SIMPLIFYING THE PATCH MANAGEMENT PROBLEM

WWT and Syncurity Partner to Drive Secure Business Outcomes

Syncurity™ IR-Flow is an agile security operations platform that reduces cyber risk. IR-Flow makes security operations centers (SOCs) more efficient and effective through automation & orchestration of tightly integrated alert and incident response workflows. The solution is designed to deploy rapidly and calibrate easily to create near-immediate value.
PATCH MANAGEMENT CYCLE TIME DRIVES CYBER RISK

IT PATCH MANAGEMENT IS A NEVER-ENDING PROCESS OF IDENTIFYING, PRIORITIZING AND REMEDIATING ONGOING VULNERABILITIES. DELAYS IN PROPERLY PRIORITIZING AND APPLYING PATCHES CAN LEAD TO SECURITY BREACHES.

Spectre and Meltdown were prime examples that severely impacted many organizations, particularly in the healthcare industry. According to the Department of Health & Human Services (HHS) Office of Civil Rights (OCR) report, “These vulnerabilities... allowed malware to bypass data access controls and potentially access sensitive data.” There are three key factors that make patching so difficult:

1. APPLICATION COMPATIBILITY

Commercial or custom applications are often affected by security patches to underlying operating systems or middleware. It takes time for external vendors or internal development teams to test the impact of new security patches on their applications and ultimately rollout newly supported versions or compatible updates. This delay creates a common barrier to effective patching, leaving critical infrastructure for some legacy applications unpatched due to stability concerns or lack of vendor support where the application can’t be properly tested, modified and updated.

2. PATCH TESTING & ROLLBACK

Application compatibility concerns are responsible for many enterprises seeking security updates. This requires security and IT teams to test patches prior to applying them in production. This involves replicating the production environment in order to apply the patch in a sandbox environment and then testing the applications sufficiently to ensure there are no issues. If an issue is discovered, the production system change must be rolled back and the system restored from the last known backup.

3. CHANGE CONTROL

In order to expedite the patch application process, applications may incur unscheduled downtime. However, business service (e.g., application) owners want to avoid downtime during critical business hours at all costs. Narrow change control windows can hamper the ability of IT teams to patch systems quickly, particularly given the number of necessary steps outlined above. The change control window may be too narrow to accomplish all the necessary steps, requiring an exception to be made which must go through a series of reviews and approvals. Every hour is critical in the world of on-demand, 24/7 access, and certain network-enabled devices in a healthcare facility or hospital are unable to be patched until they’re not in use by/or a patient (assuming they can be patched at all).

80% OF SECURITY BREACHES STILL RESULT FROM POOR PATCH MANAGEMENT.
WWT Patch Management Solution Solves the Challenge

World Wide Technology (WWT) solves the patch management challenge with a comprehensive solution that delivers rapid response and reduced cyber risk. The combination of Cisco, Tenable, Tanium and VMware solutions orchestrated with certified integrations by the Syncurity IR-Flow SOAR platform enable real-time evaluation of vulnerability risk and the automated development, deployment and validation of relevant patches.

By codifying the steps necessary to effectively identify vulnerabilities, assess potential risk and — when appropriate — remediate that risk, enterprises are able to implement a repeatable, auditable workflow that can be executed consistently, regardless of the skill level of the available analysts, application owners or IT resources supporting the infrastructure.

SOFTWARE: The WWT patch management solution is comprised of multiple software components, including Cisco ISE, Tenable and/or Tanium real-time vulnerability scanning and Tanium and VMware patch development, deployment and backup/restore capabilities. The process is orchestrated and automated using the IR-Flow SOAR platform.

SERVICES: WWT provides range of services to ensure patch management success. Our experts provide vulnerability assessments to analyze your current environment and data landscape, focusing on risk to sensitive data. We manage the hardware and software deployment, installing the patch management components within your environment. Once deployment is complete, WWT oversees integration, which includes connecting the components through the SOAR platform. WWT will identify several high-value reports specific to your industry or business requirements, optimize and model the data capture needed to support those reports. We will also build reports in the IR-Flow Business Intelligence engine to demonstrate performance improvements.
Beyond Patch Management

While patching remains one of the key barriers to more effective cybersecurity risk mitigation, the implementation of a standard, repeatable process through the WWT Patch Management solution dramatically reduces the response time associated with executing vulnerability assessment and patch management processes. The result is greatly reduced exploit and breach risk. Using a Security Orchestration, Automation & Response (SOAR) platform also ensures consistency and provides a metrics baseline that can be used for continuous process improvement. Enterprises interested in addressing this patch management use case should consider evaluating SOAR platform for other high-priority use cases that could benefit from the automation of rote, manual tasks, the consistent application of defined processes and a significant reduction in the level of risk.

Finally, this is just one of many use cases for orchestration and automation that enable a critical enterprise process. There are many more use cases, including DevSecOps, physical security, asset management, etc., and while few enterprises are ready to implement fully automated remediation now, almost all could immediately benefit from instantiating and automating these types of enterprise processes in a repeatable, auditable software platform. WWT has the people, process and technology to make that happen.

The WWT Difference

WWT delivers strategic guidance and support throughout the entire patch management solution evaluation and implementation process. Our security team shares business consulting, technology and analytics expertise while WWT’s professional services engineers, consulting service engineers and data center technical architects offer in-depth understanding of all the solution components. More than just delivering hardware and software, WWT’s patch management solution includes all of the services and support required to enable real-time risk assessment and quick patch response without burdening current or adding additional resources. Plus, our Advanced Technology Center provides hands-on access to all of the patch management components, proves ROI through proofs of concept and positions the enterprise for future success with additional SOAR use cases and business intelligence solutions.

Contact us: 800.432.7008
Learn more: wwt.com

SOAR

Gartner has defined Security Orchestration, Automation & Response (SOAR) as technologies that enable organizations to collect security threat data and alerts from different sources, where incident analysis and triage can be performed leveraging a combination of human and machine power to help define, prioritize and drive standardized incident response activities according to a standard workflow. SOAR tools allow an organization to define incident analysis and response procedures (a.k.a., plays in a security operations playbook) in a digital workflow format, such that a range of machine-driven activities can be automated.