SECURESENSE

SecurePATCHING

Secure Sense Patch Management Service

The truth about your organizational risk associated with unpatched software…

The truth about your organizational risk associated with unpatched software is that unpatched systems are the most common technological factor in breaches, and loss of productivity. Unfortunately, solutions to patch related risks are often costly in terms of identifying and purchasing quality products, staffing and expertise. Almost two-thirds of breach victims report being breached due to unpatched, publicly known vulnerabilities and almost two-thirds of these victims were unaware that their organizations were vulnerable in the first place. Over half of the impacted organizations rely on manual patching processes that make it exceedingly difficult to keep up-to-date on patching cycles; meanwhile, the attack surface has exploded recently due to remote work scenarios and tens of thousands of CVEs are reported each year (and increasing). Cyber threats are more prevalent than ever, preying on outdated operating systems and applications. Given remote work scenarios, endpoints are increasingly difficult to patch and troubleshoot due to their mobility being off-net to patching tools. Even with the right tools, the right staffing and expertise are a challenge for IT budgets, especially where patching needs are typically messy, require follow-up processes and operate on conflicting schedules for typical staff availability.

What can Secure Sense do to help?

Ultimately, it will be a combination of quality tooling with an adequately staffed and effective best practice patching program that addresses the risks associated with patching. Stakeholders will recognize a familiar refrain in terms of IT security requirements that are cost-prohibitive in terms of tooling and staffing. As usual, the best ROI to be found will be a hosted and managed solution that can deliver cost efficiency and process efficiency in one.

Secure Sense's SecurePATCHING service powered by Tanium delivers a hosted solution fully managed from our 24x7x365 SOC. Our team will provide deployment services, ongoing asset discovery and management, patching module compilation and deployment, customization of patching workflows, technical support, exclusion management, and all manner of reporting and visibility customization. Our team will work with yours to design a comprehensive patching plan that integrated with your change management and technical teams. In addition to scheduled and automated features of the service, our team is available for ad-hoc requests, emergency and zero-day patching response with criticality-based service levels.

Our Value

- Centralization of patch management across diverse assets and environments
- Cost efficiency of staffing for MSP vs. hiring full-time employees
- Process efficiency of 24x7 processes vs. availability of your resources during business hours
- Low perimeter network load of our solution means lower risk patching in terms of productivity and technical risks from pushing broad scale patches over the network
- Advanced tracking and compliance metrics and advanced visibility of how risk profiles change in real time
- All the benefits of a seasoned, experienced team to guide your patching activities
- Dedicated resources committed to your success in the form of your CSM and extended Customer Success Team!

.

TANIUM

Technology Partner

Patch Management Shouldn't Be So Painful

Tanium provides endpoint management at scale, all f rom a single platform for consolidated control and visibility.

Simplify and Accelerate Patch Management and Compliance

With Tanium Patch, IT operations teams can keep systems up to date with automated patching across the enterprise at speed and scale. This helps organizations reduce complexity and increase business resilience by efficiently carrying out patching tasks and monitoring patch status across devices.

Real-Time Patch Visibility and Control: To prevent security breaches, keep endpoints up to date with the latest patches. Tanium designed our platform architecture to maintain performance across hundreds of thousands of endpoints. The Tanium platform provides speed and scale to help ensure endpoint patches happen quickly without fail. Tanium Patch offers a consistent, fast, and scalable patching process, allowing users to significantly enhance security and compliance.

One Client—No Extra Agents or Infrastructure: Patch at scale with little to no infrastructure and minimal downtime. Patch hundreds of thousands of systems on a single Tanium instance, without the use of distribution points and caching servers. There's no need for secondary relay, database, or distribution servers at different bank branches, retail locations, or geographically dispersed corporate offices.

Customized Patch Scheduling and Workflows: Deploy a single patch to a computer group immediately or perform more complex tasks. For example, use advanced rule sets and maintenance windows to deliver groups of patches across your environment at specified times.

Tanium Patch Is a Key Component of Endpoint Management: Immediately discover assets, remediate across diverse environments and operating systems, and monitor the performance of endpoints with real-time visibility, comprehensive control and rapid response. Tanium provides endpoint management at scale, all f rom a single platform for consolidated control and visibility.

Let's talk SecurePATCHING.

Contact us below:
sales@securesense.ca | securesense.ca
866-999-7506 | @securesense

Service At-a-Glance

- 24x7 support and management of patching, support and reporting requests
- Profiling, organization and management of assets
- Asset patch compliance tracking and remediation
- Patch program design and tuning, including patch module compiling, scheduling, approval chains and notifications
- Implementation of patch modules on a scheduled basis, validation and follow-ups of exceptions
- Intelligent workflows for OS and Application patching
- Ad-hoc, emergency and zero-day patching according to criticality-based SLAs
- Tracking and metrics designed to inform service improvement over time, demonstrate risk reduction and ROI
- Progress tracking, notifications od patching activity and regular status meetings
- Custom threat and network performance reporting