

# TippingPoint Quarantine Integration Solution with Patchlink

SOLUTION – Patchlink

The innovation of TippingPoint's in-line attack protection and Patchlink's comprehensive Update solution strengthens enterprise network and end-points. As attacks grow in sophistication and end-points proliferate, the challenge of keeping them all safe can be a daunting task for many organizations.

## Summary

In-depth security is best met through a layered approach with best of breed solutions. The TippingPoint IPS solution coupled with Update from Patchlink gives real-time attack protection and vulnerability resolution. When coupled with TippingPoint's Quarantine, an automated policy based security response is enacted, saving IT organizations the need for manual responses and preventing malware threat propagation.



TippingPoint's Intrusion Prevention System (IPS) provides real time deep packet inspection to identify and stop attacks before they reach critical network assets. Working with the TippingPoint Security Management System (SMS), the TippingPoint Quarantine feature can provide the same real-time protection that can be applied to any observed behavior for an automated response to security incidents.

Patchlink Update will reduce the vulnerabilities available to exploits by keeping systems up to date. New vulnerability updates are delivered to the Patchlink Update Server and then the administrator can determine which need deployment and to which system targets.

TippingPoint's Quarantine feature allows security groups to automate responses to security events. Administrators can define the conditions and targets to include a quarantine plus the range of actions to undertake. Typically users trigger alerts to specific administrators depending on the nature of the attack or its target. More sophisticated responses have infected devices directed to self-remediation steps or when justified, switch level actions such as movement to a secure VLAN or removed from the network entirely.

## The Common Solution

End-point protection is best served by in-depth security and best of breed solutions. The TippingPoint and Patchlink solutions provide exactly that level of coverage. The TippingPoint IPS gives you optimal protection for network-based resources while Patchlink's provides pro-active

protection. Together they combine real time reaction protection and vulnerability reduction. This integration enables TippingPoint Quarantine to isolate an end-point and have Patchlink remove the vulnerability by updating the device. Once the vulnerability has been resolved according to policy then the suspect end-point can be Un-Quarantined.

The combined product set can combine to solve common problems found in any network computing environment. One such challenge would be the discovery of an infected end-point spewing attacks across the network. In this case the TippingPoint IPS would block the attacks and then initiate a Quarantine. In this particular case, it would be a compound automated response. The TippingPoint policy would send a message to the administrator noting the attack, then the device would be isolated on a secure VLAN and all Web traffic would be directed to the Patchlink resolution page. Once the system has been updated then Patchlink would send the TippingPoint Security Management Server an Un-Quarantine message. Upon receipt, the TippingPoint SMS would release the now updated device back onto the regular network.

## How Does It Work?

With TippingPoint's SMS 2.5 release, the power and flexible security response of Quarantine enables third party vendors such as Patchlink's Update to request either a Quarantine or Un-Quarantine action for a suspect end-point. With a simple and authenticated Web request the tools can cooperatively work together.