

PUBLIC SECTOR

Unlock the Cloud's ROI Advantage

Insights from Splunk and Amazon Web Services



Modernize with smarter investments for stronger outcomes

In today's evolving public sector, organizations face more pressure to demonstrate ROI. The stakes aren't just measured in dollars, but in performance, resilience, and institutional trust.

That's a high bar for any organization, but especially those at the state and local levels, which tend to have more limited budgets, smaller teams, and older infrastructure than their federal counterparts.

Often, the result is technical debt: organizations relying on quick fixes and legacy technology to meet operational needs — for now. Piecemeal solutions add up over time, creating complex

digital environments that are tough to manage and even harder to monitor. Without real-time visibility, organizations can struggle just to maintain reliable service and prevent costly disruptions, let alone innovate for the future.

That's why many state, local, and educational institutions are embracing integrated cloud solutions to help cut costs, strengthen resilience, and create lasting value.

With a more secure, agile, and resilient foundation in the cloud, public sector organizations can:



Consolidate tools



Boost operational efficiency



Find and fix problems faster



Consolidate tools to streamline savings and security

The public sector’s patchwork of tools layered on top of outdated legacy systems might offer short-term functionality, but it often leads to inefficiencies and redundant workflows. Teams may find themselves maintaining and paying for tools that serve overlapping purposes, contributing to rising IT costs.

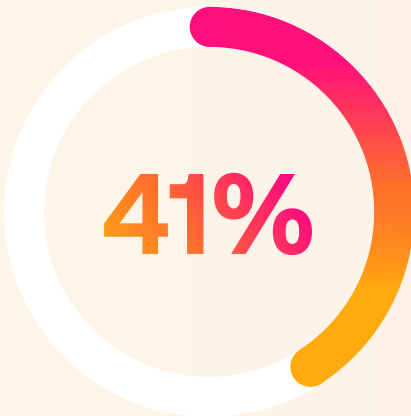
Beyond inefficiency, fragmented technology poses real risks. Each new system means more services to monitor and secure, more data to analyze, and more potential points of failure. Without operational visibility across their digital assets, it can be difficult — and costly — for organizations to detect blind spots, resolve issues, and prevent disruptions.

To get the most out of their technology investments, public sector organizations need a more strategic, streamlined approach. Consolidating tools in the cloud and centralizing log management not only reduces technical debt and operational complexity, but can also drive meaningful cost savings.

Organizations can redirect that reclaimed time and money to other priorities, such as upskilling staff and innovating for long-term value. Every efficiency gained in the cloud gives public sector organizations a crucial advantage.

Mind the gaps

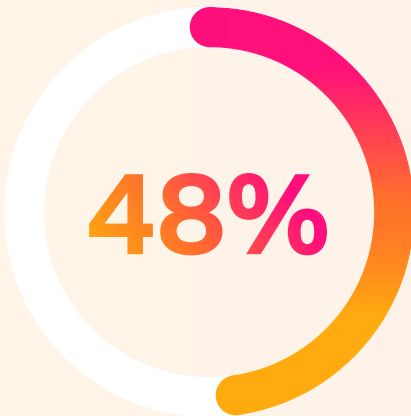
Low visibility and disconnected tools remain foundational challenges for the public sector, according to the [State of Security 2025](#) from Splunk.



of public sector respondents say their visibility over users and data needs improvement



of public sector respondents describe their visibility over network infrastructure they own or operate as somewhat or very low



of public sector respondents say dispersed security tools create significant challenges — twice the rate across all industries

Boost operational efficiency for maximum impact

The cloud can unleash new levels of productivity for state, local, and educational institutions. By automating repetitive tasks and reducing manual workflows, public sector teams can operate more efficiently and spend more of their time where it matters most: meeting their mission for the people they serve.

For example, some government employees report saving up to **105 minutes a day** through AI-powered workflows. That's time that can be reinvested in strategic, high-impact work. These gains are especially valuable as public sector organizations face a growing shortage of skilled workers and rising demand for services.

Cloud-enabled automation further augments teams to help close gaps and ease pressure on limited resources. The benefits extend to everything from IT and DevOps to HR and finance.

Additionally, the public sector faces a growing compliance burden, with organizations required to meet mandates such as StateRAMP, HIPAA, FERPA, and many others. Streamlining and automating compliance activities in the cloud helps reduce the likelihood of errors. That, in turn, minimizes the risk of fines, ransom payments, downtime, and lost productivity.

Automation also strengthens security operations by helping SOC teams act with greater speed and precision. It minimizes human error, streamlines incident workflows, and enforces security policies consistently and at scale.

With so much at stake in the public sector, cloud efficiencies aren't just a nice-to-have. They're a strategic operational imperative for remaining secure and compliant in the modern threat environment.



of **public sector boards** cite operational efficiency as a top priority



Find and fix problems faster

Access to high-quality data is the backbone of every cloud success story, whether the mission is to secure digital systems, deliver exceptional services, or anything in between. However, this is another area where the public sector’s technical debt and tool sprawl can hinder progress.

As threats grow more sophisticated and AI becomes a tool for bad actors, defending critical infrastructure and protecting sensitive data is more urgent than ever.

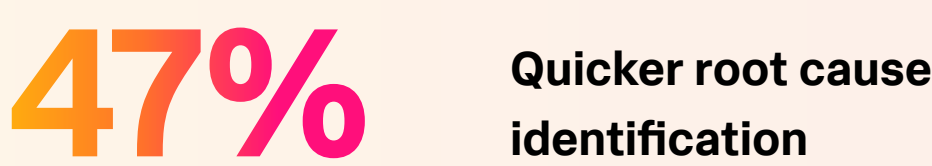
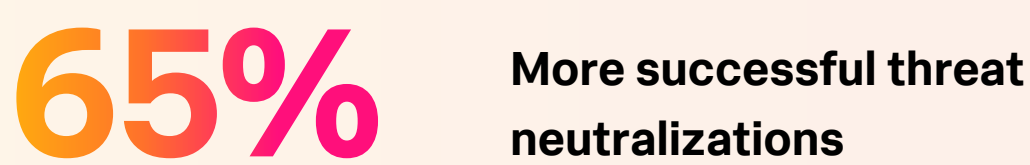
Staying ahead of these emerging cyber threats may seem like an ambitious — and expensive — goal, but the price of maintaining the status quo could be higher. Attacks on the public sector can expose valuable data or disrupt critical services that citizens and students rely on every day. In fact, **downtime costs public sector organizations \$193 million annually**, with consequences ranging from lost revenue to lasting reputational damage.

A modern cloud infrastructure, paired with the right observability solutions, offers a smarter path forward. Organizations can seamlessly ingest and analyze data from across their digital landscape. With real-time data access and unified visibility, IT and security teams can respond faster and identify problems before they turn costly.

These capabilities grow stronger with deep technical integrations and mature analytics. Predictive insights, federated search, and risk-based alerting help teams shift from reactive to proactive threat detection — and ultimately improve service delivery.

Fuel resilience with your data

Data complexity can expand an organization’s attack surface, but a winning data management strategy can help. **Data management leaders report** many improved security outcomes:



Turn your cloud investment into mission value

Today's public sector faces a tough equation: rising expectations, aging infrastructure, limited resources, and increasingly sophisticated cyber threats. To meet these challenges, organizations must prioritize modernization efforts that support real, measurable return on investment.

That's where Splunk and Amazon Web Services deliver. By combining real-time insights and the cloud's scalability and resilience, public sector organizations can unlock an ROI advantage.

With a more secure, agile, and resilient foundation in the cloud, public sector organizations can lay the groundwork for whatever comes next.

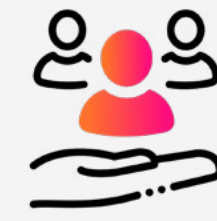
Focus on what matters most in the public sector, leveraging Splunk and AWS to:



**Optimize performance
in the cloud**



**Protect critical services and data
from cyber threats**



**Deliver better outcomes for the
people you serve**



Learn more:
www.splunk.com



Learn more:
www.aws.amazon.com

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2025 Splunk LLC. All rights reserved.

