



ORCS Web

Reducing Time and Staff Required to Meet Customer Service Level Requirements for Security and Compliance

CUSTOMER OVERVIEW:

ORCS Web is a web-hosting firm that has provided managed hosting solutions since 1996 for clients in more than 70 countries who develop and deploy their applications on Microsoft Windows platforms.

BUSINESS CHALLENGE:

ORCS Web needed an improved patch management solution to meet the aggressive security targets for system updates on a 24 hour basis without throwing more resources at the effort. In addition, a major initiative was undertaken to achieve PCI compliance.

SOLUTION:

After accepting an offer from Shavlik at a tradeshow promising that NetChk Protect could be implemented and operational within 2 hours, ORCS Web chose Shavlik's Netchk Protect and NetChk Configure to simplify and automate their patch process and ultimately achieve PCI compliance.

BENEFITS:

- Automated assessment and remediation
- Easy and fast to implement and administer
- Reduced spend-time, money and IT staff
- Achieved 100% PCI compliance

Scott Forsyth, Director Information Technology for ORCS Web

Looking for a more efficient patching solution, as well as supporting the needs of a customer to meet a PCI compliance deadline and avoid potential penalties, web-hosting firm ORCS Web was looking for a solution that could be implemented in days, not weeks or months. A chance visit to a booth at a tradeshow and a bold promise from a vendor that they could be implemented, operational, and achieving their patching goals in less than 2 hours seemed more fairytale than fact. But it wasn't. And now ORCS Web is helping customers of all sizes meet their PCI requirements.

ORCS Web is a web-hosting firm that has provided managed hosting solutions since 1996 for clients in more than 70 countries who develop and deploy their applications on Microsoft Windows platforms. As a leading web services provider, ORCS Web's customers are technically savvy and have built their business models based solely on web-based product and service delivery mechanisms. As a result, if their IT systems fail, so do their businesses. So ORCS Web must commit to some of the industry's highest standards of excellence in meeting their customer's stringent security and compliance service levels.

In early 2008, as ORCS Web's number of systems under management continued to grow, and they introduced Windows Server 2008 into the network, they reviewed their patching solution to accommodate greater levels of efficiency, and either upgrade from Microsoft SMS to Microsoft System Center, or consider a 3rd party solution. They looked to handle a growing number of servers in the same amount of time, and become PCI DSS compliant to help their clients meet the stringent requirements of the payment card industry. A major initiative was undertaken in 2008 to achieve PCI compliance.

The need for an improved patch management system, combined with the requirements for PCI compliance, presented a dual challenge that the team hoped they could address with a single technology solution.



ORCS Web

Some of the system and process challenges any new solution would need to address included the following:

- *The ORCS Web team supports more than 400 web servers that have high availability requirements, and many host public facing websites which must keep up with traffic demands on a 24/7 basis.*
- *Most of the servers ORCS Web supports have a very small maintenance window which requires them to be patched with system updates on a monthly basis, including physical and virtual machines, and the updates must be applied within a 4-hour window to ensure availability. ORCS Web was originally relying on Microsoft SMS and WSUS for its patching, but these solutions were not providing the control required to update the high availability servers within the strict maintenance window.*
- *At the time of their evaluation, Windows Server 2008 was only a beta, but ORCS Web was already using it in production. So any new solution had to provide support for it. The combination of Windows Server 2008 and older Microsoft OS software, along with a variety of legacy and new hardware created a diverse environment that needed to be centrally managed and patched.*
- *ORCS Web needed a solution that would not only meet the requirement to complete all updates within the 4 hour maintenance window, but one with flexible and powerful reporting features.*
- *As their customer's requirements for custom situations grew, it was necessary to support more patching windows for different time zones, staggered patching times for redundant web and SQL servers, and custom reports for certain customer needs.*

Meeting Patch and Vulnerability Requirements

Since ORCS Web hosts web sites exclusively on the Microsoft platform, it was natural for them to use Microsoft SMS and WSUS to update the servers used by their customers, and ORCS Web had been using and depending on those products for some time. However, because WSUS is a pull-

based solution, the timing of the updating tasks was not under ORCS Web's control as much as they liked, and last minute customer requests were difficult to accommodate. It was difficult to predict when the update process would be complete with either of these solutions, and as a result the 4 hour maintenance window was becoming increasingly difficult to satisfy. Another pain point that ORCS Web experienced with the SMS / WSUS solutions were the lack of quality reports. The reporting features of these packages were very limited, providing little, if any, information about update failures or other critical components of the update process. If a patch didn't work the first time, they had to perform a manual effort to determine which systems didn't receive the updates, causing a lot of rework for their IT staff.

Another important requirement was the need for flexibility to support clients in over 70 different countries around the world who have custom requirements. Being able to schedule scans ahead of time to support all the different time zones was critical. The solution also had to be very simple and cost effective to both implement and operate.

Scott Forsyth, Director of Technology for ORCS Web, was at an industry trade show and stopped by the Shavlik booth. He was intrigued after a brief demonstration of Shavlik NetChk Protect, "but what really caught my attention," Scott recalls, "was the promise by Shavlik's staff that NetChk Protect could be implemented and operational for us within 2 hours. The idea became sort of a challenge." So, figuring it would be a good investment in time, Scott agreed to put NetChk Protect to the test.

Accepting the challenge from Shavlik, Scott called his team on the spot and connected them with Shavlik and they were able to patch 48 ORCS Webs machines that very night during the scheduled patching window. Shavlik met their needs immediately with compelling benefits such as automated assessment, remediation, management and reporting



ORCS Web

features, and Shavlik's support for Firefox, Java, and other non-Microsoft 3rd-party applications/platforms. The powerful Shavlik scripting feature, which allows ORCS Web to identify any server and assign a specific patching window ("patch X server between 2 and 3 am on Saturday"), was also a key benefit. Amazingly," Scott says, "...we had NetChk Protect installed and operational in 2 hours. We used it to patch our systems that very night and that initial 'proof of concept' patch cycle went better than any production-level process we had previously implemented. We did a little fine tuning after that initial installation, but the solution basically went in and was ready to go in 120 minutes."

The real test for ORCS Web was to examine how NetChk Protect handled the system updates system-wide, and see how quickly they could be done to determine if the "4 hour maintenance window" requirement could be met. Because NetChk Protect offers unique agentless scan and deployment technology and is not dependent on agents, it hosts all of the patches, updates, and other resources necessary within the local network, everything is present and ready to be pushed to the servers before the updating activities even begin. This meant that ORCS Web administrators were able to schedule and complete system updates for all servers in a manner that was both simple and predictable. Best of all, the entire process took less than 4 hours, and the excellent reporting features allowed ORCS Web to show their customers precisely what systems were updated, and exactly what updates were applied. Any errors due to servers being off line, out of space, a lack of prerequisites, or other issues were clearly indicated by the reports.

Additionally, NetChk Protect's powerful scheduling features provided other bonuses. Because ORCS Web has customers all over the world, they get frequent requests to apply system updates at very odd times and hours. "It's common for some

of ORCS Web's larger customers to do their own testing of system updates prior to having those updates applied to production servers. "We get requests to patch systems in every time zone and hour imaginable. We used to have to manually perform and baby-sit each of these, but now with NetChk Protect's powerful features and user-friendly interface, we can schedule such tasks in advance and everything happens automatically, says Forsyth.

As for a cost effective solution, Scott says, "We are already seeing a return on our investment in NetChk Protect. Being able to automate the entire patch and vulnerability process has significantly reduced the amount of time and effort we spend doing this critical activity. Previously it took about 20 hours to prep for patching, not counting actual patching, and this solution brought that time down to about one hour per week of preparation. The ability to schedule scans ahead of time, taking only a few minutes to set up, frees up our IT resources allowing them to do other activities. After a couple months of perfecting the process, patching is substantially easier than in the past. The monthly patching process requirements are a fraction of what they were."

Helping Customers Achieve and Maintain PCI Compliance Status

To help their customers achieve compliance, ORCS Web needed a configuration management solution to automatically generate robust reports that demonstrate compliance with PCI requirements to prove to auditors that they are compliant. The reports they were getting from SMS/WSUS lacked clear and direct mapping of policies and configuration controls to the PCI DSS framework making it difficult to prove compliance to auditors.

The simplicity and automation of Shavlik enabled ORCS Web to produce their required quarterly compliance reports to



ORCS Web

auditors with confidence. They achieved 100% PCI compliance in record time, resulting in a measurable ROI and saving the client more than \$50,000. This added expertise has also had the bottom-line benefit of enabling ORCS Web to easily bring in new clients who require PCI compliance.

ORCS Web tested Shavlik NetChk Configure, Shavlik's configuration management solution, and found the installation process to be rapid and simple. They installed the product quickly, following the easy-to-use set up wizard. NetChk Configure discovered servers previously undetected by SMS that were out of date and required substantial effort (and disk space for the large number of patches) to bring into conformance. Working through these issues, ORCS Web found Shavlik's technical support team to be very responsive and helpful. A call to the Shavlik support line put ORCS Web immediately in touch with a live person who helped resolve their issues, so they were able to proceed without disruption.