

UnityOne | FAQs

What are the defining capabilities of Intrusion Prevention for UnityOne?

Application Protection

- Protection for Layer 2-7 Host-Based (client and server) Vulnerabilities
- Provides Zero-Day Attack Protection
- Eliminates Emergency Patching Triage
- Prevents Application and O/S Damage/Downtime

Infrastructure Protection

- Protection for Infrastructure Element (router, firewall, switch) Vulnerabilities
 - Protects Cisco IOS Vulnerabilities
 - Protects Firewall Connection Tables
- Ensures Network Availability
- Mitigates and Throttles DoS, DDoS Impact

Performance Protection

- Protects Network Resources from Being Overwhelmed and Impacting Mission-Critical Traffic
- Network Runs Faster Even When Not Under Attack
- Non-Mission Critical Applications Can Be Rate Limited
 - Eliminates Bandwidth Hijacking
 - Rogue Applications Are Controlled
 - Misuse and Abuse Eliminated
 - Peer-to-Peer Traffic Controlled

What are the new features in 1.4.2?

New capabilities in the IPS, SMS, and Digital Vaccine include:

IPS

- E-mail Gateway Protection (TCP Resets)
 - Bidirectional or Unidirectional TCP reset action set for any filter
 - Prevents mail servers from retrying mail transfers when blocked because of viruses
- Traffic Normalization *permit+notify* or *disabled*
 - Warning message to users when set as it could let through hidden attacks
 - Allows in-line deployment as a “wire,” permitting all traffic
- Hard Drive protection
 - IPS stays up even with HD failure or unplugging Hard Drive
 - RAM disk used for Block, Alert, P2P Logs and HTML+Images
 - HD functionality transitioning to RAM disk to reduce HD dependency
- FPGA (Field Programmable Gate Array) automatic upgrade with Software
 - Ability to roll forward or roll back
 - Enables a single reboot for upgrades instead of multi-reboot
- Configurable DDoS Syn Trap
 - Defaults to off. Thresholds set to 2,000 Syns, 2,000 Established (Up from 1,000 and 500)
 - Provides increased tuning capabilities for DDoS attacks
- Allow rule in Traffic Management filters
 - Will still be inspected for attacks
 - Enables an administrator to specifically allow IP-filter traffic in addition to blocking

SMS

- Thresholds/Rate Limiting (reports, events, profiles)
 - Provides additional SMS functionality previously available only on the IPS
- Granular administrator security controls
 - Per device, per profile, per segment group
 - Affects event visibility (dashboard, events, reports)
- Automatic Profile History
 - Versions keep complete audit trail
 - Instant rollback to any saved or previously distributed version
- E-mail from SMS
 - When IPS failure or critical alert
 - When automatic DV download or distribution

SMS (continued)

- SMS hot full backup, full restore
 - Easy-to-use Backup Wizard
 - Schedulable backups
- SMS Events and Reports
 - Allow for query cancellation
 - Port ranges, lists in events
 - New "Reports" Web page on SMS Web server with improved organization of HTML/CSV report results
- ARIN, ERIN, and APNIC whois lookups
 - Allows administrators to easily look up domain names associated with IP addresses from databases around the world
- "Save and Distribute" button for profiles
 - Ease-of-use feature for administrators by allowing automatic distribution when saving
- Progress bar when waiting or processing

Digital Vaccine

- DV version protection
 - i.e., prevent 1.4 DV from loading on a 1.3 device

What are the specifications for the UnityOne-50 platform?

The UnityOne-50 is TippingPoint's new hardware platform supporting remote office/branch office locations. The UnityOne-50 maintains the complete feature set of all other UnityOne IPS devices, while supporting a full 50 Mbps of network traffic.

Performance and pricing of the UnityOne-50 is superior to all similar competing products. Specifications include:

UnityOne-50 Performance

- 50 Mbps
- 5,000 Connections Per Second
- 5,000 Total Sessions
- <1 millisecond latency

UnityOne-50 Hardware Specifications

- 1U device (1.75" H)
- 17.25" W x 12" D
- Pentium 4 Mobile processor (no custom-ASICs)
- One segment protection (Two Ethernet ports)
- Copper interfaces only, 10/100/1000
- Other Ports
 - Management (10/100/1000 Copper Ethernet)
 - USB (512 MB, used for all data: TippingPoint OS, logging, Digital Vaccine, etc.)
 - Console (Serial DB9)
- No hard drive
- No redundant power

When are version 1.4.2 and the UnityOne-50 available?

1.4.2 and the UnityOne-50 are available now.

Does pricing for 1.4.2 remain the same?

All new features in 1.4.2 are available to customers with no price increase. All 1.4 customers with a valid maintenance contract can upgrade for free.

Headquarters:

7501B North Capital of Texas Hwy.
Austin, TX 78731
88-UNITYONE
www.tippingpoint.com

International Headquarters:

Joop Geesinkweg 901 - 999
1096 AZ Amsterdam
The Netherlands
+31 (0) 20 561 6222