



## Universal Instruments Corporation

### UIC Protects Global Infrastructure with PatchLink Update™

Global electronics productivity specialist Universal Instruments Corporation (UIC) places patch and vulnerability management at the top of its layered security program. With offices and satellite manufacturing locations spanning 30 countries and more than 1,500 employees, UIC Network Analyst Jeff Dmochowski, who is responsible for UIC worldwide network operations, minimizes network downtime and tracks system compliance and vulnerability risk on a 24x7x365 basis. UIC provides innovative circuit, semiconductor, and back-end assembly technologies and equipment, integrated system solutions, and process expertise to manufacturers in every sector of the global electronics industry. This Fortune 500 Company's research and development processes, equipment, systems, and software have brought electronic assembly to its current pinnacle of sophistication. In support of its aggressive business model, UIC sought to improve its security patch and vulnerability management posture through the implementation of PatchLink's PatchLink Update™.

#### UIC's Challenge:

#### Improving Network Security through Patch Deployment & Validation

"Learning from experience" is often realized in business. For UIC, this idiom came to bear when the Blaster worm hit and was able to quickly and tenaciously infiltrate the network regardless of VPN or firewall protection.

“ There was no patch installation enforcement. Consequently, only about half of our users installed the patch. The worm was able to reach a critical mass and bring down our network a short time after the Blaster outbreak. ”

Jeff Dmochowski - UIC Network Analyst

Dmochowski now understands the criticality and complexity of protecting today's criticality and complexity of protecting today's enterprise network firsthand. According to Dmochowski, "Blaster gave UIC its first taste of vulnerability. What's interesting is that we actually detected this problem early on and distributed the proper patches to our user community via email.

Unfortunately, there was no patch installation enforcement. Consequently, only about half of our users installed the patch. The worm was able to reach a critical mass and bring down our network a short time after the Blaster outbreak. We soon realized the need for a better method of distributing and enforcing these critical security patches."

Like many other companies, UIC presumed that careful attention to isolating its corporate network from the Internet with a firewall and providing thorough virus scanning on all machines and inbound email would keep the global network protected.



#### KEY FACTS:

- Fortune 500 company with 1,500 employees in over 30 countries
- Patches were distributed to end users through email
- Only 50% of users installed the critical patch to stop Blaster



However, what UIC was not prepared to deal with were the threats being released on the network through VPN connections as well as those instigated by rogue mobile computers too new to be detected by UIC's anti-virus signatures. Without a clear patch baseline or the ability to satisfactorily track and inventory software assets, UIC quickly understood the need to better equip itself with an automated security patch management solution that also encompassed intuitive and extensible features and capabilities.

### **UIC Powered by PatchLink**

Dmochowski and his team immediately began researching and testing security patch and vulnerability management offerings from PatchLink Corporation, Shavlik, St. Bernard, Ecora, and Microsoft. Having proven its abilities in the marketplace, PatchLink Update quickly escalated to the top of UIC's list as the product best able to provide the flexibility and speed to efficiently meet market security IT requirements. "We did a thorough analysis of the various product offerings that could be used to improve our Windows patching success," explains Dmochowski. "We evaluated PatchLink Update against several other products. A key factor in our decision was PatchLink's secure agent-based technology which allows UIC to inventory and extract useful system information, as well as the relative ease of rapidly deploying a global security patch and vulnerability management solution."

Tackling the growing problem of non-compliant mobile devices connecting to the corporate network was also very important to Dmochowski. PatchLink's early accomplishments with end-point security centered on patch management made UIC's selection of PatchLink Update an easy decision.

### **Investing in Proven Leadership**

With more than a decade of security patch and vulnerability management experience, PatchLink continues to help make organizations — and their customers — more secure. It's only fitting that the global leader in electronic assembly chose to align itself with a partner that understands the criticality of "getting it right" for the customer.