



## UnityOne™

### Features And Benefits

#### Switch-Like Performance

- Multi-Gigabit Per Second Attack Filtering
  - UnityOne-200  
200 Mbps Aggregate Throughput
  - UnityOne-400  
400 Mbps Aggregate Throughput
  - UnityOne-1200  
1.2 Gbps Aggregate Throughput
  - UnityOne-2400  
2.0 Gbps Aggregate Throughput

#### Provides Advanced Security and Lowers Operating Costs

#### Advanced Attack Filtering - Suppresses Attacks Before Damage Occurs

#### Peer-to-Peer Piracy Prevention Capability Protects from Peer-To-Peer Theft

#### SMARTMatch™ Attack Filters

- Precision Prevention
- Comprehensive Attack Coverage (850+ Attack Filters)

#### Auto-Configuration Capability

- Discovers Networks and Hosts
- Facilitates and Automates Deployment Process

#### Non-Stop Networking and Non-Stop Security

#### Enterprise Management - Security Management System

- Manage Up To 1,000 Systems
- Advanced Correlation Capabilities
- Policy-Based Administration

### UnityOne™ - Transforms Networks From A Weakness To A Weapon

UnityOne Intrusion Prevention Appliances are active network defense systems providing true intrusion prevention. Based on breakthrough high-speed security processors, UnityOne appliances scour networks at gigabit speeds. When a threat is detected, UnityOne instantly filters and blocks the malicious traffic before damage occurs. UnityOne becomes part of the network infrastructure and continually cleanses Internet and Intranet traffic. The appliance product line includes the UnityOne-200 for remote branch offices; UnityOne-400 for small-to-medium businesses; UnityOne-1200 for enterprises and the UnityOne-2400 for large enterprise applications.

### UnityOne Completes and Complements the Firewall

Firewalls only inspect the first four layers of a packet. UnityOne inspects and analyzes all seven layers - creating a barrier of defense that is impenetrable. UnityOne provides active security - taking network protection to a new level by recognizing and filtering **worms, viruses, trojan horses, blended threats and denial-of-service attacks** in real-time at multi-gigabit speeds.

### The Power of TippingPoint's Breakthrough Hardware

Software-based solutions running on Pentium, SPARC or MIPS processors

can no longer keep pace with the exploding security challenge. That is why UnityOne has the TippingPoint Threat Suppression Engine (TSE) at its core. The TSE, a deft blend of ASICs and network processors, detects known threats and anomalies in your network traffic at ultra-high speeds and filters malicious attacks before they become a problem.

### UnityOne - Fast, Precise and Highly Reliable

UnityOne Intrusion Prevention Appliances are extremely low-latency network infrastructure ensuring switch-like network performance, even while under attack. UnityOne also has built-in intrinsic high-availability features, guaranteeing that the network keeps running in the event of system failure. As well, UnityOne attack filters are built with such precision that they never confuse good traffic with bad traffic.

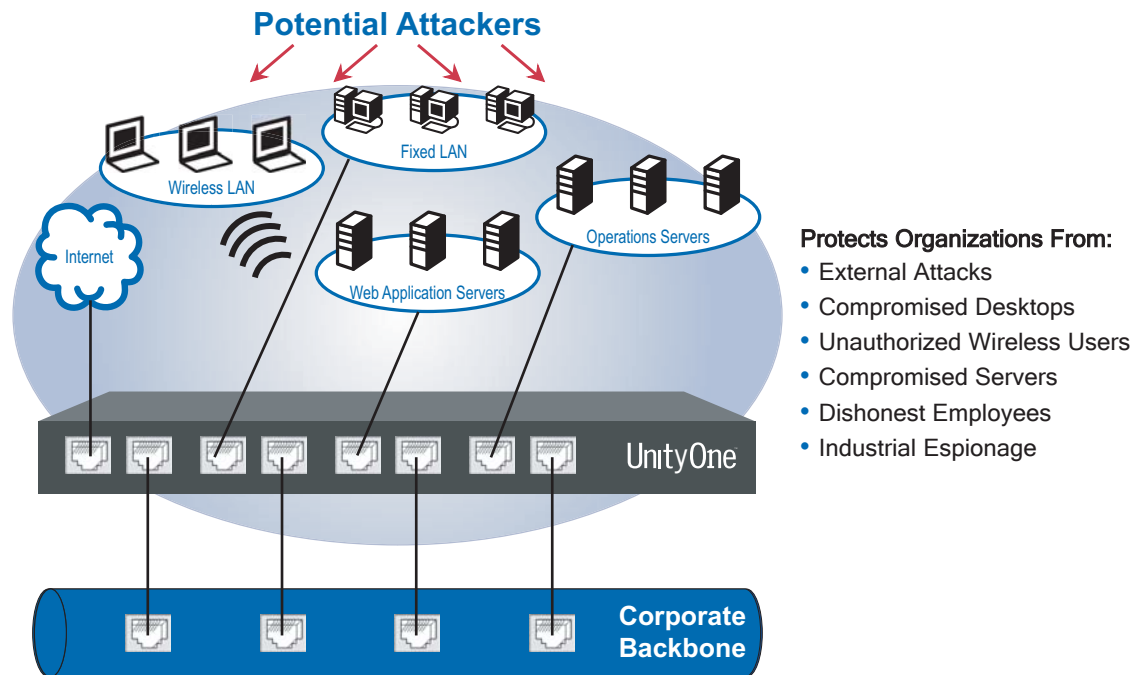
### Protection and Profitability

Web services and applications, operating systems (desktop and server), financial and operations servers, Web applications and core network infrastructure like switches and routers are all protected once UnityOne is installed. The cost of security administration is instantly reduced and corporate productivity is preserved by increased network and application availability.

## UnityOne - Omni-Directional Intrusion Prevention

UnityOne appliances are optimized to provide high resiliency, high availability security for remote branch offices, small-to-medium and large enterprises and collocation facilities. Each UnityOne (UnityOne-200: Two 10/100 Segments; UnityOne-400: Four 10/100 Segments;

UnityOne-1200, 2400: Four 10/100/1000 Segments) can protect network segments from both external and internal attacks. Multiple UnityOne appliances can be deployed to extend this unsurpassed protection to hundreds of enterprise zones.



### Lower Total-Cost-of-Security

Reactive mode security is extremely expensive and complex. Cost of administration, damage clean-up, correlation, host patch management (50 new vulnerabilities emerge every week) and anti-virus updates make today's security infrastructure unmanageable

and ineffective. UnityOne transforms your network into a massive and powerful defensive barricade protecting operating systems, applications, Web services and core network infrastructure from hostile attack:

#### Operating System Protection (Desktop and Server)

- Windows
- Windows XP
- Linux
- Unix

#### Application Protection

- Outlook
- Exchange
- Instant Messaging
- Oracle
- IBM DB2
- MS SQL

#### Web Services Protection

- WebSphere
- .NET
- Oracle 9i

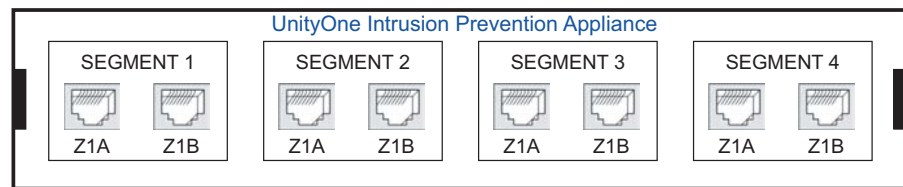
#### Web DMZ Protection

- HTTP
- FTP
- DNS
- SMTP
- Telnet
- XML
- SMB
- POP
- IMAP

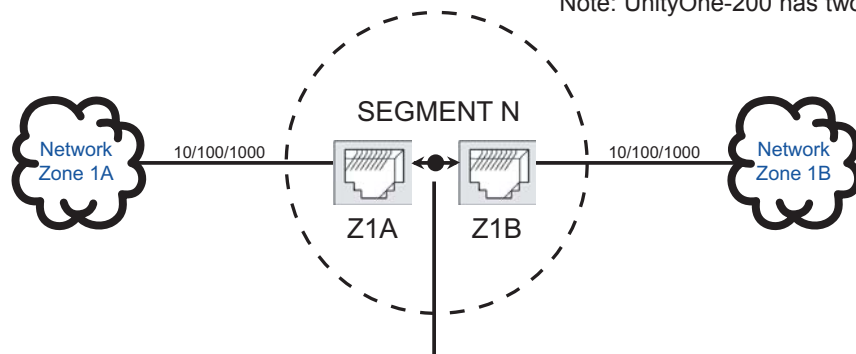
## Up To Four Intrusion Prevention Systems In One

The UnityOne-400, 1200 and 2400 appliances come with all four segments active. No additional licensing is

required. The UnityOne-200 has two active segments (four ports).



Note: UnityOne-200 has two segments



### Precision Prevention Shield (PPS)

- Protects One Physical Segment (Two Ports)
- 850+ SMARTMatch™ Attack Filters
- All Four Segments Are Enabled

### Precision Prevention Shield

Precision Prevention Shields actively, automatically and reliably filters attacks before they can be propagated. This advancement in network security can save millions of dollars in lost productivity, system downtime and theft. And, UnityOne is transparent - undetectable to the outside world. Granular policies can be set bi-directionally or uni-directionally.

### SMARTMatch™ Precision Attack Recognition

TippingPoint's System-Matching Attack Recognition Technology (SMART) is the most advanced Attack Recognition

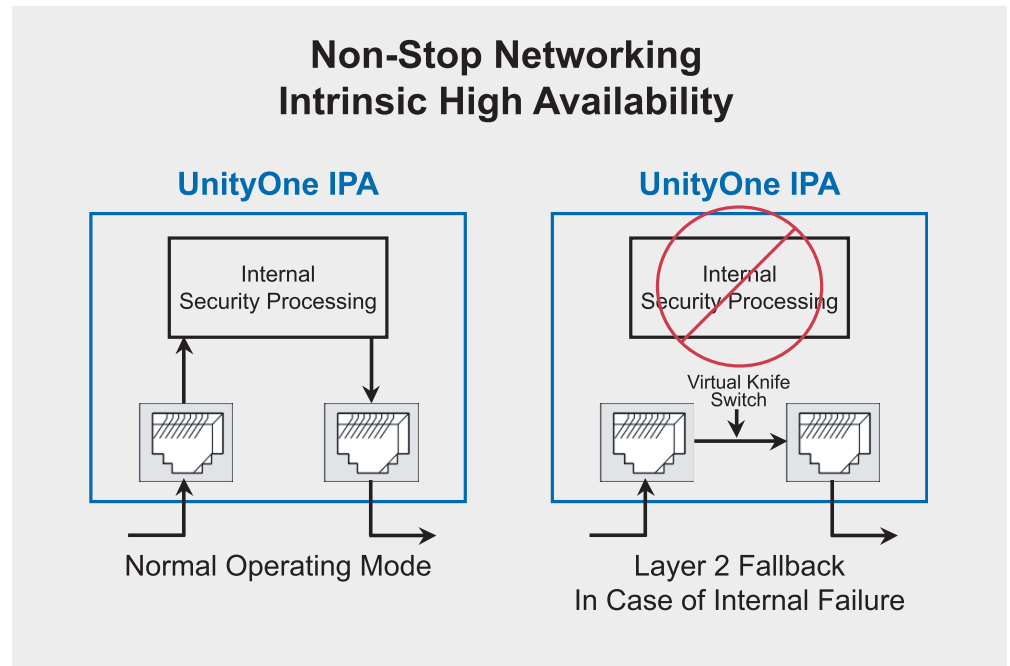
capability in the world. SMARTMatch identifies with absolute precision over 850 attacks including:

- Buffer Overflows
- Reconnaissance Probing
- Protocol Anomalies
- Covert Channel Communications
- Specific Exploits and Variations
- DoS and DDoS Attacks
- Virus and Worm Propagation Activity
- Fragmentation-Based Attacks
- Port 80 Attacks
- Bandwidth Hijacking
- Copyright Infringement (Peer-to-Peer Misuse)

## Non-Stop Networking

UnityOne appliances are designed to guarantee that your network traffic always flows at wire speeds in the event of internal appliance failure. In the case of any internal hardware or software

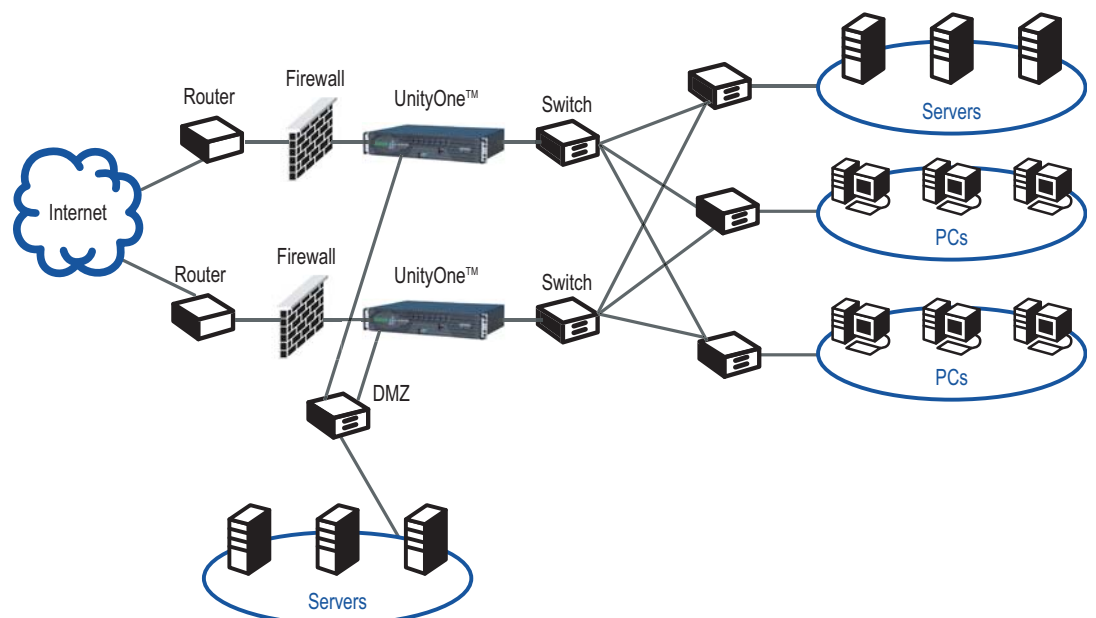
failure, UnityOne can automatically or manually fall back to be a simple Layer 2 switch, ensuring high-network availability.



## Non-Stop Security

UnityOne supports an always-on, always covered configuration. Two UnityOne appliances can be interlinked to provide consistent, redundant network

security. Active-Active and Active-Passive configurations are supported. VRRP, IGP and HSRP can all be used to create redundant security.



## UnityOne Peer-to-Peer Piracy Protection (PPPP)

### Protecting Your Bandwidth and Protecting You From Copyright Infringement

Bandwidth hijacking is the number one killer of corporate productivity. Peer-to-peer applications like Kazaa, Gnutella, Limewire, Bearshare, iMesh and WinMX can absorb 100% of your LAN and WAN bandwidth. Unnecessary Web traffic in general (including unauthorized Web servers) can consume so much bandwidth that business operations become inefficient. And, your

organization runs the risk of being held liable for any pirating your employees commit. Peer-to-Peer Piracy Prevention (PPPP) is a standard UnityOne feature that allows traffic to be limited or blocked to limit copyright exposure and ensure maximum corporate productivity. Policies and quotas can be set by client, server, IP address or application.

## Global Enterprise Systems Management

The UnityOne Security Management System (SMS) is an enterprise-class management platform that provides administration, configuration, monitoring and reporting for up to 1,000 UnityOne Intrusion Prevention Appliances. It is a zero-install rack mountable appliance that features a state-of-the-art Java client interface.

The SMS features a policy-based operational model for scalable and uniform enterprise management. It

enables “big picture” analysis with trending reports, correlation and real-time graphs - including reports on Traffic Statistics, Filtered Attacks, Network Hosts and Services, and UnityOne Inventory and Health.

The SMS dashboard provides at-a-glance monitors, with launch capabilities into the targeted management applications that provide global command and control of UnityOne.



## Local Security Management

Every UnityOne Intrusion Prevention Appliance is shipped with the embedded Local Security Manager (LSM) software. The LSM is a management application

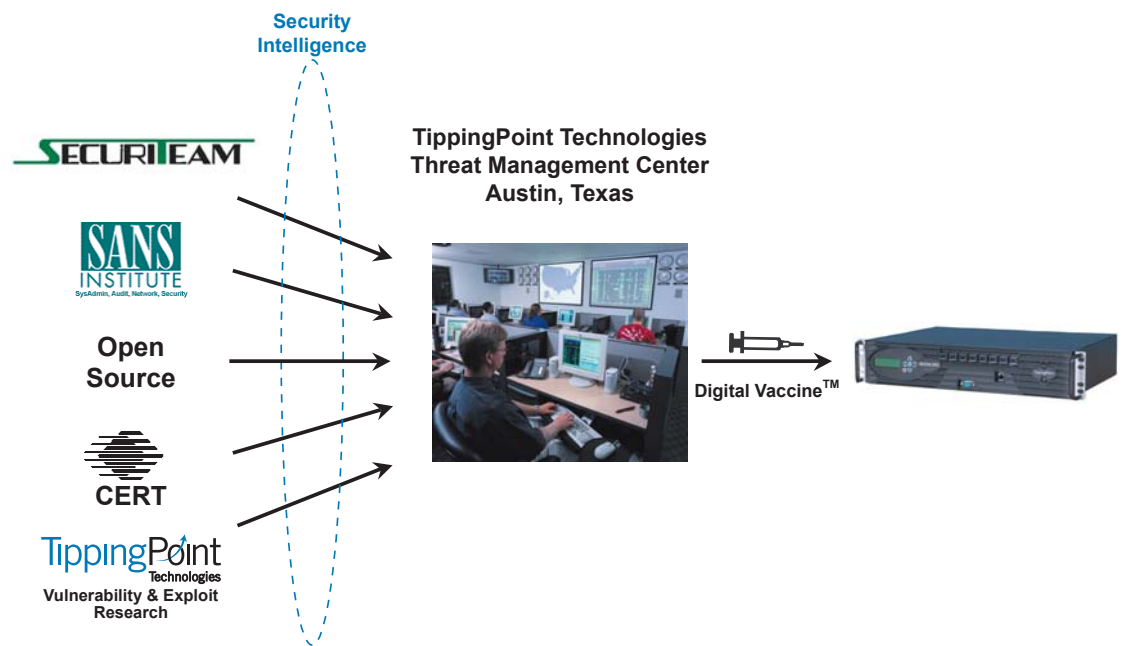
that provides administration, configuration and reporting capabilities in an easy-to-use, secure Web interface.

## Digital Vaccine™ Real-Time Network Inoculation

TippingPoint provides a real-time Attack Filter update service that delivers rapid inoculation of UnityOne appliances against emerging threats. The Digital Vaccine™ service delivers highly reliable attack filters to subscriber systems automatically. Subscribers have the option to manually or automatically instantiate new attack filters.

Digital Vaccines are developed by and delivered from the TippingPoint Threat

Management Center. The Threat Management Center monitors alert services around the world to ensure rapid inoculation against first-strike attacks. TippingPoint research performs real-time in-depth investigation of first-strike vulnerabilities, exploits and malware and then rapidly creates antidotes that are delivered in the form of a Digital Vaccine to subscribers' UnityOne appliances.



*"UnityOne was extremely effective and incredibly easy to use. The Sapphire Digital Vaccine was deployed to UnityOne, and our staff watched as thousands of SQL Slammer and other attacks were blocked per hour. Because TippingPoint researches vulnerabilities and develops attack filters for us, we no longer have to worry about international exploits. TippingPoint's intrusion prevention systems will truly revolutionize the security industry."*

Ronnie Wagers  
Network Systems and Security Officer  
University of Dayton

# Technical Specifications

## Performance

- Aggregate Throughput
  - UnityOne-200 - 200 megabits per second
  - UnityOne-400 - 400 megabits per second
  - UnityOne-1200 - 1.2 gigabits per second
  - UnityOne-2400 - 2.0 gigabits per second
- Detect Rate
  - 100% Detect Matching Against SMARTMatch™ Attack Filters
- Block Rate
  - 100% Attack Denial Against SMARTMatch™ Attack Filters
- Max. Latency
  - 215 microseconds<sup>1</sup>
- Total Sessions
  - 1,000,000
- New Sessions Per Second
  - 25,000

## Enterprise Scalability

- UnityOne-200:
  - Four 10/100 Ethernet Ports
  - Copper Only
  - Total Segments - 2
- UnityOne-400:
  - Eight 10/100 Ethernet Ports
  - Copper Only
  - Total Segments - 4
- UnityOne-1200, UnityOne-2400:
  - Eight 10/100/1000 Ethernet Ports
  - Fiber and Copper
  - Total Segments - 4

## Non-Stop Networking

- Layer 2 Fallback

## Non-Stop Security

- Active-Active Redundancy
- Active-Passive Redundancy

## Network Discovery

- Comprehensive Host and Service Detection

## Processor

- Threat Suppression Engine 2.0
  - UnityOne-200 - 200 megabits per second
  - UnityOne-400 - 400 megabits per second
  - UnityOne-1200 - 1.2 gigabits per second
  - UnityOne-2400 - 2.0 gigabits per second

## Security Certification Targets

- Common Criteria EAL2

## SMARTMatch™ Attack Filters

- Number of Attack Filters - 850+
- Attack Categories
  - Worm
  - DoS
  - Virus
  - Suspicious
  - Trojan
  - Reconnaissance
  - Access

## Protocols/Applications

- IP
- DNS
- VLAN
- TCP
- RCP
- MPLS
- ICMP
- HTTP
- FTP
- ARP
- Telnet
- UDP
- IMAP

## Actions

- Block
- Copy
- Permit
- Alert
- Log

## Messaging

- E-Mail
- Script
- Pager
- Syslog
- SNMP

## LED Indicators

- Status
- Network Activity
- Link State
- System Power

## Management Interfaces

- 1 10/100 Ethernet
- 1 Serial Port

## Peer to Peer Piracy Prevention

- Bandwidth Protection
- Policy and Quota Management:
  - Client
  - Server
- IP Address
- Application

## Attack Filter Delivery Service

Digital Vaccine™ Real-time Inoculation Service

## Web-Based Attack Filter Updates

- Updated Quarterly
- Secure Browser Access

## System Management (3 Options)

- Command Line Interface (CLI)
- Local Security Manager (LSM)
  - On-Box Web-based Management
- Enterprise Security Management System (SMS)
  - Manages Up To 1,000 UnityOne Appliances
  - Delivered pre-installed on 1U Appliance
  - O/S - Hardened Linux
  - Client Requirements - SUN JRE 1.3, Windows 2000, NT and 9X

## Power Dissipation

Units	Amps	V
AC	6/3	110/220

Efficiency	Input Range (V)	Freq. Range (Hz)
68%	100 to 240	50-60

## Dimensions

Units	Height	Width	Depth	Weight
in/lb	3.5	17.25	12	20
cm/kg	8.9	43.8	30.5	7.5

## Safety Certifications

- UL 1950: Standard for Safety of Information Technology Equipment
- CSA 22.2-60950
- EN60825: European Safety of Laser Products
- EN60950
- IEC60950

## Immunity

- EN-61000-3-2: Harmonic Emissions
- EN-61000-3-3: Voltage Fluctuations and Flicker
- EN-61000-4-2: ESD Immunity
- EN-61000-4-3: Radiated Immunity
- EN-61000-4-4 EFT: Burst Transients
- EN-61000-4-5: Surge Protection
- EN-61000-4-6: Injected RF
- EN-61000-4-11: Dips and Sags

## Emissions

- FCC Class A: Regulations for Radio Frequency Devices for Electromagnetic Compliance
- ICES-003, Class A (Canada)
- EN 55022 Class A (Europe)

## Warranty

The standard warranty is for a 12-month period. Optional hardware maintenance services are also available. Phone support and training courses are available from TippingPoint.

<sup>1</sup> Full line rate, traffic combination of TCP and UDP.

## Ordering Information

### Product

### Part Number

#### UnityOne™ Intrusion Prevention Appliances

- UnityOne-200 IPA200-C
- UnityOne-400 IPA400-C
- UnityOne-1200 IPA1200-C, F, or CF
- UnityOne-2400 IPA2400-C, F, or CF

UnityOne-200 includes four 10/100 Ethernet ports; UnityOne-400 includes eight 10/100 Ethernet ports; UnityOne-1200 and UnityOne-2400 include eight 10/100/1000 Ethernet ports (Dash number specifies port configuration - C is all copper, F is all Fiber, CF is four copper ports, four Fiber ports). All segments are enabled as prevention sensors and include piracy prevention.

#### Enterprise Security Management System

- Security Management Appliance (Manages up to 5 UnityOne appliances) SMA-5
- Security Management Expansion Licenses - 5 additional appliances SMS-5

#### Annual Maintenance Contract

MAINT-01

- Digital Vaccine™ Service
- 7x24 Support



7501B North Capital of Texas Hwy.  
Austin, TX 78731  
512-681-8000  
88-UNITYONE  
[www.tippingpoint.com](http://www.tippingpoint.com)

Copyright © 2003 TippingPoint Technologies, Inc.

TippingPoint Technologies, the TippingPoint logo, UnityOne, the UnityOne logo, Digital Vaccine and SMARTMatch are registered trademarks of TippingPoint Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.