proofpoint.

DSPM: The starting point for protecting mission-critical data

State and local governments are racing to modernize their digital infrastructure. But with that progress comes a mounting cybersecurity challenge: the rapid growth and sprawl of sensitive data.

proofpoint.

For years, state and local government agencies have relied on familiar cybersecurity staples like firewalls, data loss prevention (DLP) systems, and security information and event management (SIEM) tools to protect their data. These tools served their purpose in a time when data lived inside well-defined perimeters and security teams had clear visibility and control.

That time has passed.

Today, government data is more distributed than ever. It's created, stored, and shared across dozens of cloud services, collaboration platforms and third-party systems. Employees access files from personal devices, share documents externally via public links and store records in multi-cloud environments far beyond the reach of legacy tools.

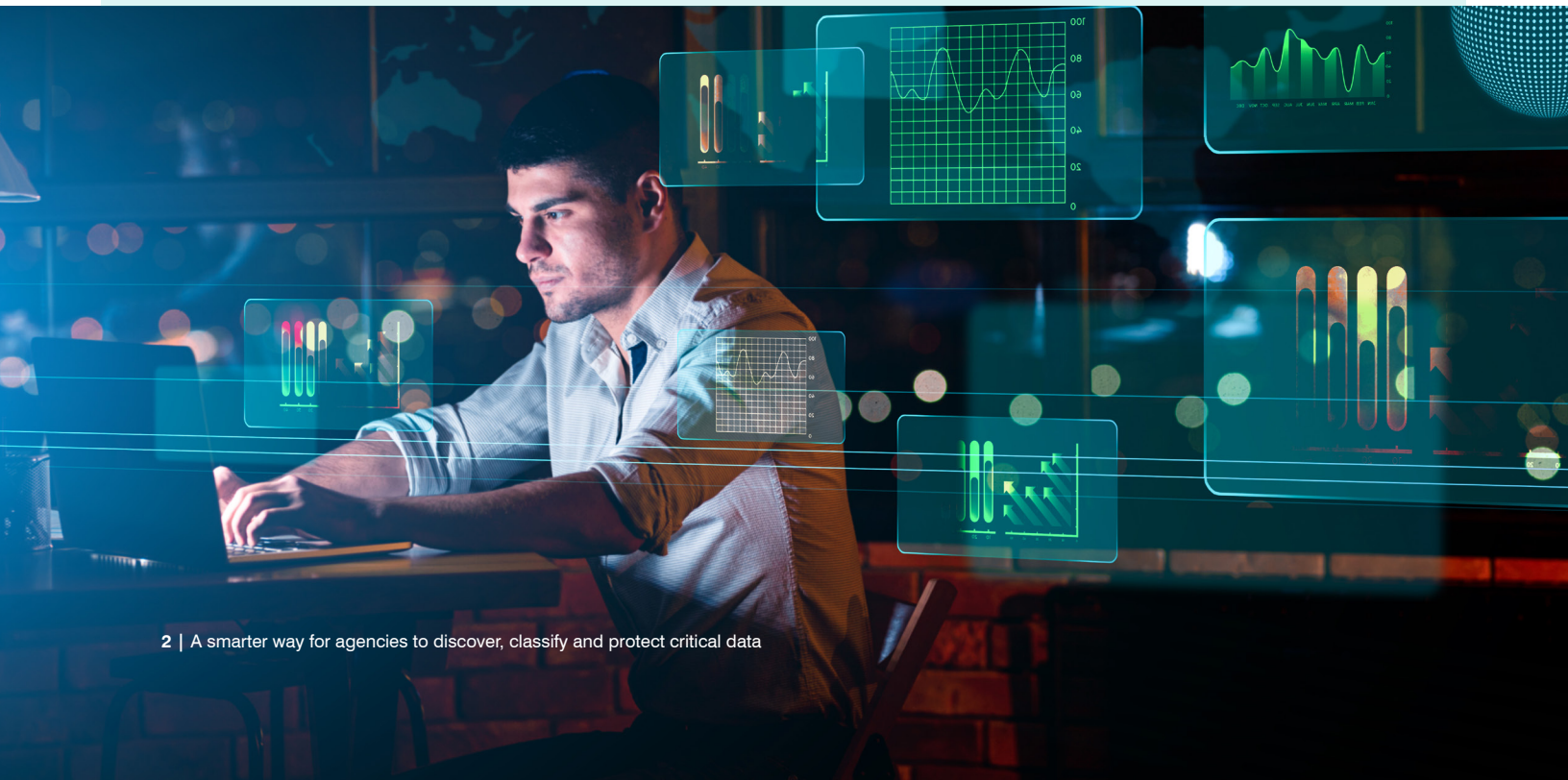
This data sprawl has created a critical visibility gap.

"Unstructured data is growing really fast," said Itir Clarke, product marketing manager at Proofpoint. "A big portion of that data is sensitive. And a significant portion is being shared broadly—sometimes with external sources and often with all employees."

Many agencies simply don't have the resources to keep up. As the Cybersecurity and Infrastructure Security Agency (CISA) warns, many state and local governments frequently lack the tools, staff and infrastructure to properly secure their environments. That leaves sensitive information exposed to misconfigurations, inappropriate access and growing cyber threats.

At the heart of the problem lies a fundamental truth: You can't secure what you can't see.

> **Unstructured data is growing really fast. A big portion of that data is sensitive. And a significant portion is being shared broadly—sometimes with external sources and often with all employees."**
>
> **ITIR CLARKE**
> Product Marketing Manager, Proofpoint



Agencies have to do more, in terms of significance, with fewer resources. Risk prioritization is key."

ITIR CLARKE
Product Marketing Manager, Proofpoint

Data visibility from discovery to defense

To regain control over their expanding risk surface, agencies are adopting data security posture management (DSPM): a modern framework for continuously identifying where sensitive data lives, who has access and how their data may be exposed. It's a proactive response to the chaos.

"With the data sprawl that's happening, it's really difficult for agencies to even know where sensitive data is," Clarke explained. "Being able to discover data stores, pinpoint the ones that have sensitive information and identify security risks gives staff the ability to prioritize risks and tackle those first."

DSPM requires agencies to continuously scan environments for common issues such as misconfigured permissions, overshared files and abandoned data. This way, agencies aren't just detecting problems; they're gaining the context they need to take meaningful action.

The result is less noise, smarter prioritization and faster remediation. Especially for government agencies with limited security staff, this kind of automation is a force multiplier.

"Agencies have to do more, in terms of significance, with fewer resources," Clarke noted. "Risk prioritization is key."

Inside Proofpoint's DSPM: Smart, efficient and built for government

Proofpoint built its DSPM solution with the needs of the public sector in mind. Rather than layering on more tools or requiring complex deployments, it offers a lightweight, high-impact solution that agencies can adopt quickly.

Here's how it works:

Rapid, agentless deployment: Proofpoint connects via API to cloud environments like Microsoft 365, Google Workspace and AWS. No agents, no disruption. Agencies can begin discovering and classifying sensitive data in hours, not weeks.

Fast, scalable discovery: At the platform's core is the One-Pass Scanner, which classifies sensitive data across SaaS, PaaS, IaaS, on-prem and hybrid environments while preserving data residency.

Visualizing real-world risk: With its access and attack path graphs, Proofpoint maps identities, resources and data stores to reveal indirect access mechanisms and exploit paths.

Real-time enforcement & automated remediation: Proofpoint provides one-click DLP policy creation to revoke excessive permissions through Proofpoint DLP. Plus, it integrates with tools like ServiceNow, Jira or Slack for guided remediation workflows.

A smarter way to secure government data

Beyond breach prevention, Proofpoint DSPM helps public-sector organizations meet growing compliance demands while reducing operational burden. The platform assigns monetary value and breach likelihood to sensitive data such as personally identifiable information (PII) and protected health information (PHI), and cross-references risks against compliance frameworks such as CJIS, HIPAA, and NIST. Agencies gain a prioritized view of their most vulnerable data.

It doesn't just monitor data — it changes how agencies think about and protect it.

"Without data classification, you can't apply the right data controls," Clarke explained. "You can't tag it, mask it, encrypt it or apply role-based access policies. Proofpoint automates classification to help agencies do all of that without overwhelming their teams."

In a world where threats are escalating and resources remain tight, Proofpoint's DSPM solution delivers what government agencies need most: clarity, control and confidence.

"Without data classification, you can't apply the right data controls. You can't tag it, mask it, encrypt it or apply role-based access policies. Proofpoint automates classification to help agencies do all of that without overwhelming their teams."

ITIR CLARKE
Product Marketing Manager, Proofpoint

Learn more about how Proofpoint is helping state and local governments modernize their approach to data security.