The State of the Federal IT Landscape

Results of a 2018 survey of Federal IT professionals
Table of Contents

About this report 2

Key findings 4

Security is a prime concern 5

The move to the cloud continues 9

High expectations for the cloud 10

Tool investments considered critical 14

Conclusion 15
About this report

For the State of the Federal IT Landscape report, OneLogin commissioned CITE Research to conduct an online, in-depth survey of 150 federal IT professionals in the United States. The goal of the survey was to understand:

- The current federal IT landscape
- Security concerns and challenges facing federal agencies
- IT plans with regard to the cloud
- Technologies in use or being considered to address concerns

This survey was conducted in late October of 2018.

RESPONDENTS

The survey was conducted with IT professionals who were managers or higher in their agency.

Respondents ranged in age from 18 to 55+.

![Pie chart showing the distribution of respondents by job title:]

- C-level: 23%
- Vice President: 12%
- Director: 31%
- Manager: 31%
- Other: 3%

Source: OneLogin
Respondents came from agencies across the country.

And from a variety of agencies.

**TYPE OF AGENCY:**

- **CIVILIAN:** 25%
- **DOD/INTELLIGENCE:** 41%
- **INDEPENDENT:** 34%
The State of the Federal IT Landscape reveals that:

Federal agencies are moving to the cloud in large part for added security. But agencies see risks—including data security—largely because of the human element. So, successful management of access to apps and systems in the cloud is top of mind.

IT departments at federal agencies already manage a large number of applications, and they expect that number to grow significantly. The added burden of securing these apps presents a serious challenge to IT professionals.

Nearly half of federal IT professionals don’t believe they have adequate staff to protect from cyberattacks. Given the strained budgets of most federal agencies, it’s critical to pick security tools that won’t require more staff or IT time to manage.

Given constrained budgets and the challenge of managing access to a growing cloud portfolio, a majority of IT professionals would prefer a centralized access management system that includes all the key security tools needed to manage user and constituent access.

Key findings
Security is a prime concern that is hard to address

IT Professional expressed significant concern about security and breaches.

**TOP ATTACK CONCERNS:**

- **Malware attacks**
- **Phishing attacks**

**Attacks of concern to federal IT professionals**

Source: OneLogin

- Younger professionals express more concern about device theft (50%).
- 35+ express more concern about ransomware attacks (45%).
- Civilian agencies worry most about phishing attacks (58%) and ransomware attacks (53%).
- DOD/Intelligence agencies worry most about device theft (43%).
FEARS ABOUT THE IMPACT OF ATTACKS

The potential impacts of an attack are many. Top of mind for federal IT professionals is loss of data.

Top worries about the impact of an attack:

Source: OneLogin

- 72% Data loss
- 48% Service outage/downtime
- 46% Loss of intellectual property
- 44% Loss of money
- 38% Legal expenses
- 36% Investigation
- 1% Other

Younger professionals (18-34) fear loss of money more (56%).

Older professionals worry more about downtime (60%).

DOD/Intelligence agencies are especially worried about IP loss (52%).
IT FEELS CHALLENGED TO ADEQUATELY ADDRESS SECURITY CONCERNS

Half of agencies spend between 41-100 hours on security operations each week.

Total hours spent on security operations

Source: OneLogin

- Less 10 hrs | 1%
- 11-40 hrs | 17%
- 41-60 hrs | 22%
- 61-80 hrs | 11%
- 81-100 hrs | 19%
- 101-200 hrs | 15%
- 201-300 hrs | 5%
- 301-400 hrs | 3%
- 401-500 hrs | 1%
- More than 500 hrs | 5%

52% of respondents spend between 41-100 hours/week on security operations.
Most agencies think their technology is on par or better than Silicon Valley tech companies.

Federal government tech compared to Silicon Valley

- 39% Our technology is more advanced
- 45% Our technology is equally advanced
- 13% Our technology is less advanced
- 3% I’m unsure

Source: OneLogin

But nearly half don’t believe they have adequate staff to protect from attacks.

My agency lacks the amount of staff to protect from cyberattacks

- 21% Completely agree
- 27% Somewhat agree
- 25% Somewhat disagree
- 26% Completely disagree
- 1% Not applicable

Source: OneLogin

And nearly half don’t believe their agency is fully prepared for attacks.

My agency is not fully prepared against cyberattacks

- 21% Completely agree
- 26% Somewhat agree
- 27% Somewhat disagree
- 25% Completely disagree

Source: OneLogin

Source: OneLogin

8 | THE STATE OF THE FEDERAL IT LANDSCAPE
The move to the cloud continues—but with challenges

Cloud use is expected to grow among agencies.

Expectation re: growth of cloud apps in next two years

- 85% Will increase
- 3% Will decrease
- 10% Will stay the same
- 2% I’m unsure

Source: OneLogin

And, by overwhelming margins, agencies feel prepared for it.

Very prepared: 52%
Somewhat Unprepared: 41%
Somewhat prepared: 4%
Very unprepared: 2%

Source: OneLogin
HIGH CLOUD EXPECTATIONS TEMPERED BY CONCERNS

IT Professionals have high expectations, but also valid concerns about moving to the cloud.

TOP DRIVERS OF THE MOVE TO THE CLOUD:

- Easier IT management
- Improved security

Drivers to increase cloud usage

- Easier IT management: 50%
- Improved security: 47%
- Better control: 35%
- Better reliability: 33%
- Ease of access for end-users: 31%
- Low cost: 27%
- Automatic updates: 27%
- Simpler remote access: 16%
- None of the above: 1%

Source: OneLogin
While they have confidence in the infrastructure and services of cloud providers, IT worries about deployment and secure use, i.e. the human element.

Concerns about the move to the cloud

Source: OneLogin

<table>
<thead>
<tr>
<th>Concern</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data security</td>
<td>49%</td>
</tr>
<tr>
<td>Compatibility with other systems</td>
<td>36%</td>
</tr>
<tr>
<td>Costs</td>
<td>32%</td>
</tr>
<tr>
<td>Complex IT management</td>
<td>32%</td>
</tr>
<tr>
<td>Reliability/downtime</td>
<td>29%</td>
</tr>
<tr>
<td>Complex implementation or migration</td>
<td>25%</td>
</tr>
<tr>
<td>Having enough staff to manage it</td>
<td>23%</td>
</tr>
<tr>
<td>Limited control</td>
<td>21%</td>
</tr>
<tr>
<td>None of the above</td>
<td>4%</td>
</tr>
</tbody>
</table>

Data security is a larger concern for those in their position 5+ years.

Complex implementation or migration is more likely to be cited by those Director-level and above.
FEDERAL AGENCIES MAINTAIN A HYBRID ENVIRONMENT

On average, teams have 50.8% of their apps in the cloud and 49.2% on-prem.

Proportion of apps in the cloud or on-premise

Source: OneLogin

APP PROLIFERATION AND A HYBRID ENVIRONMENT WILL CONTINUE

The number of applications in use in federal agencies is high.

Number of business apps currently & in two years

Source: OneLogin

Now

Two years
CLOUD APPS WILL CONTINUE TO GROW

85% of federal IT professionals expect the number of their agency’s cloud apps to increase over the next two years.

Source: OneLogin
Federal IT is investing in tools to address security and complexity

Agencies are forced to use many different security tools.

SECURITY TOOL USE:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Currently use</th>
<th>Plan to adopt (12 months)</th>
<th>Plan to adopt (1-5 years)</th>
<th>No plans to adopt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Access Security Broker</td>
<td>63%</td>
<td>22%</td>
<td>9%</td>
<td>6%</td>
</tr>
<tr>
<td>On-Prem Identity Access Mgmt</td>
<td>59%</td>
<td>23%</td>
<td>12%</td>
<td>6%</td>
</tr>
<tr>
<td>Next Generation Firewall</td>
<td>57%</td>
<td>26%</td>
<td>9%</td>
<td>8%</td>
</tr>
<tr>
<td>VPN</td>
<td>57%</td>
<td>25%</td>
<td>9%</td>
<td>9%</td>
</tr>
<tr>
<td>Identity as a Service</td>
<td>53%</td>
<td>26%</td>
<td>9%</td>
<td>12%</td>
</tr>
<tr>
<td>Multi-Factor Authentication</td>
<td>51%</td>
<td>27%</td>
<td>11%</td>
<td>11%</td>
</tr>
<tr>
<td>Secure Web Gateway</td>
<td>50%</td>
<td>30%</td>
<td>7%</td>
<td>13%</td>
</tr>
</tbody>
</table>

Source: OneLogin

APP PROLIFERATION AND A HYBRID ENVIRONMENT WILL CONTINUE

With the proliferation of access management tools and concerns about managing more apps, the vast majority of agencies reported they’d feel more secure with a centralized access management system.

My agency would feel more secure if we had a centralized access management platform (SSO, MFA, RBAC) for both cloud and on-prem apps:

<table>
<thead>
<tr>
<th>Agreement Level</th>
<th>35%</th>
<th>40%</th>
<th>16%</th>
<th>8%</th>
<th>1%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completely agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Somewhat agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Somewhat disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Completely disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: OneLogin
Conclusion

Federal agencies currently work in a hybrid environment, with a mix of on-prem and cloud applications. While they are rapidly moving to the cloud and feel prepared to do so, the hybrid environment isn’t going away anytime soon.

Moving to the cloud raises its own issues. High among them is the need to secure access to a large and growing number of applications, particularly cloud applications.

Federal agency IT professionals are using multiple security tools and access management tools. At the same time, agencies have a limited and, often, inadequate amount of staff to protect against cyberthreats.

For those reasons, a majority of agencies would prefer the security of a centralized access management system—one that includes key tools like user lifecycle management, SSO, MFA, and the implementation of flexible and granular security policies. Federal IT professionals believe that a centralized access management system would add security for their agencies while easing the management and cost burden on their IT departments.

**Learn more about the unified access management imperative**

A hybrid reality in federal IT creates challenges for existing approaches to access management. Learn how federal agencies are using new approaches to unify access management.

Read the white paper
About OneLogin

OneLogin, the leader in Unified Access Management, connects people with technology through a simple and secure login, empowering organizations to access the world™. The OneLogin Unified Access Management (UAM) platform is the key to unlocking the apps, devices, and data that drive productivity and facilitate collaboration. OneLogin serves businesses and partners across a multitude of industries, with over 2,000 customers worldwide. We are headquartered in San Francisco, California. For more information, visit www.onelogin.com, Blog, Facebook, Twitter, or LinkedIn.

See it for yourself.
Get a demo.

onelogin.com/product-demo

About CITE Research

CITE Research is a global market research firm. We partner with Fortune 500 companies to start-ups to provide expertise in support of our clients unique goals. Our collaborative model enables CITE Research to deliver insightful, value-added services across a broad range of sector verticals. For more information please visit www.citeresearch.com or call 646-206-9017.