



Micromuse Secures Business Critical Microsoft Servers with the Blue Lane PatchPoint System



Micromuse delivers industry-leading business and service assurance solutions to organizations worldwide. During the 14 years since the company's inception, their flagship Netcool® brand has become synonymous with scalable, real-time, end-to-end management of complex IT and telecommunications infrastructures. The comprehensive range of Netcool solutions enable service providers, equipment providers, corporate enterprises, and government agencies to extract maximum value from their mission-critical applications, systems, and networks.

Problem: A global company and the leading provider of ultra-scalable, real-time business and assurance software, Micromuse, Inc., like most companies today, is contending with an ever growing number of vulnerabilities affecting their production systems that need to be frequently patched and updated. However, frequent patching is not a viable solution for any production environment because patches can often break applications, making production environments unusable. Moreover, testing is a time-consuming process which leaves business critical applications at risk.

Micromuse also uses IDS/IPS devices to monitor traffic but have too many false positives that are impossible to see and understand to be able to use them in place of patching. According to Bruce Fingles, CIO of Micromuse, "An IPS looks at patterns and tries to ferret out offending traffic but can end up blocking everything, even legitimate traffic. Hundreds of thousands of events are tagged and almost none are malicious." Still, Micromuse will continue to use IPS/IDS as a forensic tool to look at specific network traffic.

Solution: "We chose the Blue Lane™ Technologies PatchPoint™ System for two reasons," said Fingles, "first and foremost, to protect our mission-critical servers and applications. As a result, I

now have peace of mind knowing that my systems are up and running and secured. Second, the PatchPoint System takes the pressure off of having to install the vendor patch immediately. It provides us with the time to perform proper tests on our servers and applications without compromising the security of those systems. Micromuse has also recognized significant cost savings because we don't have to stop everything to test a patch or risk potential downtime."

Micromuse has deployed PatchPoint in front of their mission critical servers at their headquarters in San Francisco and in their London office, where they have been up and running for six months. They anticipate installing in four more locations, in front of their servers in all of their satellite offices.

Fingles also said that the system was easy to install and he likes the patch-centric nature of the PatchPoint Enterprise Manager, which is easy to use and charts vulnerabilities that are patched as well as all traffic that has been patched.

Micromuse is protecting their business and saving time and money, allowing them to enhance their business operations while securing their mission-critical applications.