case study:

Randstad Technologies helps financial services client thwart hackers

redesigned security patching process reduces complexity, risks and costs

randstad technologies

When you're an investment services firm with more than $1 trillion in assets under your management, you're a prime target for hackers. Just think what would happen if an 80-year-old firm, running nearly 4,000 servers in 20 offices worldwide, suffered a breach of just one server. The impact could be catastrophic in terms of financial losses and customer goodwill. This was the case when a financial services firm discovered a major risk in its IT systems.

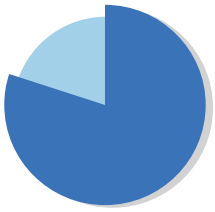
> As one well-known international electronics company found, it only takes one unpatched server to enable a serious breach.

Wrestling with a flawed security patching process, the firm was leaving itself exposed for too long — an opening that, if exploited, could jeopardize its clients' assets and their outstanding industry reputation. Since 2009, this company has relied on Randstad Technologies for a variety of IT operational support services. Because of this long-standing partnership and a history of successful collaboration, the firm once again turned to Randstad Technologies to structure a best-in-class security patch process with stunning results.

inability to deploy Windows security patches leaves the company vulnerable

Patch Tuesday, the second (and sometimes fourth) Tuesday of every month, is the day Microsoft releases security patches for its software. For this client, each Patch Tuesday posed a threat. It's the day nearly every malicious hacker attempts to breach the vulnerabilities of unpatched systems. Being in the financial services industry heightens the risk, as just one unpatched server could open the door to a costly breach — and this client had to quickly patch nearly 4,000 servers worldwide.

> One survey found **86 percent** of IT Management respondents report that Microsoft security patches are a consistent challenge.
>
> www.shavlik.com



This client's goal was to update its servers with Windows OS patches within a timeframe short enough to derail any attempted hack. Although receiving the updates and having the engineering team test them for flaws went smoothly, deployment to thousands of servers and in-house attempts to configure Microsoft's System Center Configuration Manager (SCCM) had fallen short. The company's existing processes, although well-conceived, did not completely eliminate its vulnerabilities. Furthermore, generated reports did not always correctly identify unpatched systems.

In many instances, the client was only 50 percent compliant by the Friday after Patch Tuesday. It was taking 20 people, often working four evenings, to reach 99.9 percent compliance. Like many financial services firms, this client relies heavily on technology to support its operations. The time and effort required to manage the Windows patching process was diverting attention from core business activities. After years of trying to hone the process itself, it was time to try something else.

Randstad Technologies fashions a process to attain rapid compliance

This client knew the Windows OS patching goals it wanted to meet. For critical patches, its goals were 99 percent compliance on day one after release and 100 percent compliance within 48 hours. For the

regular patching cycle, the goal was 100 percent compliance by the end of the month. The company engaged Randstad Technologies for a solution. The client's SLAs stipulated these targets, which reflected the degree of confidence it had that Randstad Technologies could develop a highly effective security patch process.

> The client needed a revamped updating process with little downtime and no business disruption.

Randstad Technologies' first step was to analyze the client's current system configurations and processes and make changes based on industry best practices and expertise. After establishing critical metrics around compliance and reporting, the team reconfigured SCCM to provide robust, timely, and accurate status updates and final reporting. They applied their technical expertise, deep familiarity with the Windows operating system, and lean IT principles to re-engineer and streamline the entire patching process.
This included:

- Standardized monthly pre-work to ensure targeted servers would be ready for patching.
- Configuration groups that established the relationships and dependencies between servers.
- A rigorous risk assessment to determine the order in which servers should receive updates.
- Automation of a number of manual tasks.
- Continual Service Improvement (CSI) specialists to conduct a CSI-focused event and integrate a CSI approach to the ongoing management of the patch process.

patching performance now soars: 99 percent compliance on day one, 100 percent within 24 hours

Randstad Technologies quickly took what was an imperfect and overly complex process and constructed a straightforward, lean approach that maximized the effectiveness of the people, process, and technology involved. The revamped processes allowed the client to achieve a previously unattainable level of compliance that also integrated ongoing CSI methods intended to further fine-tune operations.

> Randstad Technologies cuts 99.3 percent patch compliance target from four days to nine hours.

In the year preceding Randstad Technologies' assignment, overall performance levels stood at 43 percent compliant and 57 percent noncompliant. Additionally, a number of core updates had not been deployed, as Microsoft security updates were not noted as applicable despite their real need. Installing additional software made formerly compliant services noncompliant, which required manual intervention to fix. Inadequate reporting meant this often went undone.

The table below offers a summary of patch performance before and after Randstad Technologies took on this assignment.

security patch performance	before	after
99.3 percent Windows patch compliance	**4 days**	**9 hours**
number of people required to deploy security patches	**20**	**8**
number of man-hours to apply all patches each month	**320**	**105**
number of undeployed security updates	**45**	**0**
number of partly deployed security updates	**131**	**0**

annual labor savings total a quarter million dollars

Randstad Technologies' management of the patching process resulted in many important benefits. In addition to the significant cost savings realized through a two-thirds reduction in the number of required man-hours, the new patching process and technological improvements provided other positive results:

- Every SLA has been met for nearly a year.
- Within one hour of the update handoff, SCCM reporting provides a precise picture of the deployment's status.
- A focused CSI program drives process enhancements, including reordering the patching sequence and improving preparatory communications.
- Completing the patching has no impact on the client's business operations.
- Productivity has improved due to greater machine availability and reduced labor downtime.
- Avoidance of a security breach has prevented the associated negative publicity and lost goodwill.

fulfilling this client's challenging expectations, again

Based on previous operational support work, this client believed that Randstad Technologies could meet its stringent Windows patching SLAs, and it was proven right. The Randstad Technologies team did what they've done on so many similar projects — they took an imperfect methodology, acquired an understanding of the client's requirements and designed a process to reach the objective. In this case, they did so via technology that did not disrupt the client's business and allowed it to attain its patching goals. This client's vulnerability to security breaches has been significantly reduced, finally allowing peace of mind.

stay in touch:

visit us online | www.randstadtechnologies.com