

i500™ /i500v™ Appliances

CLOUD-INTELLIGENT APPLIANCES PROVIDE LOCALIZED CONTROL FOR TRITON® AP-WEB CLOUD DEPLOYMENTS

TRITON AP-WEB Cloud deployments use cloud infrastructure for real-time analytics and threat protection. However, sending all web traffic to the Cloud may not always be in the best interest to your company. The i500 appliance or the virtual i500v appliance provide an innovative deployment option to analyze some traffic on-site, especially useful for organizations in countries with national firewalls, or to speed up traffic flow in offices experiencing heavy traffic volumes.

WHY CHOOSE THE I500 OR I500V APPLIANCE?

The i500 and i500v appliances complement a TRITON AP-WEB deployment by adding flexibility and control over web traffic flow for analysis, improving traffic speed in bottleneck locations, and adding application and protocol control. Appliances can be deployed in select locations throughout a network to enhance traffic flow, user experience and policy enforcement.

LOCALIZED CONTROL OVER CLOUD TRAFFIC

- Deployed in conjunction with Cloud Web Security Gateway, the i500 and i500v appliance offer greater control over which traffic gets sent to the Cloud for analysis.

INTELLIGENT USE OF THE CLOUD DECREASES LATENCY

- The i500 and i500v appliances use real-time cloud defenses when required to minimize on-site appliance footprint and investment.
- Benign web requests go "direct-to-net" for optimal performance and user experience, while suspicious requests or requests which need real-time content classification (e.g., Facebook) are sent to real-time cloud defenses for optimal protection.

ADDED APPLICATION AND PROTOCOL CONTROL

- Network Agent, included in both appliances, adds full-port monitoring capabilities to Cloud Web Security Gateway deployments.
- Network Agent enables monitoring of traffic outside of proxy analysis, and provides controls for hundreds of applications and protocols.

INDUSTRY-LEADING, REAL-TIME WEB SECURITY

- Forcepoint™ web security solutions are powered by Forcepoint ACE (Advanced Classification Engine), which provides real-time protection by using eight defense assessment areas with over 10,000 analytics.
- ACE analytics are derived from the Forcepoint ThreatSeeker® Intelligence Cloud, which unites more than 900 million endpoints and analyzes over 5 billion web requests per day for global threat awareness.



The i500 appliance provides fast on-box analysis for most traffic and cloud-based analysis for questionable requests. It is also available as the i500v virtual appliance.

▶ **ADVANCED DEFENSES**

- Scalable real-time contextual defenses surpass AV and URL filtering defenses, avoiding the trade-off of performance over security

▶ **REDUCE COSTS & COMPLEXITY**

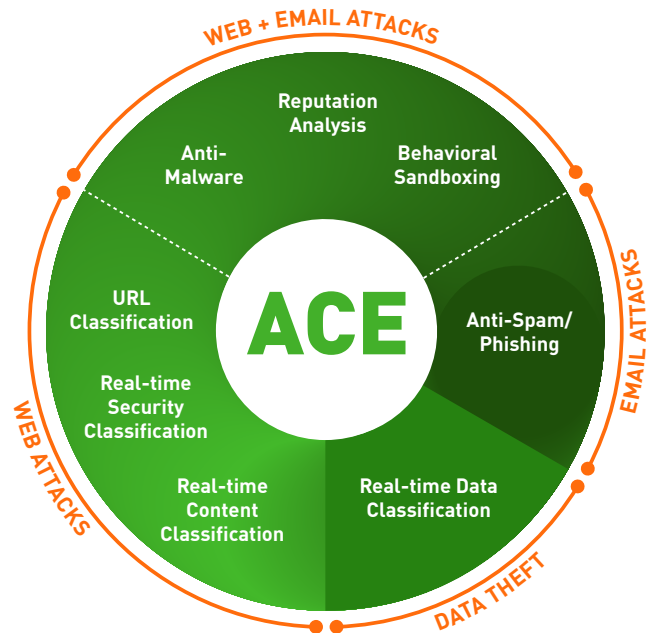
- Select appliance deployment throughout a TRITON AP-WEB deployment
- Deploy appliances only in select locations to decrease latency, localize control, or add application and protocol controls

▶ **RELY ON SUPERIOR CLOUD SERVICE**

- Global Data Centers (ISO 27001 certified)
- Industry-leading 99.999% SLA

▶ **PROVEN FORCEPOINT TRITON ARCHITECTURE AND LEADERSHIP**

- TRITON architecture unifies web, email and data security with appliance, Cloud, software and hybrid deployments
- Worldwide customers with over 16,000 users
- Gartner leaders quadrant positions for Secure Web Gateway (SWG) and Data Loss Prevention (DLP)¹



THE FORCEPOINT DIFFERENCE

ACE (Advanced Classification Engine)

Forcepoint ACE provides real-time, inline contextual defenses for Web, Email, Data and Mobile security by using composite risk scoring and predictive analytics to deliver the most effective security available. It also provides containment by analyzing inbound and outbound traffic with data-aware defenses for industry-leading data theft protection. Classifiers for real-time security, data and content analysis — the result of years of research and development — enable ACE to detect more threats than traditional anti-virus engines every day (the proof is updated daily at <http://securitylabs.forcepoint.com>). ACE is the primary defense behind all Forcepoint TRITON® solutions and is supported by the Forcepoint ThreatSeeker® Intelligence Cloud.

¹ Gartner, "Magic Quadrant for Secure Web Gateway" by Lawrence Orans and Peter Firstbrook, 2014 and "Magic Quadrant for Content-Aware Data Loss Prevention" by Eric Ouellet, 2013



FEATURE	DESCRIPTION
Intelligent Hybrid Design	Intelligent security path analysis sends benign traffic direct-to-net for faster performance and better end-user experience, while utilizing real-time cloud defenses when required. It also provides more control over which traffic gets sent to the Cloud for analysis.
Network Agent	Provides hundreds of protocol and application controls.
Industry-Leading Security	Based on ACE, the same real-time, inline technology that protects many global corporations against unknown and advanced web threats.
Affordable Appliance	Provides the convenience of an appliance with the power of the cloud for a consistent and light on-site footprint .
Simple Installation and Operation	Deploys in less than one hour. Intuitive user interface enables quick policy and security setup as well as flexible reporting.

G3 HARDWARE SPECIFICATIONS*

CAPACITY: Approx. 1300 TPS (h/w) , 1100 TPS (VM)	RAILS: Post Static Rails – DIB Kit included
PROCESSOR: Intel Xeon E3-1231 v3 3.4GHz, 8M Cache, Turbo, 4C/8T, 80W, OEM XL	DIMENSIONS: 1U form factor, 15.5”D x 17.1”W x 1.67”H (39.37cm D x 43.10cm W x 42.6cm H)
CHIPSET: Intel 3420	WEIGHT: max. 17.76 lbs (8.058 kg)
MEMORY: 8 GB (2 x 4 GB)	HARDWARE SUPPORT : Globally available 24/7 by phone.
HDD: 500 GB, SATA, 3.5-in, 7.2K RPM	REGULATORY & COMPLIANCE: FCC / ICES / EN55022 / VCCI/BSMI / C-Tick / SABS / CCC / MIC Class A and UL60950-1 / Verified to comply with RoHS Directive / Energy consumption and noise emissions in accordance with ISO 9296
ON BOARD NIC: Broadcom 5720 Dual Port 1Gb LOM	
ADD ON NIC: Silicom Dual Ports Copper Gigabit Ethernet PCI Express NIC	
POWER SUPPLY: 250 W	

VIRTUAL APPLIANCE HARDWARE REQUIREMENTS

VMware ESXi 5.1	Dedicated 4 cores and 12 GB RAM
VMware ESXi 5.5	Optional Hardware bypass card for fault resilient installs

* For G2 specs, contact your SE

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

Forcepoint™ is a trademark of Forcepoint, LLC. SureView®, ThreatSeeker® and TRITON® are registered trademarks of Forcepoint, LLC. Raytheon is a registered trademark of Raytheon Company.

All other trademarks and registered trademarks are property of their respective owners.

[DS-I500/I500VAPPLIANCES-ENUS]-100012.011416