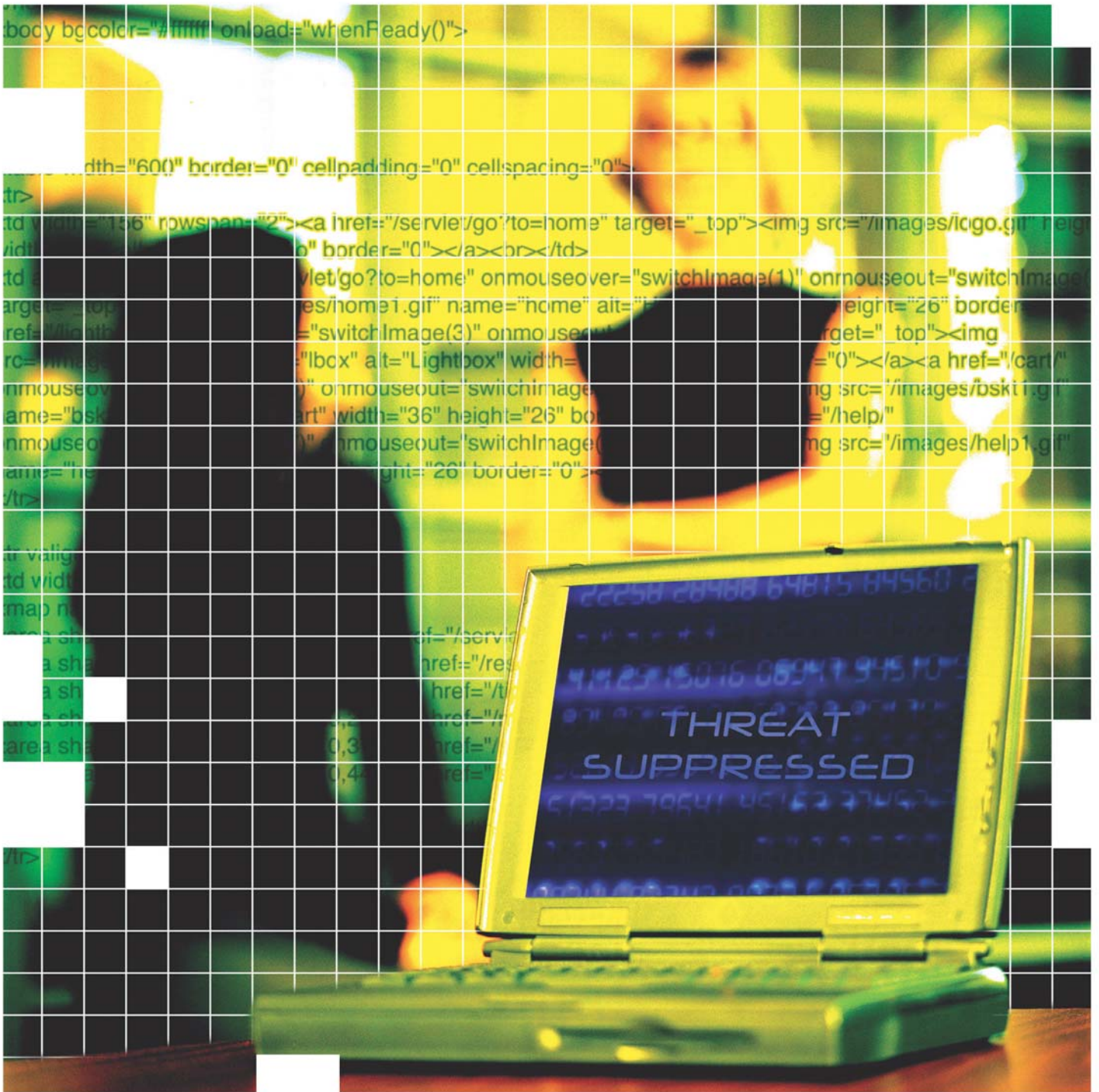# UNIFIED NETWORK-DEFENSE APPLIANCES...

A SOLUTIONS PRIMER

Security is more than just a buzzword.

It is a state of being.

Networks, the lifeblood of most corporations, demand security.

Yet, the medieval fortress-and-moat defense offered by most network security tools provides little protection from sophisticated hacks and frequent cyber attacks.

Protection takes on a whole new meaning in the 21st century. The same technology and equipment that enable networks to operate at high speeds also provide superhighways for viral diseases to spread like wildfire – and they proffer dormant threats yet to be invoked.

TippingPoint Technologies' UnityOne™ Threat Prevention Appliances are the first integrated appliances for enterprises seeking true, continuously updated protection for their networks at multigigabit speeds. UnityOne is composed of three interlocking building blocks – Vulnerability Assessment, Intrusion Detection, Firewall/VPN – built on top of a high-speed security processor– bound by a single management system. UnityOne offers real, trusted protection for both WAN and LAN applications. UnityOne does not just detect threats. It blocks and suppresses threats.

Security Management System		
UnityOne™ OS		
Vulnerability Assessment	Intrusion Detection	Firewall/ VPN
Threat Suppression Engine™		

Untrusted → → Trusted
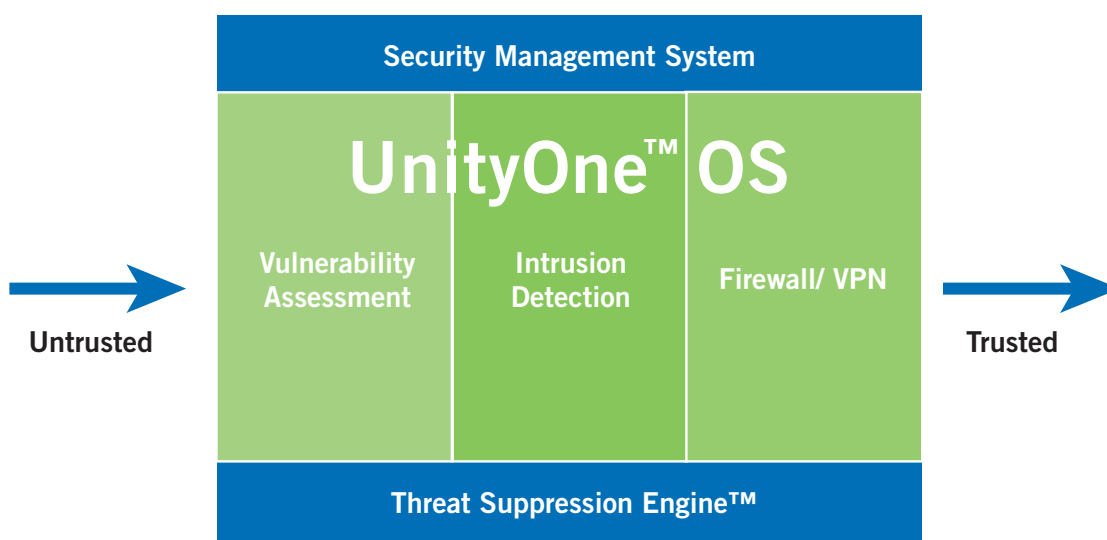
UnityOne™ Interlocked Capabilities

Blocks over 2000 attack types.

The Unity of One
UnityOne™ Threat Prevention Appliances

UnityOne™ Threat Prevention Appliances combine the best of high-speed security processors, a collaborative security application suite, and integrated management. Whether protecting the perimeter or critical Intranet interconnection points, TippingPoint's UnityOne offers strong resistance that self-adjusts to the color and shade of the enterprise environment and potential threats.

Current security tools are disparate devices, such as vulnerability assessment scanners, intrusion detection systems and firewalls, each with its own management system. This mixed nuts solution may be protein to some, but to manage a network with this fragmented approach to security is – dare we say – NUTS!

In contrast, TippingPoint offers a complete set of high-speed security solutions that are comprehensively managed and updated by one active, interlocking system.

Anchored by the high-speed **Threat Suppression Engine™**, TippingPoint's UnityOne Threat Prevention Appliances offer an all-in-one security solution that thrives at speeds up to 2.0 Gbps. UnityOne provides utmost reliability and protection from both external and internal threats. The UnityOne system is composed of the following key elements:

• **Threat Suppression Engine™.** At the heart of TippingPoint's solution is a powerful high-speed processing engine that offers breakthrough enabling technology.

• **UnityOne™ OS.** Integrated in one system are the functions of a firewall, an intrusion detection system and a vulnerability assessment scanner. This unique system provides continuous threat prevention that assesses, detects and suppresses known hostile code, while eliminating false alerts. Threats are assessed continually to ensure up-to-date coverage for the network.

UnityOne offers a front-line defense at the perimeter, the extreme edge and within the LAN. Easily installed, the UnityOne is a plug-n-play appliance that starts working for the enterprise right out of the box.

UnityOne™-2000

The UnityOne™-2000 large enterprise solution delivers full perimeter, extreme edge and Intranet multi-zone network-defense at 2.0 gigabits per second speeds.

UnityOne™-600

The UnityOne™-600 small & medium enterprise solution delivers perimeter network-defense at 600 megabits per second speeds.

Threat Suppression Engine™
The Heart and Soul of UnityOne™

The heart of UnityOne, the Threat Suppression Engine, is designed to handle security-specific functions at gigabit speeds and execute sophisticated threat suppression signatures and anomaly algorithms to protect the enterprise.

These functions include: **Address Translation, Flow Assembly, Classification, Stateful Inspection, Content Searches and Traffic Shaping.**

Network and Port **Address Translation** are critical for hiding the true internal network addresses from hostile outsiders. TCP **Flow** and fragmented packet reassembly are critical for detecting and thwarting disguised attacks (where independent packets may appear harmless).

Classification of packets and flows requires sophisticated header processing at OSI layers 2-4 for finer-grain packet filtering.

Deeper unanchored payload **Content** processing is needed for higher layers. Polymorphic attacks require matching of complex patterns (based on regular expressions) in order to be detected and blocked.

Stateful Inspection is needed to selectively allow applications to penetrate a firewall through dynamic ports.

Traffic Shaping is a powerful way of protecting and prioritizing mission critical traffic and containing potential DoS traffic.

Security Management System™

TippingPoint's Security Management System (SMS) is a pre-configured management appliance that ensures a comprehensive and simple user interface to manage your security environment. The SMS provides a single console from which to configure, monitor and update up to 1000 UnityOne Threat Prevention Appliances per SMS enterprise-wide.


Threat Management Center

TippingPoint's Threat Management Center (TMC), the central intelligence bureau for UnityOne, is staffed 24/7 with TippingPoint's security experts. The TMC searches for emerging vulnerabilities, new signatures and algorithms to defeat attacks on the enterprise network. Customers have the option of two services – Web Access and **Digital Vaccine™**.

Web Access is a web-based reference for IT administrators to access the latest threat suppression signatures.

A real-time continuous update service, Digital Vaccine delivers signatures and algorithms to UnityOne enterprise systems.

TippingPoint has taken a whole new approach to signatures and algorithms. The TMC pre-hardens signatures to ensure 100% reliability.
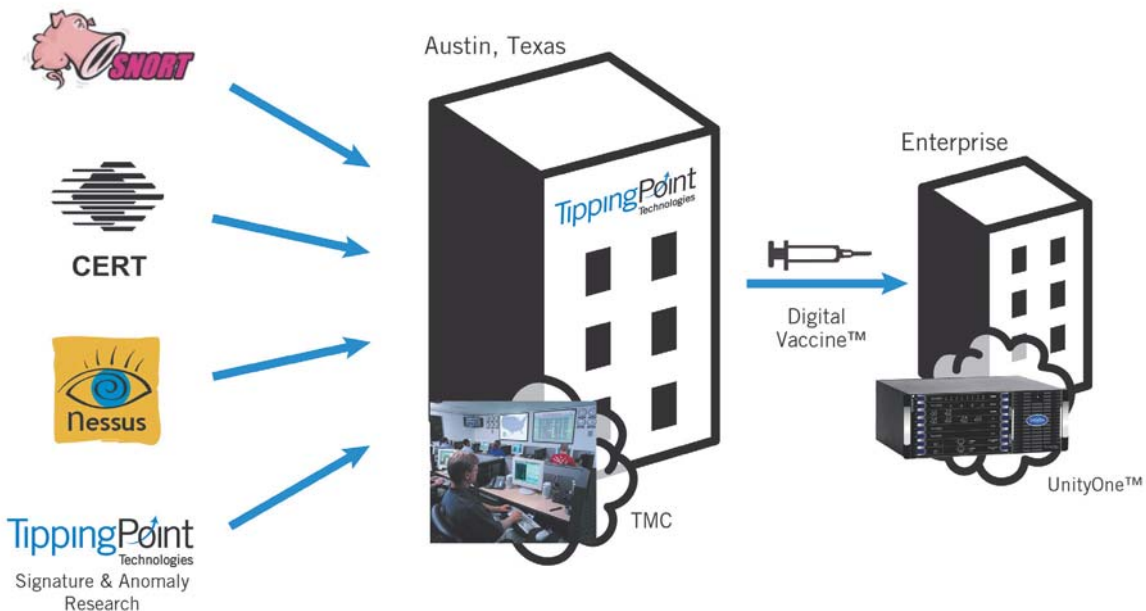
Deploying UnityOne™

Enterprise Solutions

With the UnityOne™-2000 and UnityOne™-600, TippingPoint offers unified network-defense appliance solutions specifically designed to meet the different needs of the large enterprise (LE) as well as the small & medium enterprise (SME).
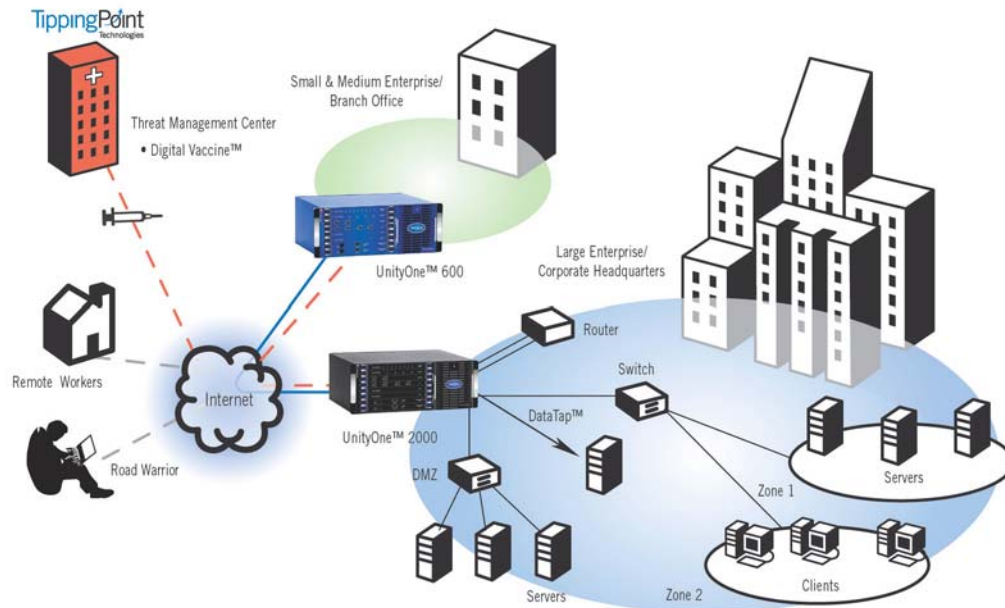
Enterprise defense starts with UnityOne's Perimeter, ExtremeEdge and Multi-Zone solutions.

Perimeter Protection

UnityOne provides unprecedented unified protection of the enterprise perimeter. At the perimeter, UnityOne protects the flow of information between the LAN, DMZ and WAN. In addition, UnityOne provides VPN capability to manage and extend secure connections across the Internet.
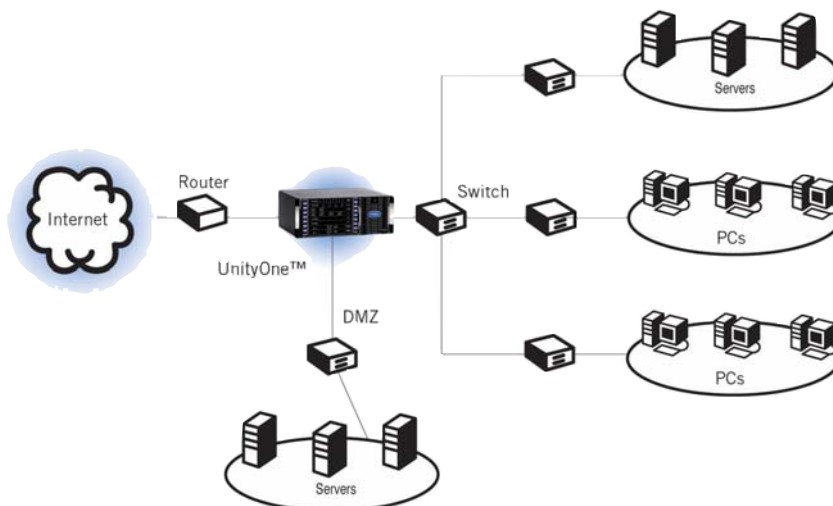
ExtremeEdge

Router vulnerabilities are increasingly being targeted by attackers. UnityOne is equipped with ATM WAN interfaces, so that it can be installed at the WAN access point in front of the router, while at the same time protecting the LAN and DMZ of the Intranet. In effect, UnityOne wraps around the router, protecting it from attacks.
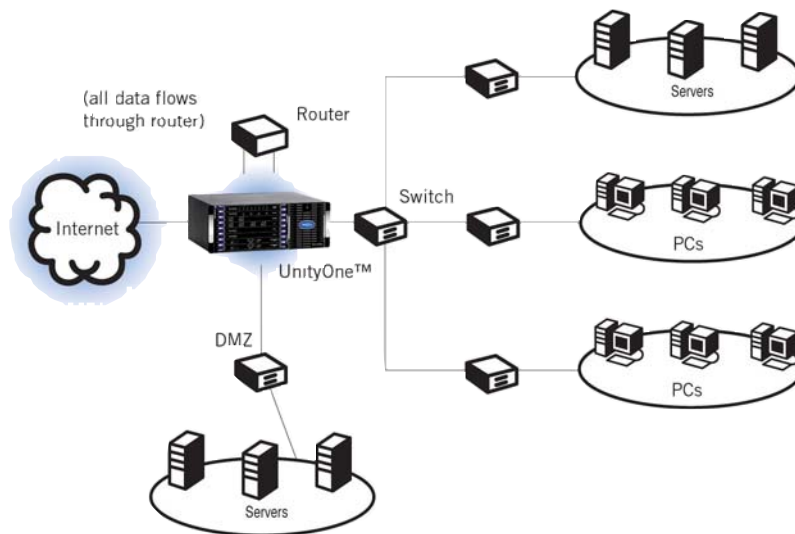
Multi-Zone

UnityOne is designed to handle the high bandwidth of Intranet connections and can be configured to provide an internal layer of protection between LAN segments. The UnityOne DataTap™ can be used to redirect Web traffic for URL filtering, or to mirror selective traffic for tracking and analysis.
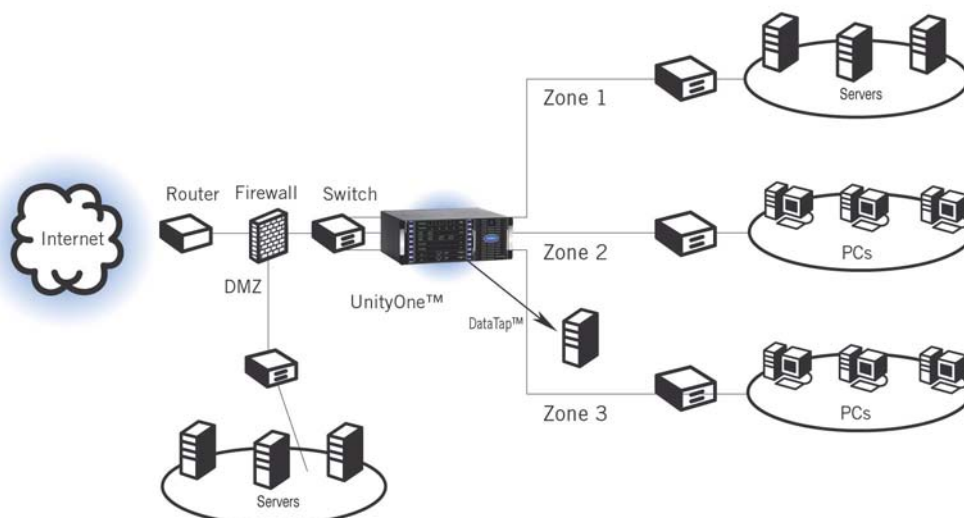
Benefits of Unification
Speed, Strength, Simplicity & Savings

Speed

Thanks to the Threat Suppression Engine's specialized hardware, UnityOne delivers, at speeds up to 2.0 Gbps, enterprise security has never been faster.

Strength

UnityOne delivers unsurpassed vulnerability assessment, attack *detection* and *prevention*, benefiting from the strength of a unified, interlocked system. With Digital Vaccine, world-class reconnaissance starts and ends by steadily and consistently monitoring and updating the major live threat databases - **UnityOne™ blocks over 2000 attack types.**

Simplicity

The riches of finding security solutions capably managed under one system should be plenty for hampered, overworked network administrators. UnityOne automatically learns and automates the firewall configuration and IDS tuning process, removing a source of constant headaches. Couple that coup for all three functions, with an easy-to-use interface, and the UnityOne can not be beat when it comes to securing the enterprise.

Savings

By integrating and interlocking assessment, detection, and firewall functions into a single appliance, enterprises automatically benefit from lower first-in and total-cost-of-ownership when choosing UnityOne. The cost of security is immediately reduced by purchasing one system, instead of the traditional three needed for patchwork security coverage. Compared to today's patchwork systems, UnityOne's first-in costs are 50% less and the total cost of ownership is reduced by as much as 75%.

TippingPoint's UnityOne™
Value Propositions

What we offer	How it benefits the enterprise
Multigigabit hardware	Secures network without degrading network performance

Integration of three security systems into one Unified system	• Interlocking applications provide comprehensive security – attack blocking, not just detection
	
	• Lower first-in and total-cost-of-ownership
	
	• Ease of use
	   - Auto tuning
	   - Single management system

Hardened signature and anomaly algorithms	Highly reliable signatures – greatly diminishes false positives

UnityOne™

Threat Prevention Appliances

TippingPoint Technologies

7501B North Capital of Texas Hwy   Austin, TX 78731

512.681.8000 phone   512.681.8099 fax

www.tippingpoint.com