



**CONTACT:**

Kate Fly  
TippingPoint, a division of 3Com  
512.681.8218  
Kate\_fly@3com.com

**LANCOPE, MAZU NETWORKS, AND PATCHLINK TEAM WITH  
TIPPINGPOINT FOR INTEGRATED SECURITY SOLUTION**

*Third Party Security Solutions Now Auto-Remediate and Enforce Policy via  
TippingPoint's Quarantine Capability*

**AUSTIN, TX. – January 15, 2007** –TippingPoint, a division of 3Com and the leader in intrusion prevention systems, today announced third party security solutions can interoperate with the industry's only IPS-based quarantine capability for active security policy enforcement. Lancope, Mazu Networks, and PatchLink now work directly with TippingPoint™ products to quarantine endpoints in violation of network policies as well as automate endpoint remediation.

TippingPoint's quarantine feature was launched in February 2006 as an innovative IPS capability that leverages network infrastructure to isolate and resolve any internal sources of malicious activity. By ensuring any device can be contained for remediation, businesses maintain a healthy network and block the internal spread of attacks, significantly reducing technical support calls and costs.

The TippingPoint Intrusion Prevention System (IPS) quarantine capability works with TippingPoint's Security Management System (SMS) and existing network switches or management systems to block malicious traffic, contain infected endpoints, and provide support for remediation of infected devices. Now, quarantine is interoperable with third party patch and vulnerability management solutions for automated remediation, and with network behavior analysis (NBA) tools to move from policy violation alerting to in-line policy enforcement. TippingPoint's quarantine feature offers a broad set of enforcement capabilities including displaying a remediation Web page,

blocking a port, or redirecting the infected endpoint to a secure VLAN based on administrator policy.

“This is an important step in the evolution of enterprise security,” said Neal Hartsell, vice president of marketing for TippingPoint. “Security is getting more complex to administer and manage. One way to alleviate complexity is to extend the power of our IPS’s traffic classification and policy enforcement strength to patch management and network behavior analysis tools, enabling customers to maximize their existing security investments, automate endpoint security, and reduce the cost and complexity of overall security policy enforcement.”

With the integration of PatchLink, the global leader in security patch and vulnerability management, infected users who request network access can now be automatically directed to a personalized PatchLink Web site that guides users to download specific patches that eliminate infections and remediate vulnerabilities.

“The integration between PatchLink and TippingPoint truly enables customers to automate security incident response,” said Rich Hlavka, PatchLink’s senior vice president of business development. “By combining our industry leading remediation engine with enterprise class intrusion prevention, we’re enabling users to automatically enforce security policies and remediate vulnerabilities while greatly reducing the risks and costs associated with IT security incidents.”

Additionally, TippingPoint now integrates with two leading NBA systems, Lancope and Mazu Networks. These systems compile data from multiple network devices and provide visibility into network activity to improve internal security and IT operations. Through the integration, the NBA system can send commands to the TippingPoint system for quarantine and policy enforcement.

“This integration brings together best of breed NBA and IPS technologies to enhance security postures and improve overall network health, while reducing the total cost of securing the enterprise,” said Harland LaVigne, president and CEO of Lancope.

“TippingPoint’s flexible quarantine capabilities complement StealthWatch’s end-to-end network visibility to ensure network security, performance, and availability. Together, we are furthering our commitment to provide our customers with the most expedient and effective means of mitigating risks to the network and eliminating threats.”

“The combination of Mazu with TippingPoint IPS provides customers with a powerful solution for addressing a multitude of network operations and internal security challenges,” said Paul Brady, CEO of Mazu Networks. “While Mazu provides enterprises with a global view of how users, applications, hosts, and devices behave on a network, TippingPoint enables a more granular enforcement option. Now the market’s leading IPS and NBA products can work in conjunction to greatly improve network and security operations for enterprise customers.”

Quarantine and associated software capabilities are available at no charge to TippingPoint IPS customers. Third party solution integration is supported in release 2.5 of the TippingPoint Security Management System, available since October. For more information on TippingPoint’s Quarantine Protection, please visit: [http://www.tippingpoint.com/technology\\_quarantine.html](http://www.tippingpoint.com/technology_quarantine.html).

### **About Lancope**

Lancope is the provider of StealthWatch, the most widely used network behavior analysis (NBA) and response solution that unifies behavior-based anomaly detection and network optimization capabilities to protect critical information assets and ensure network performance by preventing costly downtime, repair and loss of reputation. StealthWatch streamlines security and network operations into one process, reduces time and resources, and eliminates the costs and complexity associated with non-integrated point products. Both OPSEC and Common Criteria-certified, StealthWatch was named Best of Show at Interop2006 and InfoWorld 2005 Technology of the Year. Defending the networks of Global 2000 organizations, academic institutions and government entities, StealthWatch protects hundreds of enterprise customers, more than all direct competitors combined. Lancope’s Technology Alliance Partners include Cisco Systems, Foundry Networks, ArcSight, IBM Tivoli, TippingPoint, SecureWorks, CheckPoint and A10 Networks. Lancope is a privately held, venture-backed company headquartered in Atlanta, Georgia. For more information, call 888-419-1462 or visit [www.lancope.com](http://www.lancope.com).

### **About Mazu Networks, Inc.**

Mazu Networks provides continuous global visibility into how users, applications, hosts and devices are behaving on a network, and detects if there are meaningful changes from

their typical behavior that indicate a network performance issue, a security threat, or an application problem. Through Mazu, enterprises understand usage patterns, consumption rates and dependencies between users, applications and network infrastructure. Only Mazu offers continuous global visibility; rapid, agent-less deployment, automatic and custom behavior analysis; and superior integration with network and security products. Mazu's customers optimize their network infrastructure to support their business, secure their internal networks and maximize application availability. For more information, please visit [www.mazunetworks.com](http://www.mazunetworks.com).

### **About Patchlink ® Corporation**

PatchLink® is the global leader for security patch and vulnerability management solutions, delivering comprehensive, multi-platform assessment and remediation for continuous protection across the enterprise. Offering the most comprehensive platform and application support, PatchLink maintains the largest tested and most up-to-date security patch repository, enabling organizations to accurately assess and remediate vulnerabilities based on established industry best practices. Currently protecting thousands of commercial and government organizations and millions of PCs and servers worldwide, PatchLink effectively eliminates vulnerability risks and enforces security and compliance policies while reducing overall IT costs. PatchLink is headquartered in Scottsdale, Arizona and was founded in 1991 by Sean Moshir.

### **About TippingPoint, a division of 3Com**

TippingPoint, a division of 3Com, is the leading provider of network-based intrusion prevention systems. The TippingPoint IPS is the most decorated in its industry. For a full list of awards, visit [http://www.tippingpoint.com/products\\_certifications.html](http://www.tippingpoint.com/products_certifications.html). Our innovative approach offers customers unmatched network-based security with ultra-high performance, scalability and reliability. TippingPoint is based in Austin, Texas, and can be contacted through its wWeb site at [www.tippingpoint.com](http://www.tippingpoint.com) or by telephone at 1-888-TRUE-IPS.

### **About 3Com Corporation**

3Com Corporation (Nasdaq: COMS) is a leading provider of secure, converged voice and data networking solutions for enterprises of all sizes. 3Com offers a broad line of innovative products backed by world class sales, service and support, which excel at delivering business value for its customers. Through its TippingPoint division, 3Com is the leading provider of network-based intrusion prevention systems that deliver in-depth application protection, infrastructure protection, and performance protection. 3Com also is the majority owner of Huawei-3Com Co., Ltd. (H3C), a China-based joint venture formed by 3Com and Huawei in November 2003. H3C brings innovative and cost-effective product development and manufacturing and a strong footprint in one of the world's most dynamic markets. For further information, please visit [www.3com.com](http://www.3com.com), or the press site [www.3com.com/pressbox](http://www.3com.com/pressbox).

Copyright © 2006 3Com Corporation. 3Com and the 3Com logo are registered trademarks and TippingPoint is a trademark of 3Com Corporation or its subsidiaries. All other company and product names may be trademarks of their respective holders.

###