TRITON® AP-ENDPOINT

STOP ADVANCED THREATS AND SECURE SENSITIVE DATA FOR ROAMING USERS

FORCEPOINT
POWERED BY Raytheon

TRITON® AP-ENDPOINT

STOP ADVANCED THREATS AND SECURE SENSITIVE DATA FOR ROAMING USERS

From a damaged reputation to regulatory fines and penalties, a data breach can have devastating consequences. Securing roaming users against threats and data theft remains a significant challenge for IT security professionals. TRITON® AP-ENDPOINT protects roaming users against Advanced Threats and data theft on and off your network in an easy-to-use solution. Advanced technologies help you quickly identify and protect sensitive data and provide actionable forensic insight into attacks on endpoint devices on or off network. Forcepoint™ TRITON AP-ENDPOINT protects your data, allowing your mobile workforce to do business wherever and whenever they need to.

Forcepoint Empowers Your Endpoint Security

- Secure sensitive data on Mac OS X and Windows endpoint devices off your network.
- Protect off-network endpoints from Advanced Threats.
- Secure inbound threats or outbound data hidden in SSL traffic from all endpoints.
- Control the use of USB storage devices by blocking or encrypting sensitive data transferred to removable media.
- Adopt cloud services like Office 365 and Box Enterprise with safety and confidence.
- Easily demonstrate security controls to auditors and executives for compliance and regulatory requirements.

Key Features

- **Fingerprinting** (including partial fingerprinting) support for endpoint devices on or off the network.
- **Mac OS X and Windows** supported endpoints.
- **Protect sensitive data** sent to USB devices, removable media, printers, or cloud services like Office365 and Box Enterprise.
- **Portable decryption** for USB/media.
- **Drip DLP** considers cumulative data transmission activity over time to discover small amounts of data leakage.
- **Efficiently inspect** HTTPS traffic with the flexibility to decide which type of SSL traffic to inspect.
- **Identify Advanced Threat** web activity across the entire Kill Chain on endpoints operating beyond the reach of network defenses.
- **Identify high-risk** employees through anomalous cumulative activity analysis compared to peer group and past behaviors.

"We run a remote Forcepoint agent that is pre-configured to push Forcepoint out to the laptops. Whenever a laptop goes outside our network it communicates back to the network, which then applies our Internet access policies to the laptop. That way all laptops always operate on the same policies as our internal network."

— Jeff Howells, Network Architect, Wollongong City Council

TRITON AP-ENDPOINT Capabilities

ENABLE OFF-NETWORK ROAMING USERS

Users often require access to sensitive information even while operating remotely. TRITON AP-ENDPOINT delivers the necessary data theft controls on Mac OS X and Windows laptops so you can safely empower those users. Find and secure critical data residing on endpoints, whether the user is on or off your organization's network, including powerful data fingerprinting capabilities often lacking in endpoint DLP solutions.

WEB SECURITY FOLLOWS YOUR ROAMING USERS

The risks from web-based attacks, including Advanced Threats, are even greater for users operating beyond your organization's network. TRITON AP-ENDPOINT extends web security to roaming users, safely allowing them access to web-based resources. More than simple URL filtering, attack activity across the Kill Chain can be identified and blocked, even while working in a proxy-free environment. TRITON AP-ENDPOINT sees into SSL traffic to secure the Web channel for your roaming users even while using Cloud, Email, Social Media or other services that employ secure connections.

EMBRACE INNOVATION WITH SAFETY AND CONFIDENCE

Meeting your customer needs and remaining competitive requires innovation and empowering your workforce with new solutions and technologies. TRITON AP-ENDPOINT helps you safely adopt new cloud services such as Office 365 or Box Enterprise with both web threat defenses and the ability to retain control of sensitive data. Users on Mac OS X and Windows, on or off the network, working anytime, anywhere, receive the full benefit of advanced threat defenses and DLP. Control the use of removable media, like USB drives, with options to block or encrypt policy-identified data. Control the flow of data to cloud services, all while innovating as needed to grow your organization.

MANAGE EASILY WITH YOUR EXISTING IT STAFF

Staffing challenges within IT include limited headcount and finding skilled security personnel. The TRITON architecture unifies the management of Web, Email, Data, and Endpoint security, including policies that can be easily defined and deployed where needed. Quickly respond to new threats across multiple channels, including securing roaming users. Secure your sensitive IP and PII data while easily meeting your compliance and regulation requirements with and extensive library of out-of-the-box policies.

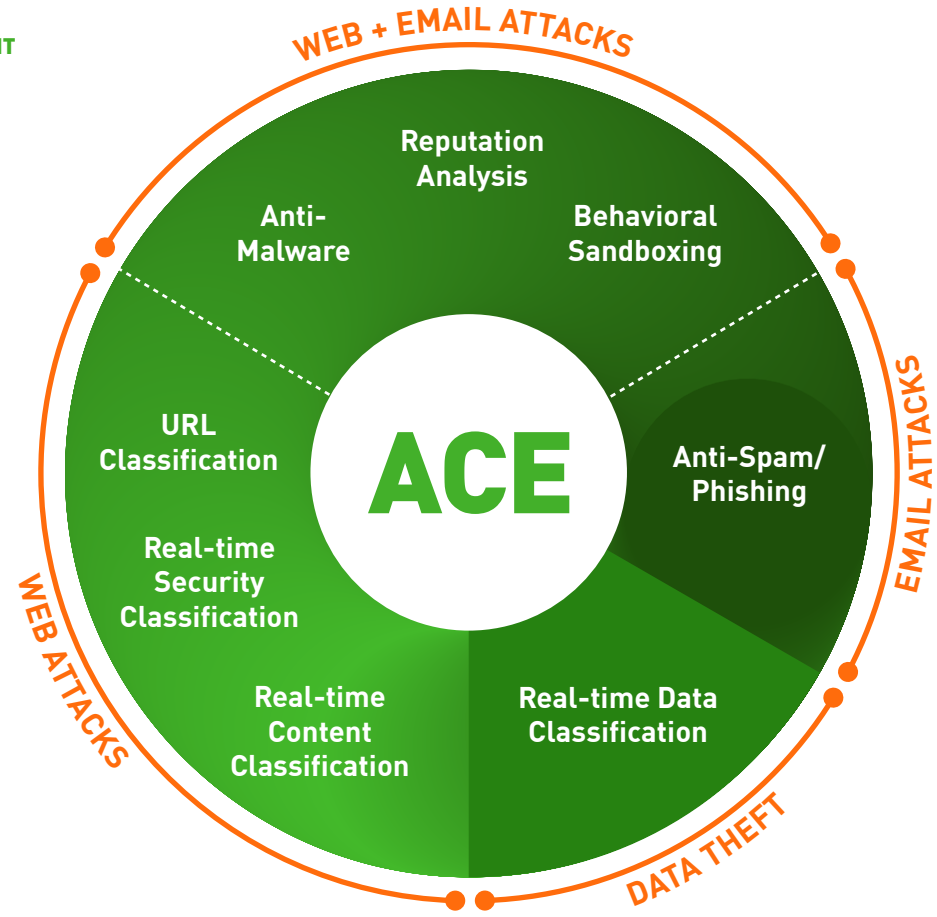
The power behind TRITON solutions

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.

INTEGRATED SET OF DEFENSE ASSESSMENT CAPABILITIES IN 8 KEY AREAS.

- 10,000 analytics available to support deep inspections.
- Predictive security engine sees several moves ahead.
- Inline operation not only monitors, but **blocks** threats.



ThreatSeeker® Intelligence Cloud

The ThreatSeeker Intelligence Cloud, managed by Forcepoint Security Labs™, provides the core collective security intelligence for all Forcepoint security products. It unites more than 900 million endpoints, including inputs from Facebook, and, with Forcepoint ACE security defenses, analyzes up to 5 billion requests per day. This expansive awareness of security threats enables the ThreatSeeker Intelligence Cloud to offer real-time security updates that block Advanced Threats, malware, phishing attacks, lures and scams, plus provides the latest web ratings. The ThreatSeeker Intelligence Cloud is unmatched in size and in its use of ACE real-time defenses to analyze collective inputs. (When you upgrade to Web Security, the ThreatSeeker Intelligence Cloud helps reduce your exposure to web threats and data theft.)

TRITON Architecture

With best-in-class security and a unified architecture, Forcepoint TRITON offers point-of-click protection with real-time, inline defenses from Forcepoint ACE. The unmatched real-time defenses of ACE are backed by Forcepoint ThreatSeeker Intelligence Cloud and the expertise of Forcepoint Security Labs researchers. The powerful result is a single, unified architecture with one unified user interface and unified security intelligence.

TRITON APX

TRITON APX provides many key benefits to organizations interested in deploying the best possible protection against Advanced Threats across the 7-Stage Kill Chain. They can be summarized in these three statements:

- **Deploy Adaptive Security** - Deploy adaptive security solutions for rapidly changing technology and threat landscapes.
- **Protect Everywhere** - The perimeter is the data. Protect critical information from theft whether on-premise, in the cloud or on mobile devices.
- **Raise the Security IQ** - Combat the cyber security skills shortage by providing predictive actionable intelligence across the entire threat lifecycle.

CONTACT
www.forcepoint.com/contact

[BROCHURE_TRITON_AP_ENDPOINT_EN] 400005.042016

FORCEPOINT
POWERED BY Raytheon