Data Protection Takes Center Stage (And It's About Time)

MARKET TRENDS REPORT

govloop

Trustwave® Government Solutions

carahsoft®

Introduction

Federal agencies experienced 31,000 cybersecurity incidents in 2018 alone, while state and local agencies endured countless more. Many of those incidents resulted in hackers gaining access to critical, often sensitive data, which they can exploit for their own gain.

As data breaches continue to plague government agencies, it has become clear that there is no proverbial silver bullet for protecting valuable, often mission-critical data. The vast amount of data that government agencies collect, the proliferation of legacy systems and an overwhelming shortage of cybersecurity professionals compound the challenge.

Today, ensuring that data is fully protected requires more than simply securing networks and endpoints. Comprehensive protection requires a multifaceted approach incorporating both advanced data protection and threat detection and response. Often, the best way to get the visibility, coordination and response needed for full protection is to rely on experienced personnel who can leverage the power of cutting-edge technologies around the clock.

To learn more about how agencies can protect their critical assets, GovLoop teamed with Trustwave, a cybersecurity and managed security services provider specializing in threat detection and response that helps organizations fight cybercrime, protect data and reduce security risk. This report covers the importance of developing a cohesive strategy to protect an agency's valuable data and the best ways to accomplish the task.

By the Numbers

9,700

breaches from errors by authorized users at federal agencies in 2018

Source: FISMA Report to Congress for fiscal 2018

7,000

phishing attacks on federal agencies in 2018

Source: FISMA Report to Congress for fiscal 2018

207

vulnerabilities patched in five of the most common database products in 2019

Source: 2020 Trustwave Global Security Report

5%-20%

of IT budgets federal agencies typically spend on cybersecurity

Source: SANS.org

<15%

of employees at a typical state IT organization are cybersecurity staff

Source: Deloitte

8

federal agencies use legacy or outdated systems that vendors no longer support with security updates

Source: Senate report: "Federal Cybersecurity: America's Data at Risk"

17

federal agencies have not fully established agency- and system-level policies for assessing, responding to and monitoring risk

Source: Government Accountability Office cybersecurity report

74%

of states have adopted a cybersecurity strategic plan

Source: NASCIO 2019 State CIO Survey

"Wherever the government sector is weakest, cybercriminals motivated by financial gain will do more. State and local governments, municipalities, city councils, and local law enforcement agencies lacking strong security defenses and suffering from a dearth of cybersecurity professionals will remain in the crosshairs."

Source: Osterman Research

The Challenge: Protecting Critical Assets

Although hackers are typically interested in infiltrating all types of organizations, government agencies are particularly attractive targets. Not only does the sheer amount of information make protection complicated, but the type of information agencies have is often sensitive, making it especially valuable to hackers and nation-state adversaries.

To make matters worse, agency systems often lack enough cybersecurity professionals to keep things secure, and many use outdated or legacy systems. Some of these systems can't be cloud-enabled or moved from the hardware they run on. Often, these systems are considered an "acceptable risk" because they contain mission-critical data, yet they present security risks.

The most important challenge agencies face is protecting the data itself. Whether it exists in databases or other types of data stores, that data is vulnerable — and the data stores housing vulnerable information often have undetected vulnerabilities and misconfigurations.

A recent report from Trustwave found that database vulnerabilities were on the rise. The number of vulnerabilities patched in five of the most common database products increased by about 36% in the past year. Of those patched, many allowed denial-of-service attacks and some resulted in information disclosure.

"The actual data stores that house the most sensitive and potentially damaging mission-critical data has often been overlooked, often focusing just on protecting the endpoints, like laptops and servers," said Bill Rucker, President of Trustwave Government Solutions. "We are just now starting to see a trend where data protection for those systems and data stores is being looked at through a different lens. Given today's environment, this is a critically important change."

The Solution: Real-Time Threat Detection and Response

Comprehensively protecting critical assets requires both advanced data protection and threat detection and response. A data protection solution should include the most advanced capabilities available, including the ability to discover, inventory and monitor all data stores across the environment, both in the cloud and on premises; identify and audit excessively privileged user accounts; detect, alert and respond to policy violations; implement controls; and run analytics and reports.

But safeguarding data is only part of the solution. It must be complemented by real-time threat detection and response driven by high-level security experts who continuously evaluate log and data sources, along with endpoints, to identify potential threats and recommend proactive actions that can stop them in their tracks.

The most effective threat-detection and response solutions incorporate advanced automation, such as machine learning (ML) and artificial intelligence (AI), and integrate with an agency's Security Orchestration, Automation and Response capabilities. This combination of capabilities creates economies of scale that humans can never hope to replicate. According to Rucker, it allows anomalies to be analyzed in seconds, as opposed to several minutes or hours.

Then, incorporate highly skilled cybersecurity analysts to add their expertise to those results.

"In our threat hunts with organizations, we almost always find at least one instance where there was either a compromise underway they weren't aware of or an existing vulnerability that could cause a compromise in a mission-critical system," Rucker noted.

Although it's technically possible to implement and manage solutions such as these internally, doing so requires skilled cybersecurity staff and continually updating those solutions to take advantage of the latest advances. That's why so many organizations are shifting toward a managed security services approach to supplement efforts. In this setup, the provider delivers advanced cybersecurity services, working as an extension of the organization's internal cyber team.

"Adversaries only have to be right once, where we have to be right every time, for every system for every possible vulnerability," Rucker said. "If you don't have automation, efficient people and processes, and leading-edge technologies in place, it is a losing battle."

Best Practices: Implementing Proactive Data Protection

Don't ignore insider threats

Insider threats have always been a concern, but they are more of a problem today than ever before. The frequency of insider threat incidents has grown by 47% in the past two years, a recent report shows. Part of this growth is due to the changing paradigm of cybersecurity. "As organizations get better at defending the exterior, users with direct access to these systems continue to be the weakest link," Rucker said. It's not always a malicious act; often, it's due to a misconfiguration or user mistake. All of these risk factors mean that agencies should be just as careful monitoring people and processes on the inside of the organization as they are for adversaries on the outside. That requires the right tools and processes to detect and eradicate all threats in real time.

Improve your asset visibility

With so many datasets and systems created throughout so many decades on so many platforms in so many locations, it's hardly surprising that most organizations don't know where everything is. "This tends to be our customers' biggest Achilles' heel," Rucker said. Yet knowing exactly what you have is the first step to protecting it. Conduct a full asset inventory that includes exactly where everything is, who has access to it and the status of their permissions. With this information, you can start building a vulnerability list that includes everything from common misconfigurations to systems that have been installed but not maintained to users with extraneous permissions. "Sometimes users become power users on a system where they really just need read access," Rucker said. Once you understand what you have and who can access it, you can put in place the necessary vulnerability management, user rights management and activity monitoring.

Eliminate manual cybersecurity processes

The real-time nature of business today and the struggle to keep up with new threats require automation, optimally combined with ML, AI and advanced data analytics. Things are simply moving too fast. "We talked with a [chief information security officer] recently who was dealing with an unprecedented amount of data due to COVID-19. If they didn't have the automation that provides better efficiencies and orchestration, it would be like finding needles in a haystack," Rucker said.

Case Study: Government-Focused Security Council Improves Data Protection

A major federal security council with a mission of advancing the U.S. cybersecurity posture wanted to improve data protection. The council asked Trustwave to conduct a data-protection pilot that involved numerous types of database servers hosted in cloud-based and on-premise environments.

To conduct the pilot, Trustwave deployed both the Trustwave DbProtect Console and Scan Engine for cloud-based databases on Amazon Web Services and Trustwave AppDetectivePRO for on-premise databases.

- Trustwave DbProtect enables organizations to scan databases to discover and remediate vulnerabilities, perform continuous monitoring, run ad-hoc scans against security standards and compliance policies, identify and enforce least privilege access, monitor for anomalies, and audit and respond in real time to abnormal activity and policy violations.
- Trustwave AppDetectivePRO identifies configuration errors, identification and access control issues, missing patches, and any toxic combination of settings that could lead to bad outcomes such as data loss and distributed denial-of-service attacks.

Within 72 hours, the pilot identified all assets and more than 100 vulnerabilities. Results included 30 high-risk vulnerabilities in MySQL and 21 lower risks; 98 high-risk vulnerabilities in Oracle databases and 59 lesser vulnerabilities; and 56 high-risk vulnerabilities in Microsoft SQL Server with 42 lower risks. Within three to five days, the pilot resulted in a patch or remediation strategy that eradicated all vulnerabilities.

The council reported many lessons learned during the pilot, including the importance of documenting and reviewing architecture complexities, network requirements, and user permissions; how to define success criteria and expectations; and the importance of identifying policies for security checks to test.

As a result of the pilot, the council plans to deploy a second DbProtect Scan Engine, and to configure and deploy the Rights Management and Activity Monitoring features in DbProtect. These additions will provide advanced user rights review, access controls and real-time alerting for the most critical data stores.

HOW TRUSTWAVE HELPS

Trustwave supports the public sector with advanced cybersecurity services and solutions that enable local, state and federal governments to defend sensitive data and protect critical infrastructure while complying with applicable requirements. Trustwave's unique set of solutions and managed services provide agencies with an unprecedented level of visibility into their networks that enables new defense capabilities in mission threats. This allows agencies to shift from being reactive to proactive about security, identifying potential incidents before they become bigger problems.

Solutions include a host of prevention technologies and managed security testing, database security, threat detection and response, proactive threat hunting, digital forensics, and incident response. Trustwave helps ensure that government agencies strengthen cyber defenses, expand visibility, boost security maturity and maintain a security-first approach to compliance.

To learn more visit :
www.trustwave.com/government

Conclusion

Agencies today have enough to deal with just keeping networks running, users connected and constituents served. But without fully secure data, those missions are threatened, and public confidence can falter.

The only way to ensure ironclad data protection is by knowing exactly what data you have, where it is located and who has access to it at every moment of every day. That type of proactive data protection requires the right tools, processes, cybersecurity personnel and expertise. For agencies stretched to the limits, that often means using a managed security services approach that incorporates 24-hour monitoring with leading-edge data protection and threat detection and response capabilities.

Trustwave® Government Solutions

ABOUT TRUSTWAVE

Trustwave Government Solutions is a leading cybersecurity and managed security services provider who helps the United States government fight cybercrime, protect data and reduce security risk. Offering a comprehensive portfolio of managed security services, consulting and professional services, and data protection technology, Trustwave Government helps governments embrace digital transformation securely.

Learn more at www.trustwave.com/government/

govloop

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