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td><strong>Device</strong></td>
<td><strong>Device</strong></td>
</tr>
<tr>
<td><strong>Automation/orchestration</strong></td>
<td><strong>Data</strong></td>
<td><strong>Applications/workload</strong></td>
</tr>
<tr>
<td><strong>User</strong></td>
<td><strong>Applications/workload</strong></td>
<td><strong>Network/environment</strong></td>
</tr>
<tr>
<td><strong>Visibility/analytics</strong></td>
<td><strong>Visibility/analytics</strong></td>
<td><strong>Automation/orchestration</strong></td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td><strong>Automation/orchestration</strong></td>
<td><strong>Visibility/analytics</strong></td>
</tr>
</tbody>
</table>
Which pillars will likely require the most resources to implement? Please rank each with 1=most resources and 7=least resources.

<table>
<thead>
<tr>
<th>Discovery</th>
<th>Baseline</th>
<th>Intermediate</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base: 35</td>
<td>Base: 60</td>
<td>Base: 46</td>
<td>Base: 32</td>
</tr>
<tr>
<td>1</td>
<td>Data</td>
<td>User</td>
<td>Network/environment</td>
</tr>
<tr>
<td>2</td>
<td>Applications/workload</td>
<td>Device</td>
<td>Network/environment</td>
</tr>
<tr>
<td>3</td>
<td>Automation/orchestration</td>
<td>User</td>
<td>Network/environment</td>
</tr>
<tr>
<td>4</td>
<td>Visibility/analytics</td>
<td>Applications/workload</td>
<td>Data</td>
</tr>
<tr>
<td>5</td>
<td>Network/environment</td>
<td>Data</td>
<td>Applications/workload</td>
</tr>
<tr>
<td>6</td>
<td>User</td>
<td>Automation/orchestration</td>
<td>Automation/orchestration</td>
</tr>
<tr>
<td>7</td>
<td>Device</td>
<td>Visibility/analytics</td>
<td>Automation/orchestration</td>
</tr>
</tbody>
</table>
CONCLUSIONS

Inflated sense of capabilities?
While agencies have come a long way in modernizing their IT, the relatively high proportion of executives saying their agency has reached intermediate or advanced zero-trust security capabilities may overstate their true condition. That could be because advanced capabilities are only being applied to a portion of agency systems, not agency-wide; and/or because C-suite respondents may underestimate what must be completed to actually achieve zero trust.

Deeper leadership support required
Senior agency leaders appear aware of zero trust’s importance, but many still may not understand the breadth and depth of IT capabilities required to implement it. Given that federal zero trust mandates remain largely unfunded, it is critical that agency leaders take ownership of assessing and prioritizing the investments required to address their IT and security gaps.

Zero trust: A journey for everyone
“Zero trust isn’t a journey for security teams. It’s a journey for the entire agency,” one federal CISO told FedScoop. Implementing zero trust impacts everyone. So agency leaders must recognize the importance of allocating resources for training and education throughout the entire agency.

Identity drives everything else
While zero trust depends on executing prescribed security practices on multiple dimensions, agency leaders must ensure their IT departments have the necessary resources upfront to master user identity and access management. Because identity will be applied in networking, devices, data access, workloads and automation, getting identity right is foundational to the rest of the pillars in zero trust.

Underappreciated pillar: Log management
While the study highlights which zero trust pillars will likely require the most resources, one capability that remains underappreciated is the need to dramatically scale the collection, storage and analysis of log files, the CISO at one large agency told FedScoop. He estimated zero trust would mean a 40-fold increase in log files, plus the staff, to manage it all.
Contact
Wyatt Kash
Senior Vice President Content Strategy
Scoop News Group
Washington, D.C. 202.887.8001
wyatt.kash@scoopnewsgroup.com