Moving Federal Government Forward Securely With Data Protection

MARKET TRENDS REPORT

govloop FORCEPOINT | FOUR POINTS TECHNOLOGY

Introduction

Federal government security has reached an inflection point – and not one that has resulted in a decline of data attacks. Data loss prevention (DLP), the traditional security system for protecting information, has tried to keep data safe in the past, but there's a question as to whether it's the best strategy to deal with a widening landscape of new risks.

Data loss prevention operates on an antiquated basis of securing data via binary and sometimes restrictive policies – and those principles mean that it is no longer adequate for modern cybersecurity standards.

As organizations move data to the cloud and federal regulations follow, data loss prevention has failed to adapt to the mobile era of today. As importantly, data loss prevention can bring productivity to a halt, especially in an environment where there are more drivers of data than ever. Agencies need a way to enable mobile, multiplatform workflows that are still secure – and today, data loss prevention falls short.

Fortunately, there are innovative technologies in the fight against network attackers and a new strategy that is suitable for today's workforce. Dynamic Data Protection can pick up the slack where DLP lags.

To learn how modern data protection strategies can enable agencies and unburden security, GovLoop partnered with Forcepoint, a leader in delivering human-centric cybersecurity solutions, and Four Points Technology, an experienced government IT solutions provider. Reading on, you'll learn about how contemporary solutions can translate the positives of old security into the digital era. We'll also speak with Bharath Vasudevan, Senior Director of Product Marketing at Forcepoint, and Denise Harrison, Chief Information Officer of Four Points Technology, to survey the landscape of dangers and defenses, as well as receive best practices.

By the Numbers

38% **of federal cyber incidents came from unidentified methods of attack, "suggesting limited situational awareness"**

16% **of agencies achieved the governmentwide target for encrypting data at rest**

73% **of agencies reported full implementation for encryption of data in transit**

31% **of agencies that suffered an insider threat incident did not directly employ the insider**

98% **of insider threat incidents in government were motivated by financial gain**

236k **government datasets are available to the public on Data.gov**

"Federal Government data is critically important to the US economy. Moreover, maintaining trust in Federal data is pivotal to our democracy."

President's Management Agenda: One Year Of Progress

THE CHALLENGE

Choosing Between Halting Progress and Stopping Threats

Traditionally, data loss prevention has governed the way agencies have guarded their data. But as workflows expand to remote locations and agencies go to the cloud to enable modern, mobile workflows, DLP becomes less effective.

Oftentimes security concerns are what preclude agencies from considering cloud migrations and remote applications, despite potential productivity gains for their IT organizations and encouragement from the federal hierarchy. Data loss prevention works by identifying sensitive data housed within an agency and stopping its sharing outside of agency networks. By operating on these premises, however, DLP can drastically slow projects in progress as employees may not immediately be able to conduct legitimate business outside of networks because of security protections against potential data leaks.

As such business cases are common, DLP overloads security IT teams with a deluge of alerts, many of which may not be threats at all but legitimate business activities. The problem of false positives – or denying legitimate actions – has become so critical that some security teams have decided to lift some permissions, which in turn opens the floodgates to attackers.

"Nobody loves their DLP implementation," Vasudevan said. "It's just a necessary evil that people have implemented to demonstrate regulatory compliance, and it usually brings far more challenges than it actually solves."

Agencies have years of data on their systems, but often lack visibility into what they actually possess and what is worth protecting.

This can be dangerous in the case of archaic data policies that fail to understand the unique role of every individual and the data they need access to. Insider threats, furthermore, are enabled by the openness of unsecured, uncounted-for data.

While these challenges of DLP are well known, they are not likely to diminish as systems progress. Conversely, more devices and more access points, from more locations and on unlimited networks, threaten to overwhelm DLP administrators. The dark data of today's on-premises world is small compared to what dark data could be when introducing the cloud.

To answer a spate of cyberattacks against federal agencies, regulations mandate that agencies secure their data at rest and have incident response plans in place. Agencies that rely on DLP alone could fail to meet many of these requirements.

"Government is recognizing the value of cloud solutions as well to allow for agility and growth, and the advancements in security tools have given them confidence to move their data. Much is still being evaluated by agencies based on each agency's data management rules and regulations," Harrison said. Those regulations can include the Federal Risk and Authorization Management Program (FedRAMP) for cloud and the Health Insurance Portability and Accountability Act (HIPAA) in health care, as well as others such as the Payment Card Industry Data Security Standard (PCI DSS).

With DLP, agencies face greater roadblocks on the path to satisfying regulations and incorporating modern technologies. As the amount of data and number of access points grow, agencies need a new solution that enables productivity instead of hindering it.

"Government is recognizing the value of cloud solutions as well to allow for agility and growth, and the advancements in security tools have given them confidence to move their data."

Denise Harrison
Chief Information Officer of Four Points Technology

THE SOLUTION

Protecting Your Information Anywhere With Dynamic Data Protection

Traditional DLP solutions have been able to classify and stop the sharing of agencies' sensitive information in some common insider threat situations, but these solutions haven't offered enough answers to frequent problems. The inability of DLP to answer the ***why*** questions of data usage is what has led to rigid restrictions, false positives and stalled productivity.

Dynamic Data Protection resolves that problem while offering even better security assurance than DLP. By establishing a user risk profile – compiled from the actions and behavior of a person on agency networks – Dynamic Data Protection allows administrators to gain a window into intent. A log of actions can indicate motivations with higher accuracy, weighing the considerations of modern workflows.

For example, if an employee in human resources printed out a document with the Social Security numbers of new hires, his or her risk profile may not elevate to the point of triggering different policy actions. Dynamic Data Protection could tell this was a legitimate business purpose, despite the inclusion of sensitive materials.

If that same employee, however, had frequently pulled up classified documents, saved them and printed them from a remote location after hours, those actions would cause Dynamic Data Protection to raise the risk level of the individual, flag the actions and even block the employee's ability to move files through different channels..

By partnering the same security principles as DLP with enhanced flexibility, Dynamic Data Protection leads to more automated policy enforcement based on user risk level from threat vectors of all kinds.

The combination of behavioral analytics and employee coaching can help delineate safe business activities from insider threats. Employee coaching can steer well-meaning employees away from sharing a file or exposing sensitive information by accident, as are the causes of many insider threat leaks. Coaching can help users self-correct their behaviors before they become a problem.

As it stands, many insider threat programs lack enforcement, so the incorporation of security protocols that can interface with users while also automatically determining whether to allow sensitive data movement can save organizations time and resources. It also braces them for the modern era of computing capabilities, such as cloud technology and remote workflows.

"In today's environment, over-restrictive policies cause headaches and avalanches of alarms, while under-restrictive policies leave you exposed," Vasudevan said. "Individualized, adaptive security blocks actions only where you need to and drives a more productive organization forward."

With automated policy enforcement, Dynamic Data Protection reveals anomalies in actions and can proactively adjust controls in near-immediate response to potential threats. With behavioral patterns, security is able to eliminate the problem of false positives.

Therefore, agencies no longer need to worry about security teams hassling field employees. In fact, the two sides can work in harmony to keep the agency safe and productive.

"Individualized, adaptive security blocks actions only where you need to and drives a more productive organization forward."

Bharath Vasudevan
Senior Director of Product Marketing at Forcepoint

BEST PRACTICES

Moving to Dynamic Data Protection

1. Establish a set of data policies.

Asking important questions about what data is moving through an agency and how data classification can help with silos is an important component of data protection. Some files might not need extra protection besides secure encryption when moving to USB drives, as some government agencies practice.

However, to know the right fit for data protection, agencies need visibility and policies around their data. Knowing what data they possess and where it resides is a crucial step for agencies.

2. Evaluate the business case for data protection.

What is the impact to the agency if secure data is lost? Are there certain technologies that your agency has wanted to adopt but doesn't have the bandwidth for? Or does data frequently need to touch many different people in multiple offices before fulfilling its purpose? Antiquated security can slow down processes and make new technologies incompatible with information in-house. Modern, cloud-ready security capabilities can cut down on time and allow agencies to bring in innovative workflows and technologies.

3. Ask questions of employees.

Do employees know what they should and shouldn't be sharing from their work accounts? See what employees think and craft a strategy, considering their needs, that establishes normal baselines of data handling. By answering employees' questions about regular and anomalous behavior, agencies can reduce the number of false positives that security teams encounter.

4. Coordinate with security.

In adopting a new data protection strategy, there are three camps of security teams: those who are working proactively, those who are working reactively to a new set of policies or technology and those who are responding to an incident. That comes down to organizational design and how early security comes into the process.

"You have organizations that have security embedded within the lines of business," Vasudevan said. "That's a smart way to solve a problem, because there are security considerations throughout the decision-making process."

5. Partner with industry.

Rather than continue in the mire of incident management and regulatory reporting, organizations need to consider security as a part of the design upfront. Therefore, to deliver the best value, agencies must integrate security and business tools immediately – stoking confidence in workloads and data. Leadership should consider cost savings and future business potential when evaluating new solutions, and the right industry partner will help make sure that organizational data policies match the protection plan.

Case Study

For quite some time, data theft prevention and data security had been on the agenda for the IT team at Sweden's Borlänge Municipality. For a government organization, it was especially crucial that Borlänge meet strict compliance regulations. When the existing information security solution in Borlänge had reached the end of support, the IT team started a serious search for a new and more advanced platform.

After a thorough selection process, Borlänge selected Forcepoint. Since then, Borlänge's ability to protect its data has improved significantly without increasing pressure on IT management.

"With Forcepoint, we have a greatly enhanced insight into the security risks, which have been mitigated," Jan Stegaras, IT Operations Manager for the Borlänge Municipality, said. "The solution provides excellent reporting capabilities and is easy to manage. Also, the support from Forcepoint always provides exactly what we need, when we need it. We are very happy with this platform and convinced we have made the right choice."

Forcepoint's unified approach is one of the reasons why Borlänge selected this solution.

"Up until now we were very much focused on providing maximum security in a reactive manner. Now we are ready to take the next step and secure our systems more proactively. Forcepoint provides the tools necessary for this process."

Jan Stegaras
IT Operations Manager, Borlänge municipality

HOW FORCEPOINT AND FOUR POINTS HELP

Forcepoint is an experienced solution provider in data protection, addressing legacy limitations by fusing new capabilities with a human-centric design. By applying a user-risk-based approach to data security, Forcepoint can holistically cover an enterprise's data and is ready for cloud and on-premise environments. Specifically, Forcepoint harnesses the power of behavioral analytics to offer security teams real-time threat detection and automatic enforcement to keep data safe.

Four Points is a service-disabled veteran-owned small business that matches IT solutions with government partners. Partnering with top software companies, Four Points can closely tailor solutions to the needs of federal acquisition teams, promising a rapid and clear return on investment. Four Points' portfolio includes GSA Schedule 70 and SEWP V solutions, as well as agency-tailored options.

To learn more, visit: https://www.4points.com/forcepoint.

Conclusion

In a data-driven world, agencies can't afford to be behind the ball in securing their data. DLP, the legacy standard, can impede productivity, delay evolution and fail in the face of widening attack surfaces. Meanwhile, an expanding force of cybersecurity threats can force agencies further back into their shell.

Dynamic Data Protection, however, offers the opportunity to enable new technologies and promote productivity. Employees' patterns of behavior can be tracked over time to measure and balance insider threat precautions, while endpoints can be secured just the same. For a workforce that's increasingly on the move, data protection needs to be as dynamic as the people relying on it.

ABOUT FORCEPOINT

Forcepoint is the global human-centric cybersecurity company that understands people's behavior as they interact with confidential data on devices and in the cloud. Forcepoint's behavior-based, risk-adaptive cybersecurity systems deliver converged solutions that enable organizations to continually empower their employees to innovate, while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.

For more about Forcepoint, visit www.forcepoint.com and follow us on Twitter at @ForcepointSec.

ABOUT FOUR POINTS TECHNOLOGY

Four Points Technology is a CVE verified Service Disabled Veteran Owned Small Business (SDVOSB) dedicated to providing IT Products and Professional Services to the Federal Government. Four Points Technology offers solutions that support a wide variety of business initiatives specifically suited for Government organizations. Four Points Technology supplies services and products meeting numerous Cybersecurity, DataCenter, Mobility, and MedicalIT challenges within the Federal customer market. As an RSA Platinum partner, Four Points Technology evaluates customer challenges and helps to bring solutions that solve those problems cost effectively and with exceptional service.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop