Improving Federal Security With Automated Patching

MARKET TRENDS REPORT

Introduction

Cyberattacks are rising. In 2017, federal agencies reported 35,277 cybersecurity incidents for their IT systems (Source: GAO). The government today realizes it is in a cyberwar and must defend its agencies from attackers.

But focusing on perimeter security in an attempt to keep bad actors out is no longer enough, particularly as government accelerates moving its applications into the cloud. Federal agencies need effective layers of protection in their data centers and clouds. Tools like Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are a start – but they cannot always provide effective protection against all the vulnerabilities that may be present throughout the environment.

"Our own secretary said that the cyberthreat now exceeds the physical threat," Matthew Travis, Deputy Undersecretary of DHS's National Programs and Protection Directorate, has said. "The threat is real. A lot of people on the cyber front think the biggest threats come from brute force. But it's the simple stuff, like not patching your software."

One of the main reasons systems remain vulnerable is that they are either not patched or not patched quickly enough. Lack of proper security patching is a global problem. For example, it has been reported that more than 110 unique common vulnerabilities and exposures (CVEs) that had fixes released in 2007 were successfully exploited in 2016, over ten years later!

Automating manual processes, particularly security patching, in the data center can be a key factor to help federal agencies keep systems and data secure while freeing up resources for other critical tasks.

To understand how federal agencies can automate and operationalize their security patching efforts, GovLoop partnered with Oracle for this market trends report. In the following pages, we'll discuss the challenges federal agencies currently face in the world of cybersecurity and why patching automation is critical. We'll also provide agencies guidelines and recommendations for building security into their IT infrastructure from the start.

BY THE NUMBERS

38%

of federal cyber incidents did not have an identified attack vector, suggesting limited situational awareness.

Source: Wired

Six months into using automated security tools, DHS has already identified more than

$300,000 in cost savings

Source: Federal News Network

84%

of organizations say traditional security solutions don't work in cloud environments.

Source: Crowd

In 2018, malicious cyber activity have been estimated to cost the U.S. economy between

$57 billion & $109 billion

Source: The Cost of Malicious Cyber Activity to the U.S.

12 Weeks

time most organizations took to complete their patching process.

Source: Verizon Data Breach Investigations Report

46%

of cybersecurity and IT professionals delay patching because down-time impacts their ability to meet service level agreements (SLAs)

Source: Oracle and KMPG Cloud Threat Report 2019

On Nov. 21, 2017, the FITARA Enhancement Act of 2017 became law, which among other things requires the Chief Information Officer of each covered agency to conduct a risk management review of those investments that have received a high-risk rating for four consecutive quarters.

THE CHALLENGE
Increasing IT Infrastructure Security in Federal Agencies

If one thing is constant in the IT world, it's change. Technology and procedures are often changing for the better in government, which improves processes and services that citizens can then use to improve their lives.

"Agencies are advancing their thinking in terms of what they need to protect," Federal CIO Suzette Kent said at an industry event earlier this year, adding that agencies nevertheless need to continue looking at what they measure and automate some of those activities. "But we have to aggressively keep the mindset that we are never done," she said. "It's just a step in the journey."

But this change also means that fresh attack vectors and cybersecurity threats are constantly developing. We've seen that firsthand with discoveries of speculative execution vulnerabilities affecting certain hardware such as Spectre, Meltdown, Foreshadow, and L1TF.

Unfortunately, IT professionals often have limited resources, which makes proactively combating ever-evolving security vulnerabilities challenging, and leaves agencies' data and applications exposed.

In addition, security patching can be an extremely manual and time-consuming process. Because of this, many agencies and departments fail to patch in a timely manner. The patch that could have solved a security issue often exists – but may just never have been applied because of the complexity of doing so. As a result, environments remain vulnerable because the traditional network-based security tools do not provide effective mitigation against the exploitation of these issues.

Proper patching can be complicated. According to the National Institute of Standards and Technology (NIST), "Timing, prioritization, and testing are intertwined issues for enterprise patch management. Ideally, an organization would deploy every new patch immediately to minimize the time during which systems are vulnerable to the associated software flaws."

But the reality is that prioritization and limited resources affect when and which patches are applied. More importantly, bringing systems down to apply OS patches is very disruptive to the agency's operations, and administrators see it as a risk. Not applying patches right away, however, actually increases the likelihood that a security vulnerability will be successfully exploited by a malicious actor.

It is likely that manual patching and security processes will never be able to catch up with the changing field of cyberattacks, and the sheer number of vulnerabilities being disclosed every day.

The best way for federal agencies to overcome these issues and meet security and compliance demands is by moving to an operationalized and automated process for patching that does not disrupt their operations.

"Agencies are advancing their thinking in terms of what they need to protect, but we have to aggressively keep the mindset that we are never done. It's just a step in the journey."

-Suzette Kent, Federal Chief Information Officer

THE SOLUTION
Security and Patching Automation

It is critical that the federal government leverage its technology investments – both on-premises and in the cloud – and expand automation of security patching and reduce the amount of manual configurations and operations.

Automated patch solutions are essential for agency security programs because they work to reduce operational costs and narrow the window during which mission-critical systems are exposed. This approach also aids in standardizing and automating system components across an agency. Standardization across the enterprise allows security controls to be uniformly implemented and maintained, thus minimizing risk-management issues.

Operating system (OS) patching is an important part of keeping the systems and applications in an environment safe from attackers who may discover vulnerabilities left open when operating systems are not kept up-to-date. Keeping track of the necessary operating system patches and updating agency computers with each of them can be cumbersome. But doing so is essential. The WannaCry ransomware attack was a perfect example of what can happen if agencies don't keep operating systems updated with the latest patches.

Patching the OS kernel is critical, but many vulnerabilities are located in user space. Heartbleed is a good example of a huge user space vulnerability that cost companies hundreds of millions of dollars. This vulnerability resided in the OpenSSL library, which is used as an essential component to ensure the privacy of online transactions. Patching critical user space libraries with no system reboot is another key factor required to keep agencies secure so that organizations can apply patches while normal operations are not disrupted.

Finally, agencies should also work to automate the hypervisor patching process, reducing the time required to provision new operating system/application environments, helping standardize application deployments by cloning pre-certified configurations, and minimizing planned downtime. Making use of the right technology platform will also allow automated patching of operating systems and the software running inside the guest virtual machines.

Oracle Linux is the only operating environment that offers kernel, user space and hypervisor live patching, with no downtime required. Patches can be applied easily with Oracle Ksplice, and you can choose to automate patching to address newly discovered vulnerabilities. Oracle has successfully delivered millions of patches to organizations through Oracle Ksplice.

BEST PRACTICES
For Improved Federal Security With Automation

1. Keep your systems secure with automated zero-downtime patching

Zero-downtime patching automates the rollout of patching or updates across a domain while allowing your applications to continue servicing requests. This allows you to roll out distributed patches to multiple clusters or to your entire domain with a single command, all without causing any service outages or loss of session data for the end user. Oracle Linux and Ksplice provide the kernel, hypervisor and selected user space live patching required for automated zero-downtime patching. It takes what was once a tedious and time-consuming task and replaces it with a consistent, efficient and resilient automated process, that does not disrupt operations. Additionally, it removes the need to negotiate and schedule downtime for the layers above the operating system, such as the database and applications, saving time and resources.

2. Address critical compliance requirements and close security gaps

To comply with government regulations and standards, enforce comprehensive security controls wherever your data resides across complex hybrid environments. Use technology that can help you address these compliance risks and help you close the security gap, like an OS that automatically applies patches and security updates while running – reducing downtime and human error, and providing increased protection against emerging threats .

3. Implement repeatable practices – in the data center and the cloud – using prebuilt or customized templates

Consistency is key. Use standard prebuilt or customized templates for deploying new database and application environments. This will help you enforce best security practices and reduce human errors while ensuring consistent environments across your data centers. Additionally, templates that already include your database and applications save you a lot of time and effort, enabling rapid deployment.

4. Partner with a trusted vendor that has a track record of supporting mission-critical infrastructure

Agencies can't navigate this journey alone, and will require vendors in their path to improve the security of their infrastructure. Partner with vendors that offer the technology and support you require. Oracle has a proven track record of meeting government agency requirements with their solutions, expertise and technical support. Oracle's enterprise-class operating system, Oracle Linux, can provide the performance, data integrity and application uptime necessary for business-critical production environments. Thousands of customers run Oracle Linux to enable continuous availability and Oracle runs its cloud with over 61 billion transactions per day on Oracle Linux.

CASE STUDY

A large American airline operates more than 4,500 flights daily to 339 airports across five continents. In 2016, the organization operated more than 1.6 million flights carrying more than 143 million customers. With this much air traffic, the airline, its employees and customers are in perpetual motion. To consistently guarantee superior customer experience, the company has to ensure maximum uptime for both internal- and external-facing applications – which means rolling out patches with zero downtime.

The airline turned to Oracle Linux to boost security and service-level agreement (SLA) compliance with an automated and fully documented patching regimen. The ability to patch their operating systems live with Oracle Ksplice, without a reboot, helped the airline meet their security compliance requirements. Additionally, they improved their application management, streamlined change management and accelerated time-to-value by adopting Oracle Linux.

This capability freed IT professionals to focus on initiatives that drive innovation across the airline. In federal agencies, the same approach would not only help increase security, but also free up IT professionals from manual processes to work on more mission-centric projects that could improve issues for the organization and the citizens it serves.

HOW ORACLE HELPS

Oracle helps you address security issues with several capabilities. Available to Oracle Cloud Infrastructure (OCI) customers at no additional cost, and Oracle Linux on-premises customers with Oracle Linux Premier Support, Oracle Ksplice allows your agency to apply a security or stability patch to the OS kernel, hypervisor and critical user space libraries such as glibc and openssl while the system is running – and the patch takes effect immediately. This unique capability provides greater agility, making it easier to meet service-level requirements and address critical compliance gaps. It also enables you to automate your patching processes , while avoiding costly downtime disruptions.

Additionally, Oracle Linux provides a set of cryptographic libraries, services, and user level cryptographic applications that are validated to Federal Information Processing Standard (FIPS) Publication 140-2. Products implementing FIPS 140-2 validated cryptography provide assurance to government and industry purchasers that the cryptography has been independently tested and verified to meet the security requirements of the FIPS 140-2 Standard. Oracle Linux 7 has also obtained a Common Criteria certification compliant with the U.S. Protection Profile for General Purpose Operating Systems, Version 4.1.

Moreover, with Oracle Linux you get access to prebuilt Oracle tested and approved Docker container images for Oracle products such as Oracle Database, MySQL, Middleware and Java. These prebuilt templates, enable you to increase security by standardizing containers across your organization. They reduce the amount of human error involved with manual operations, and help improve compliance. Using these container images will also save you significant time and resources.

Whether on-premises or in the cloud, Oracle Linux and Ksplice offer the same level of availability and security for your systems and VMs

Learn more here: ***www.oracle.com/linux/security/***

Conclusion

Federal agencies must move away from manual approaches and toward automation that will help increase agency security. The ability to automate security patching without downtime and standardizing new deployments using templates allows for systems that are more reliable and more secure and able to meet both end user and citizen needs.

Automation of security in today's government IT environment will allow teams to focus on innovative cyber operations, keeping the federal enterprise and citizen data safer in an increasingly hostile cyber environment.

ABOUT ORACLE

Oracle helps customers develop roadmaps, migrate to the cloud, and take advantage of emerging technologies from any point: new cloud deployments, on-premises environments, and hybrid implementations. Oracle's approach makes it easy for companies to get started in the cloud and even easier to expand as business grows.

Tried, tested, and tuned for enterprise workloads, Oracle Linux is used by Oracle developers worldwide and is backed by support services from experts who understand the entire Oracle technology stack. Optimized for hybrid cloud environments, Oracle Linux is used by thousands of enterprises worldwide on premises as well as in the cloud, running billions of transactions per day.

Learn more at: **www.oracle.com/linux/security**

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