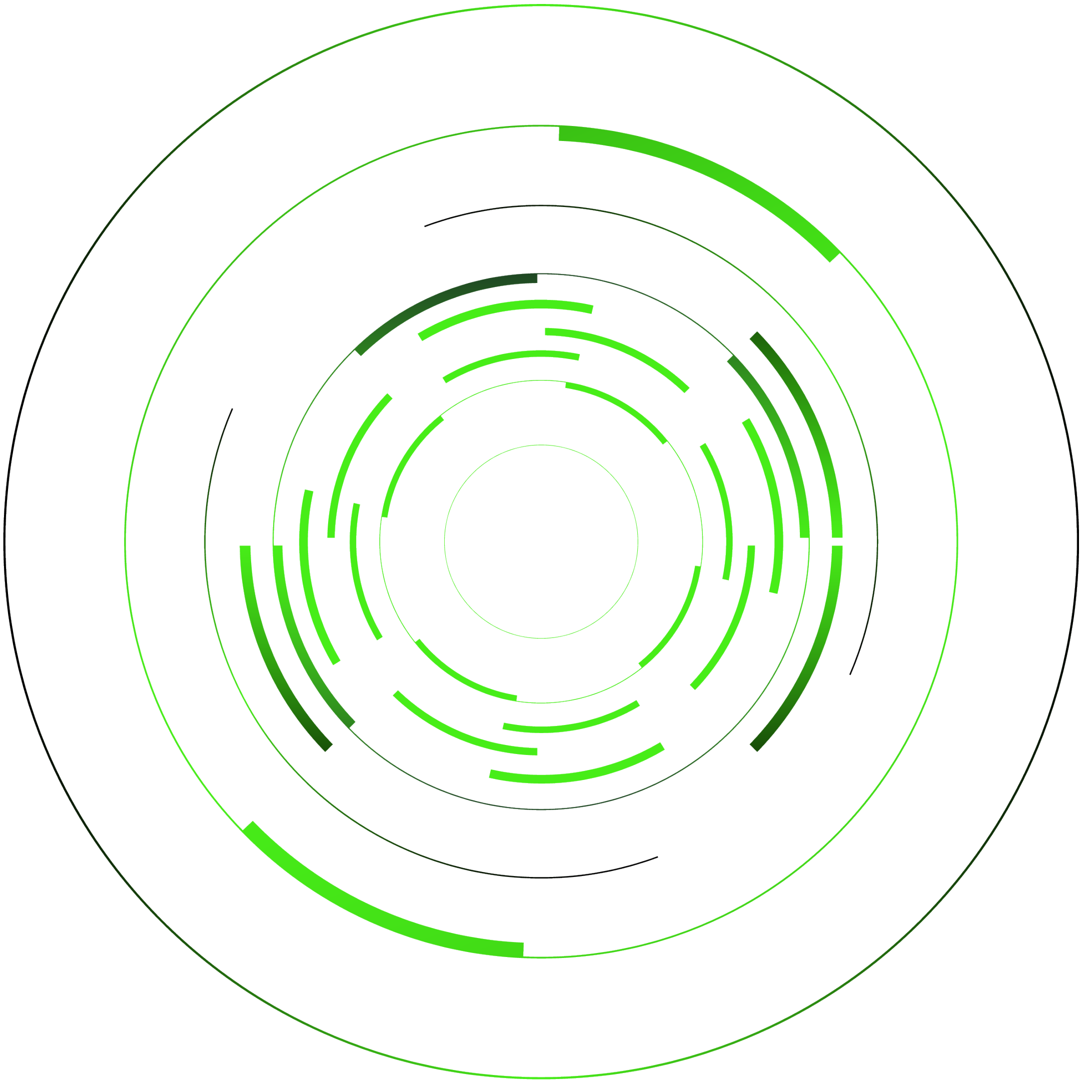
Deloitte.



Patch Automation

White Paper
March 2024

What's the real story?

In today's technology-dependent culture, IT has become a crucial part of everyday life. As organizations become more reliant on technology, the risk grows daily from bad actors seeking exploits. IT organizations carry great responsibility to safeguard users' information and stay current on the latest security updates. To combat vulnerabilities and secure complex IT environments, automated patch management is critical to maintaining business operations and keeping organizations secure. Automation allows organizations to react and mitigate potential reputational damage while retaining customer trust and affirming investments in personnel and security platforms. The past 5 years have set the tone of what can be done with automation tools like Ansible, Satellite, and System Center Configuration Management (SCCM) in complex environments with high operational tempos and customers expecting systems to be perpetually available.

The Pentagon's February 2022 memo on continuous Authority to Operate (cATO) emphasizes the need to implement a living strategy to security management[1]. cATO works to grant systems an ongoing authorization as long as three key competencies have been met: "Ongoing visibility of key cybersecurity activities inside of the system boundary with robust continuous monitoring of RMF controls; ability to conduct active cyber defense in order to respond to cyber threats in real time; and the adoption and use of an approved DevSecOps reference design".

- Hundreds of thousands of hours have been saved by automated processes performing smart scans of assets, subsequently deploying patches, and remediating threats in real-time.
- Specifically for cloud systems, risk has been minimized by using FedRAMP-approved IT platforms which reduce the scope of patching physical assets, allowing organizations to focus on operating system (OS) vulnerabilities, and the coded applets.
- Having a strong patch automation strategy reduces the active number of vulnerabilities on the network, increasing the overall security posture, and reducing time spent preparing for an ATO submission. This gives IT leadership a greater chance for success when adopting the cATO model.

How are agencies responding?

Agencies are able to take advantage of commercial off-the-shelf (COTS) products to expedite critical security functions, and readily adopt vetted solutions through pre-built playbooks, such as those for DISA Ansible. Shifting to Patch Automation introduces a set of challenges with change approval boards (CAB), addressing how personnel will be aligned to manage patch automation both technically (day-to-day) and administratively (procedural). How organizations respond is synonymous with growth and has been made clear through self-audits that there is a need to adapt and evolve practices using modern cyber defense tools to keep pace with ever-expanding cybersecurity threats.

- Bringing patch automation online in any environment comes with inherent red tape to obtain approval for procurement, and required amendments to an ATO where the automation platforms will live.
- Concurrently, program management needs to be engaged on staffing personnel; bringing the right skillset onboard to not only deploy one or more automation tools, but to develop processes, and balance the workload of agency needs versus wants.
- Lastly, to avoid never-ending project lifecycles, project management must effectively track cross-team staff who are developing automated solutions to ensure these solutions meet the customer-accepted definition of success.

[1] Continuous Authorization to Operate (cATO), available at Continuous-Authorization-to-Operate.pdf (defense.gov)

Where can you make improvements?

A multi-technology approach is recommended for organizations who need to bring automation to the forefront of patching. While a single solution that encompasses all systems is the goal, using a combination of available tools provides the best overall coverage. Organizations need to evaluate automation tools based on specific need and technology stack:

- **Ansible:** Utilizing a Continuous Improvement Continuous Development (CI/CD) pipeline methodology, Ansible implements baseline security before deploying Linux, Windows, Cisco, and VMware assets. By using playbooks, agencies can enable a strong cyber security posture before the asset ever hits production. Ansible is an open-source technology that doesn't rely on proprietary software and allows for low-cost prototyping.
- **System Center Configuration Manager (SCCM):** For Microsoft Server and endpoints, SCCM deploys both regular and ad-hoc. patching, both in the form of windows updates and application-specific updates, such as web browsers (Chrome, Firefox, Opera). This approach prevents out of date applications from running until patched.
- **Satellite:** Satellite is the Linux version of SCCM, performing inventory, patch, and content management to physical, virtual, and cloud systems in a central web based administrative interface.

How can you get started?

Agencies can protect their systems and assets from data breaches and other potential vulnerabilities with the help of automated patching. To develop an automation strategy, Deloitte suggests beginning with these four steps:

1. **Know Your Environment:** Create a complete list of assets and objectives for both your on-premise and cloud systems. This increases the chance of success when procurement and deployment of patch automation occurs. Additionally, establishing cost constraints and personnel requirements at the outset are critical to managing automation tools.
2. **Develop, Stand Up & Test:** Once automation tools have been procured and are in an operational state, a best practice is to test on a sampling of cloned systems starting with the most critical systems. Testing how unique environments react to automated actions before deployment into production permits development and test of an incident response plan. This approach also enables testing continuity of operations in case of adverse effects or critical failures in a low-risk environment. After-action write-ups should drive documentation and processes before a production deployment.
3. **Prioritize, Deploy & Monitor:** Use of automation tools in production starts with prioritized patching and configuration based on criticality or severity of the ongoing vulnerabilities. Deployed patches need to be monitored for success and any rollback options utilized in case of adverse effects according to previously developed documentation.
4. **Automated Feedback:** As proof of concept, automation tools report live metrics including remediated and ongoing vulnerabilities. This approach validates the overall patch process, demonstrating improvement in network security.

Deloitte's Core Technology Operations helps agencies with their own automation strategies:

- From 2017 to 2023, Deloitte provided services to Federal Clients, including patch automation deployment to successfully secure and manage thousands of assets.
- Most recently (Q3 2023), Deloitte deployed centrally managed patch automation to systems inside and outside of the United States, both on-premise and in the cloud. Patch automation now provides kernel-level updates and secure configurations to thousands of end-user devices, servers, and network appliances.

Contact us today for more information.

Contributors

William Lucas

Author
Cyber Infrastructure

Austin Sincock

Operations & Innovation Leader
Core Technology Operations
asincock@deloitte.com

Designed by CoRe Creative Services.