monarx

A Nexigen Digital Success Story with Monarx

A Leading Australian Hosting Company Needs a Better Malware Solution

Client: Nexigen Digital

Industry: Digital Infrastructure and Web Hosting

Head of Infrastructure: Bradley Silverman

Partnership Duration: 1 year (and counting)

Solution: Monarx Complete Protection

Since its founding in 2008, Nexigen Digital, a 100% Australian-based company, has evolved from a small web hosting company into a powerhouse of digital infrastructure, serving over 300,000 businesses across Australia. With over 250,000 websites hosted on their platform, Nexigen Digital is committed to supporting Australian businesses through cutting-edge technology and dedicated support. However, with significant growth, new challenges, such as phishing and spam-related incidents, started to increase.

> “Monarx found more threats during our testing than any other solution, and it’s been a game-changer for us.”
>
> **Bradley Silverman**
> Head of Infrastructure, Nexigen Digital

monarx

Challenges of Rapid Growth and Security Needs

Managing a fleet of 1,000 servers, the company increasingly struggled with malware infections on customer websites, leading to phishing attempts and spam. Bradley Silverman, Nexigen Digital's Head of Infrastructure, described the impact this had on operations and reputation: "Our staff was spending valuable time handling complaints related to compromised sites, and it was taking a toll on our reputation." Silverman stated that even though it was often due to outdated plugins on customer websites, the company was still bearing the brunt of the issues.

Recognizing the need for a more robust and reliable solution, Nexigen Digital evaluated potential options. They focused on the following key criteria to find a solution that could handle their security needs:

- **Real-time malware detection:** Immediate threat identification without relying on scheduled scans.
- **Minimal system impact:** Low resource usage, particularly CPU load, during operation.
- **Seamless deployment:** A solution that could be integrated across their server fleet without interrupting customer services.
- **File cleaning versus quarantine:** A preference for cleaning infected files in real-time, allowing servers to continue running without interruption.
- **Price:** Strong value at a competitive price point.

Monarx met these expectations and outperformed other options during testing by detecting more threats with less impact on system resources. After rigorous testing, Monarx stood out for its real-time malware detection and unique 'clean file' approach, which resolved threats without disrupting service.

A Seamless Integration with Immediate Impact

Deploying Monarx across their server fleet was a turning point for Nexigen Digital. The entire fleet moved to Monarx in one month, thanks to Monarx's flexibility and Nexigen Digital's use of an Ansible playbook (a YAML script that automates software deployment across multiple servers). There was no need for a phased rollout. Monarx worked from day one without complications.

During the rollout, Nexigen Digital requested a small change to Monarx's cPanel plugin. "Monarx promptly made the modification, and it noticeably increased the plugin's usability for our customers," said Silverman, emphasizing Monarx's flexibility and dedication to customer support.

Reflecting on the transition, Silverman noted, "The implementation was incredibly easy, and Monarx's 'clean file' approach made it less intrusive for us and our customers." This seamless deployment improved operational efficiency and allowed Nexigen Digital to provide a better customer experience without disruptions.

monarx

> “Since switching to Monarx, we’ve seen a significant reduction in customer complaints and support tickets. It’s given our team the breathing room to focus on proactive solutions rather than constantly putting out fires.”

Bradley Silverman
Head of Infrastructure, Nexigen Digital

Improving Security and Performance Metrics

Monarx’s deployment quickly proved to be more than just an upgrade in malware detection; it significantly improved Nexigen Digital’s overall infrastructure performance. With the new solution, Nexigen Digital saw a marked reduction in CPU load during scans, which had previously strained resources. “What stood out immediately was how much lighter the system load became,” Silverman noted.

Nexigen Digital’s previous solution relied on scheduled scans, which were slow and used a lot of resources. These scans left significant gaps between intervals, allowing threats to operate undetected for extended periods. The resource-heavy nature of the scheduled scans also caused noticeable performance degradation. These challenges made it difficult for Nexigen Digital to maintain optimal server performance while addressing malware issues. The new malware detection process allowed the team to balance resources across their server fleet.

The real-time protection from Monarx produced immediate results. The number of detected infected files increased from tens of thousands to over a million in the first month, as Monarx identified many previously undetected threats. By preventing malware infections before they cause further issues, Monarx maintains performance without needing resource-heavy scheduled scans. “Monarx allows us to catch threats before they affect our customers, which has a huge impact on uptime and system reliability,” Silverman explained. This new proactive security directly impacts Nexigen Digital’s ability to deliver uninterrupted service and maintain their strong reputation among the 300,000 businesses they serve.

In addition to reducing malware infections, Nexigen Digital experienced a dramatic decrease in complaints to their NOC team. Monarx’s proactive scanning prevented phishing and spam incidents from affecting the server fleet, helping Nexigen Digital avoid IP reputation issues, which had previously been a concern.

The number of detected infections stabilized over time, with the monthly average reaching around 250,000-far fewer than the initial spike of over 1 million in the first month. With fewer security incidents to address, Nexigen Digital’s support team saw a significant decrease in customer complaints. This, in turn, allowed the team to shift focus from reactive issue resolution to more forward-thinking improvements in service delivery.

With Monarx, Nexigen Digital staff and customers can see what was infected and which files were quarantined. Files are often cleaned without the customer's knowledge. On the rare occurrence that a false positive comes up, marking a file as “safe” will reinstate it on the entire fleet, so an issue that could have taken hours or days to resolve is solved in minutes.

monarx

Looking Ahead: Expanding Security and Exploring New Features

With Monarx's protection integrated into Nexigen Digital's infrastructure, the Australian hosting company is considering additional features offered by Monarx to help expand Nexigen Digital's security offerings. One such feature is Monarx's WordPress Site cleanup service, where customers pay for professional support to clean compromised sites. This service aligns with Nexigen Digital's mission to provide clients with comprehensive protection, safeguarding their systems while allowing customers to address potential vulnerabilities.

Nexigen Digital is also interested in sending detailed reports to customers, alerting them when their websites have been cleaned of infections. The report would provide customers with insights into potential vulnerabilities and encourage proactive website maintenance, such as upgrading compromised plug-ins. This transparency would help Nexigen Digital's customers stay ahead of potential threats and strengthen their trust in the service.

As Nexigen Digital continues to grow and evolve, Monarx remains a key partner in maintaining the security and performance of their digital infrastructure. Bradley Silverman expressed confidence in the future of this partnership, stating, "Monarx has delivered exceptional results, and we're excited to explore more of what they offer as we continue to scale our operations."

Key Takeaways

Proactive Security
Real-time malware detection and infection resolution.

Stabilized Protection
Ongoing detection of 250,000 infected files per month.

Immediate Impact
Over 1 million threats detected in the first month.

Enhanced Performance
Reduced CPU load during scans and fewer customer complaints.