UnityOne Network-Defense Systems

UnityOne™

Features And Benefits

- **Ultra High-Speed Intrusion Prevention**
  - UnityOne-600 – 600 Megabits per second
  - UnityOne-2000 – 2 Gigabits per second (Upgradable to 10 Gigabits per second)
- **Up to 40 Security Zones Per System**
  - Thwarts both internal and external attacks
- **Advanced Attack Blocking**
  - Suppresses Attacks Before Damage Occurs
- **SMARTMatch™ Attack Filters**
  - Comprehensive Attack Coverage (2000+ Attack Types)
  - 90% Reduction In False Positives
- **High Availability Mode**
  - Host Management Mirroring
  - Dedicated High Availability Channel
  - Heartbeat Monitoring
- **Enterprise Security Management System**
  - Manage Up To 1000 Defense Systems
  - Advanced Correlation Capabilities
  - Policy-Based Administration

TippingPoint Technologies

UnityOne™–600 Small to Medium Enterprise

UnityOne™–2000 Large Enterprise

UnityOne™ – Active and Automatic Intrusion Prevention

UnityOne Network-Defense Systems (NDS) are the most advanced and comprehensive security systems ever developed. Based on breakthrough high-speed security processors, UnityOne scours networks at **2 gigabits per second**. When a threat is detected, UnityOne **instantly blocks** the malicious traffic before damage occurs. Unlike software-based intrusion systems, UnityOne becomes part of the network infrastructure and **continually cleanses** Internet and Intranet traffic. The product line includes the UnityOne-600 for small-to-medium enterprises and the UnityOne-2000 for large enterprises.

UnityOne Advances Network Defense from Tools to Weapons

Legacy Gigabit Intrusion Detection Systems (IDS) supply passive security – they provide notification of attacks after the fact, but do little or nothing to prevent them. UnityOne NDS's provide active security – they take network protection to a new level by detecting and blocking **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 detects known threats and anomalies in your network traffic at ultra-high speeds and blocks malicious attacks before they become a problem.

The TSE is specifically designed for high-speed network security applications – it performs packet and flow reassembly, stateful inspection, packet classification, and unanchored content searching at 2 gigabits per second. The TSE makes the **UnityOne the only true multi-gigabit intrusion blocking system**. It is capable of finding even the most esoteric attacks - across packet boundaries or hidden in fragmented flows - and can **suppress over 2000 attack types**.

Example Threat Suppression Engine Capabilities:

Threat Suppression Engine Performance

Packet Size	Pentium Equivalents*(PE) TSE-6	TSE-20
64 bytes (Fragmented Attacks)	30PE	78PE
384 bytes (Average Enterprise Packet Size	12PE	42PE
1500 bytes (Max IP Packet Size)	6PE	21PE

*Pentium III 1 GHZ, 768 MB RAM when applied to Intrusion Blocking. Performance metrics derived from NSS Group—Europe's foremost independent network and security testing organization.

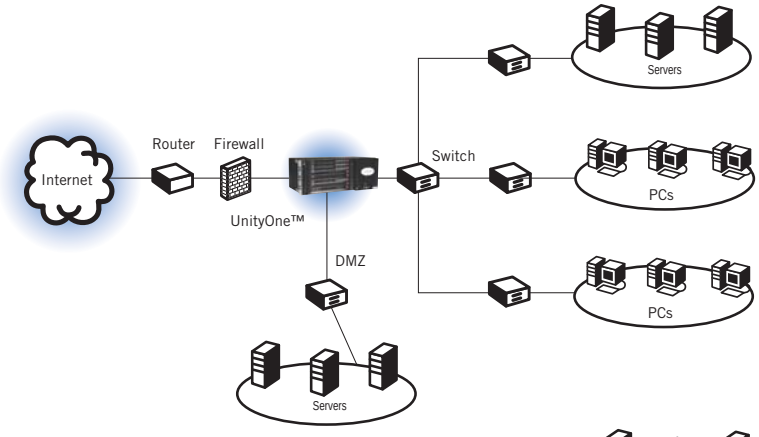
- TCP Session Flow Reassembly
- IP & UDP Fragment Reassembly
- State Tracking for 250,000 Sessions
- Application Layer Protocol Decoding
- Full Regular Expression Matching Across Multiple Packets
- Host Sweep and Port Scan Detection
- Packet Flood and Syn Flood Detection

Enterprise Scalability - Hardware

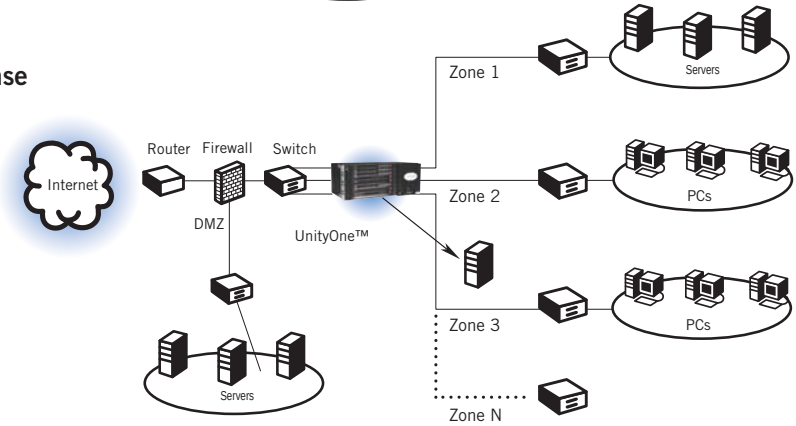
UnityOne NDS's are optimized to provide high resiliency, high availability security for large enterprises and collocation facilities. Each UnityOne NDS can protect up to 40 network zones from both external and internal attacks, and multiple NDS's can be deployed to extend this unsurpassed protection to hundreds of enterprise zones.

The UnityOne NDS ships with one 10-port Multi-Zone Defense Module and has expansion slots to accommodate up to three additional 10-port Multi-Zone Defense Modules. Multi-Zone Defense Modules support combinations of 10/100/1000 copper and fiber Ethernet ports (see Ordering Information).

Perimeter Defense



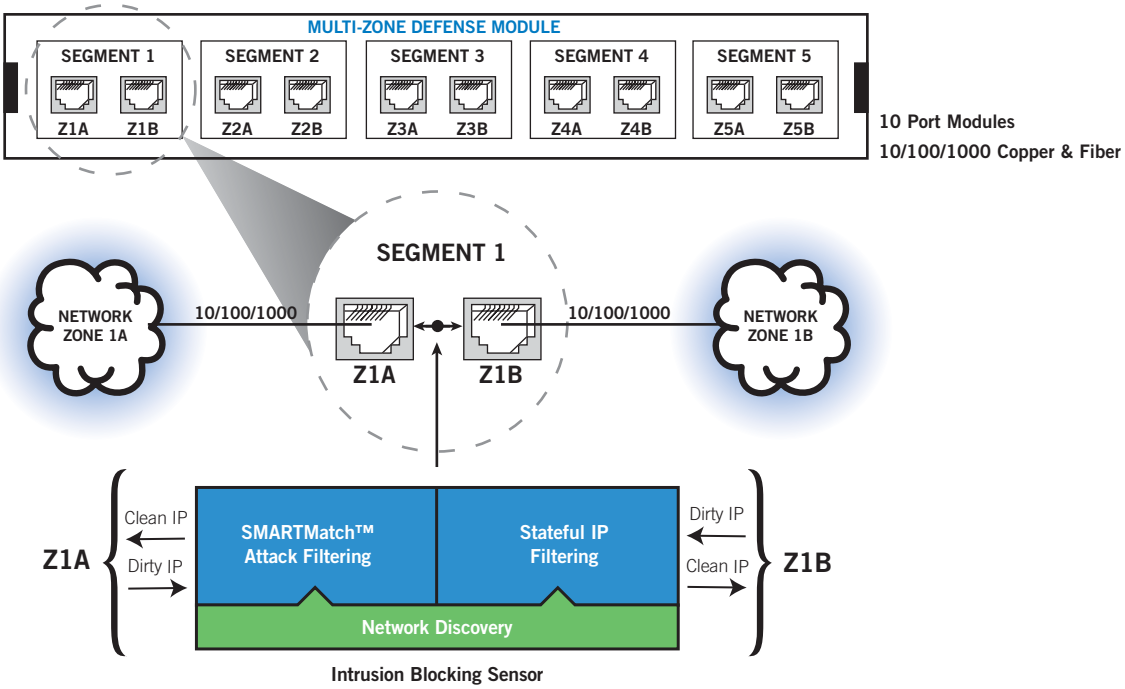
Multi-Zone Defense



Intrusion Blocking Sensor - Software

UnityOne Intrusion Blocking Sensor (IBS) software is a highly intelligent third generation sensor technology that provides unsurpassed enterprise network protection. Each IBS protects two zones. Up to 20 IBS's can be licensed and installed on a single UnityOne system (Base System ships with one IBS. For additional IBS licenses, see Ordering Information).

The IBS software is comprised of three interlocking capabilities – SMARTMatch™ Attack Filtering, Stateful IP Filtering and Network Discovery. In combination, these capabilities offer powerful and resilient network defense capabilities.



SMARTMatch™ Attack Filtering

TippingPoint System-Matching Attack Recognition Technology (SMART) is the most advanced Attack Filtering capability in the world.

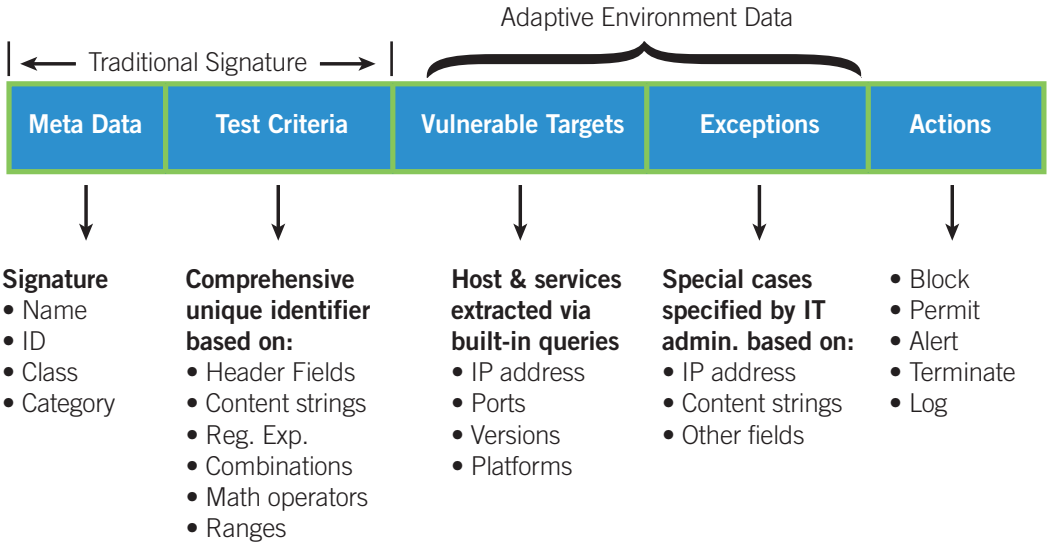
SMARTMatch Attack Filters detect and block over 2000 attacks including:

- Buffer Overflows
- Protocol Anomalies
- Specific Exploits and Variations
- DoS and DDoS Attacks
- Reconnaissance Probing
- Covert Channel Communications
- Virus and Worm Propagation Activity
- Fragmentation-Based Attacks
- Port 80 Protection

SMARTMatch™ Eliminates Human Denial of Service

SMARTMatch Attack Filters dramatically improve security reliability and efficacy over legacy IDS products. Using both signature and protocol anomaly techniques, SMARTMatch Attack Filters reliably detect and block attacks with 100% reliability.

The UnityOne embedded Network Discovery tool **automatically tunes** the SMARTMatch Attack Filters to ensure reliable detection and to filter out false alerts resulting from benign attacks - **reducing false alert rates by up to 90% over those of legacy systems.**



Network Discovery

In addition to auto-tuning, the Network Discovery capability provides a complete enterprise-wide report of the Hosts and Services active on your network to enable sensible network and service configuration choices.

Stateful IP Filtering

The embedded Stateful IP Filtering application interlocks with SMARTMatch Attack Filters to provide service level macro permissions and policies.

Operational Modes

UnityOne is installed in-line or attached to a switch span port and can be set to one of two default postures:

IDS Mode (Passive Mode) – IDS Mode actively searches network traffic for all known attacks and alerts the administrator when an attack is detected. This mode is similar to a traditional IDS but adds value by dramatically reducing false negatives (missed attacks) and false positives (benign attacks).

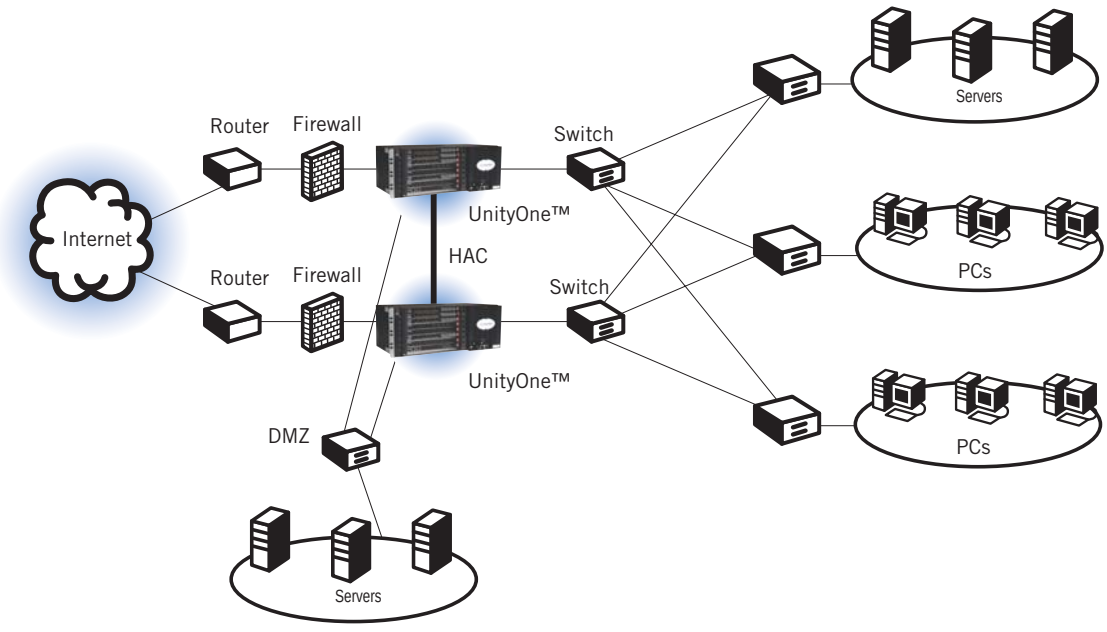
Protection Mode (Active Mode) – In Protection Mode (must be in-line), UnityOne actively, automatically and reliably blocks detected attacks before they can be propagated. This advancement in network security can save millions of dollars in lost productivity, system downtime and theft. In Protection Mode, UnityOne NDS's are transparent – meaning they are undetectable to the outside world.

High Availability Configuration

UnityOne supports an always-on, always-covered configuration. Through Host Management Mirroring technology, two UnityOne NDS's can be interlinked to provide consistent, redundant network security.

A dedicated High Availability Channel (HAC) enables linked UnityOne NDS's to synchronize system configuration and to engage in heartbeat monitoring. Configuration operations performed on the primary UnityOne NDS will be transparently propagated to the secondary UnityOne NDS.

Hot failover capabilities make sure that a line failure on either side of an NDS will be reported and that switching devices on both sides of the failure will be aware of the failure.



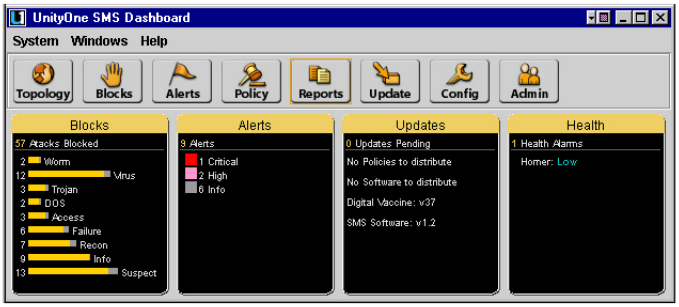
Local Security Management

Every UnityOne Network-Defense System is shipped with the embedded Local Security Manager (LSM) software. The LSM is an NDS-based management application that provides administration, configuration and reporting capabilities in an easy-to-use, secure Web interface.

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 1000 UnityOne Network-Defense Systems. It is a zero-install rack mountable appliance that features a state-of-the-art Java client interface.

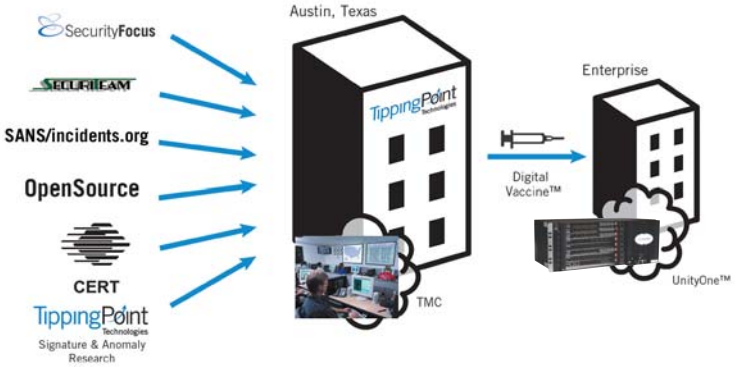
The SMS features a policy-based operational model for scalable and uniform enterprise management. It enables "big picture" analysis with trending reports, correlation and real-time graphs - including reports on Traffic Statistics, Blocked Attacks, Alerts, Network Hosts and Services, and UnityOne Inventory 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 the UnityOne Network-Defense Systems.

Digital Vaccine™ Real-Time Network Inoculation

TippingPoint provides a real-time Attack Filter update service that delivers rapid inoculation of UnityOne Network-Defense Systems against emerging threats. The Digital Vaccine™ service delivers highly reliable SMARTMatch™ 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 over 10,000 sensors 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 systems.

Technical Specifications

Performance
- Aggregate Throughput
  - UnityOne-2000 – 2 gigabits per second (Upgradeable to 10 Gigabits per second 2003)
  - UnityOne-600 – 600 megabits per second
- Detect Rate
  - 100% detect matching against SMARTMatch™ Attack Filters
- Block Rate
  - 100% attack denial against SMARTMatch™ Attack Filters
- Induced latency
  - 3ms. max

Enterprise Scalability
- Expansion Modules – Multi-Zone Defense Module (10 Zones)
  10/100/1000 Ethernet Ports
  Fiber and Copper
- Expansion Slots Per Chassis – 4
- Total Security Zones Per Chassis – 40

High Availability
- Redundant System Synchronization
- Intelligent Heart Beat High Availability Channel
- Hot Fail-Over (1 Second)

Network Discovery
- Comprehensive Host and Service Detection

Processor
- Threat Suppression Engine 1.0
  - UnityOne-2000 – 2 gigabits per second
  - UnityOne-600 – 600 megabits per second

Security Certification Targets
- Common Criteria EAL2
- ICSA

SMARTMatch™ Attack Filters
- Protocol Anomaly Filters
- Signature Filters
- Attack Categories
  - Worm
  - Virus
  - Trojan
  - Access
  - DoS
  - Suspicious
  - Reconnaissance

Protocols/Applications
- IP
- TCP
- ICMP
- ARP
- UDP
- DNS
- VLAN
- MPLS
- HTTP
- Telnet
- IMAP
- RPC
- FTP

Actions
- Block
- Permit
- Deny
- Terminate
- Copy
- Alert
- Log
- Redirect

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

LED Indicators
- System Power
- Link State
- Link Configuration
- Network Activity
- Threat Detection
- System Health

Management Interfaces
- 2 10/100 Ethernet
- 1 Serial Port

Attack Filter Delivery Service
Digital Vaccine™ Realtime Inoculation Service

Web-based Attack Filter Resource
- Updated Weekly
- 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 1000 NDS's
  - 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)
60%	90 to 240	47-63

Dimensions

Units	Height	Width	Depth	Weight
in/lb	7	17	12	45
cm/kg	18	43	31	20

Safety Certifications
- UL 1950: Standard for Safety of Information Technology Equipment
- CSA 22.2-950 (Canada): Canadian equivalent of U.S. UL1950
- EN60825: European Safety of Laser Products
- EN60950 (Europe/UK): European equivalent of U.S. UL1950
- EMC Certifications

Immunity
- EN-61000-3-2: Standard for controlling harmonic emissions and voltage fluctuations
- 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): Equivalent of FCC Class A
- EN 55022 Class A (Europe/UK): Equivalent of FCC Class A VCCI
- Class 1(Japan): Equivalent of FCC Class A

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

Ordering Information

Product	Part Number
TippingPoint Base Systems	
• UnityOne-2000 Network-Defense System	NDS2000-C20, F20, or CF20
• UnityOne-600 Network-Defense System	NDS600- C6, F6, or CF6

Base Systems include Chassis with TSE and Management Processor, 10-Port Multi-Zone Defense Module (Dash number specifies port configuration – **C** is all copper, **F** is all Fiber, **CF** is 6 copper ports, 4 Fiber ports), 2 power supplies, and One Intrusion Blocking Sensor (Attack Detection and Blocking, Stateful IP Filtering, Network Discovery)

Multi-Zone Defense Modules (Hardware I/O Expansion)

For UnityOne-2000:

• All Copper 10/100/1000 – Ten RJ-45 Jacks	MZD-C20
• All Fiber 10/100/1000 – Ten SFP Slots	MZD-F20
• Mixed Fiber/Copper – Six RJ-45, 4 SFP Slots	MZD-CF20

Note: must order SFP interfaces (either multi-mode Part # SFPMM01, or single-mode Part # SFPSM-01) to plug into SFP slots.

For UnityOne-600 (10/100 only):

• All Copper 10/100 – Ten RJ-45 Jacks	MZD-C6
• All Fiber 100/1000 - Ten SFP Slots	MZD-F6
• Mixed Copper/Fiber – Six RJ-45, 4 SFP Slots	MZD-CF6

Note: must order SFP interfaces (either multi-mode Part # SFPMM01, or single-mode Part # SFPSM-01) to plug into SFP slots.

Product	Part Number
Additional Intrusion Blocking Sensors	
(Each Sensor includes Intrusion Detection, Intrusion Blocking, Stateful Filtering and Network Discovery)	
• 100 megabit/sec sensor	IBS100-01
• 1 Gigabit/sec sensor	IBS1000-01
• Upgrade from 100 to 1000	IBSU-01
Enterprise Security Management System	
• Security Management Appliance (Manages up to 5 UnityOne NDS's)	SMA-5
• Security Management Expansion Licenses	
- 5 additional NDS's	SMS-5
- 25 additional NDS's	SMS-25
- 100 additional NDS's	SMS-100
Real-Time Inoculation Service	
• Digital Vaccine™ Service	DV-01
Annual Maintenance Contract	MAINT-01
Spares	
• Additional Power Supply (N + 1 redundancy)	PS-01

TippingPoint Technologies
7501B North Capital of Texas Hwy.
Austin, TX 78731
512-681-8000
www.tippingpoint.com