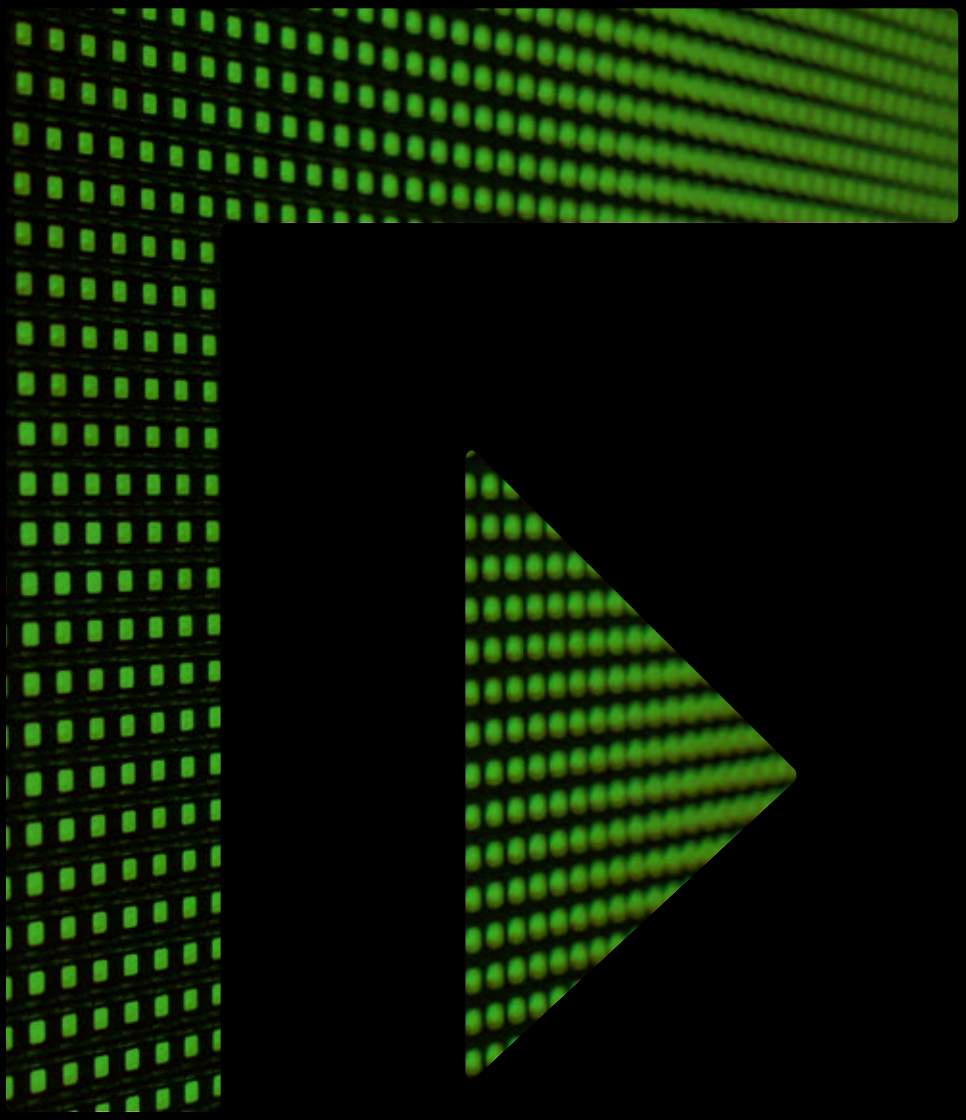


TRITON® AP-EMAIL

STOP ADVANCED TARGETED ATTACKS, IDENTIFY HIGH RISK USERS AND CONTROL INSIDER THREATS

FORCEPOINT
POWERED BY Raytheon

TRITON® AP-EMAIL

STOP ADVANCED TARGETED ATTACKS, IDENTIFY HIGH RISK USERS AND CONTROL INSIDER THREATS

From socially engineered lures to targeted phishing, most large cyberattacks begin with email. As these advanced, multi-stage threats blend web and email elements throughout attacks, they present a "Kill Chain" of opportunities to stop them before the breach occurs.

Maximize your use and safety of email

TRITON® AP-EMAIL identifies targeted attacks, high-risk users and Insider Threats while empowering mobile workers and the safe adoption of new technologies like Office 365 and Box Enterprise. From inbound attack activity to outbound data theft or botnet communication attempts, Forcepoint™ TRITON Email Security protects email communications as part of a complete TRITON APX defense against APTs and other Advanced Threats.

Email security challenges

- APTs commonly use email for early stages in their advanced attacks.
- Email must do more to address data theft and Insider Threats.
- Businesses need to adopt Office 365 and other services to expand and compete.
- Risky user habits can easily lead to security breaches and data loss.

"Ultimately, we are very happy with the Forcepoint products. Forcepoint TRITON Email Security is doing its job and stopping any problems before they reach our server."

— Ray Finck, Manager of Information Systems, Lowe Lippmann

TRITON AP-EMAIL capabilities

STOP APT AND OTHER ADVANCED TARGETED THREATS

The Forcepoint ACE (Advanced Classification Engine) is at the heart of all TRITON solutions and identifies malicious lures, exploit kits, emerging threats, botnet communications and other advanced threat activity across the Kill Chain. This enables TRITON AP-EMAIL to identify the early stages of an attack. With its powerful malware assessment capabilities that include a fully-integrated, file behavioral sandboxing, it can even identify Zero-day malware threats.

SECURE SENSITIVE DATA AGAINST EXTERNAL ATTACKS AND INSIDER THREATS

To prepare for a malicious Insider Threat or the potentially successful cyberattack, it's vital that outbound communications be monitored. This is also necessary both for data theft compliance needs as well as for business requirements. Only Forcepoint provides the technology to stop data infiltration and exfiltration with capabilities such as:

- OCR (Optical Character Recognition scanning to identify sensitive data hidden in images such as scanned documents or screen shots.
- Encrypted file detection to recognize custom encrypted files designed to defy identification.
- Drip DLP monitoring to identify where sensitive data is leaked in small quantities over time.

SAFELY ADOPT NEW TECHNOLOGIES LIKE OFFICE 365 AND BOX ENTERPRISE WHILE SUPPORTING YOUR ROAMING WORKFORCE

IT departments are strained to maintain current systems while supporting an increasingly mobile workforce and the demands to adopt new technologies like Office 365. TRITON AP-EMAIL provides industry-leading capabilities that leverage systems and other information to control communications, such as preventing total access to sensitive email attachments on vulnerable mobile devices, while permitting full access on fully-secured laptops. These inbound and outbound defenses are all supported on Office 365.

IDENTIFY 'HIGH-RISK' USER BEHAVIOR AND EDUCATE USERS TO IMPROVE AWARENESS

The rich data collections in TRITON AP-EMAIL are used by a number of policies to report and identify systems that may require special IT attention. They generate a report on a number of Indicators of Compromise to identify infected systems and more proactive reports on suspicious behavior, or even "disgruntled employee" activity as potential Insider Threats. User feedback capabilities help educate employees as mistakes are made, helping them to better learn and understand safe email best practices.

Enhanced Protection Modules

EMAIL CLOUD OR EMAIL HYBRID MODULE	**Leverage cloud services for performance and scalability** Combine on-premise threat defenses with cloud-based prefiltering services to preserve bandwidth with industry-leading anti-spam SLA's. Or choose a 100% Cloud deployment of all TRITON AP-EMAIL services.
EMAIL DLP MODULE	**Block data theft with enterprise-class content-aware DLP** Prepare for the Insider Threat and malware data theft, achieve compliance goals and further mitigate the risk to personal information or IP. Advanced capabilities detect data theft concealed in images or custom-encrypted files, or even transmitted in small amounts over time to evade detection.
EMAIL SANDBOX MODULE	**Integrate behavioral sandboxing for additional malware assessment** Supplement Forcepoint ACE analytics with an integrated file sandbox for additional deep inspection, and take advantage of behavioral analysis in a virtual environment to uncover the malicious behaviour of Zero-day and other advanced malware. Test files automatically or manually to generate detailed forensics.
EMAIL ENCRYPTION MODULE	**Ensure the confidentiality of sensitive communications** Enable mobile devices in your workplace by extending your existing security policies to mobile devices to protect them from Advanced Threats, mobile malware, phishing attacks, spoofing and more.
IMAGE ANALYSIS MODULE	**Identify explicit images to enforce acceptable use and compliance** The Forcepoint Image Analysis Module allows employers to take proactive measures to monitor, educate and enforce the company email policy in regard to explicit or pornographic image attachments.
TRITON APX	**The Forcepoint recommended solution for complete protection** Extend your protection from TRITON AP-EMAIL to TRITON AP-WEB, TRITON AP-DATA or TRITON AP-ENDPOINT for powerful, unified protection across all channels of attack.

"TRITON Email Security was attractive because it took away the overhead of managing our email security and delivered more than we expected in terms of resilience and ease-of-use. Overall, TRITON Email Security has enabled us to deliver a more resilient, professional and cost-effective service to our users."

—Martin Law, Head of IT, NCP

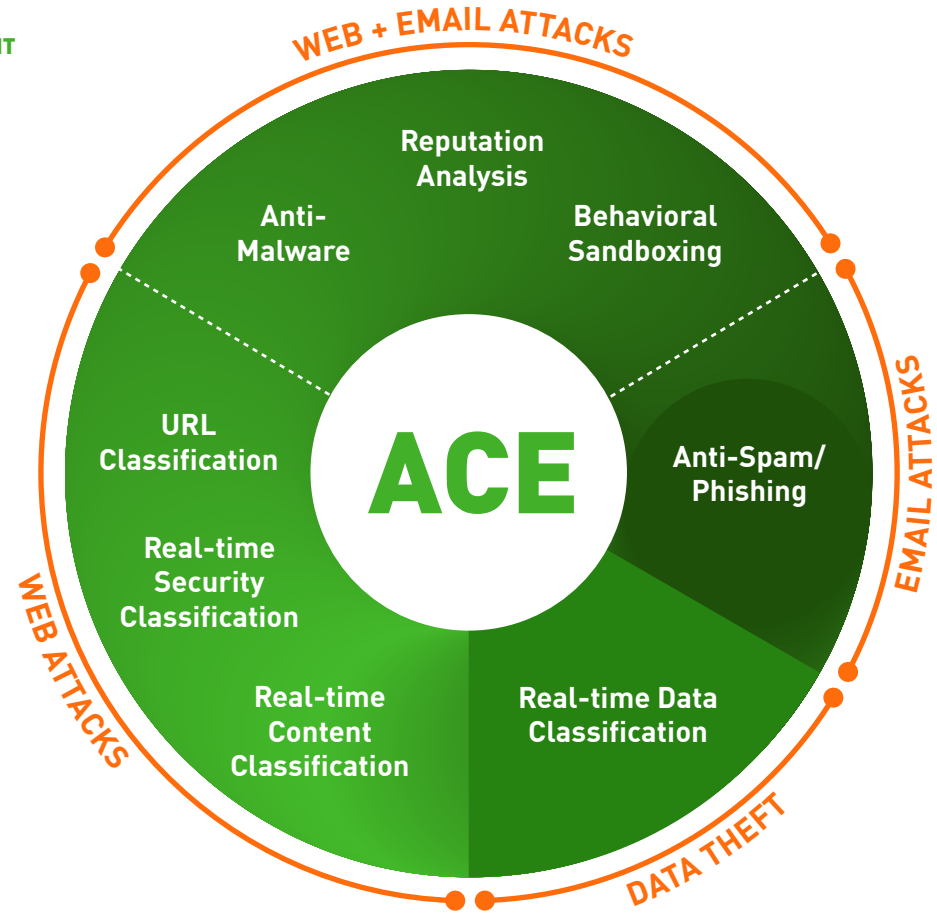
The power behind TRITON solutions

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.)

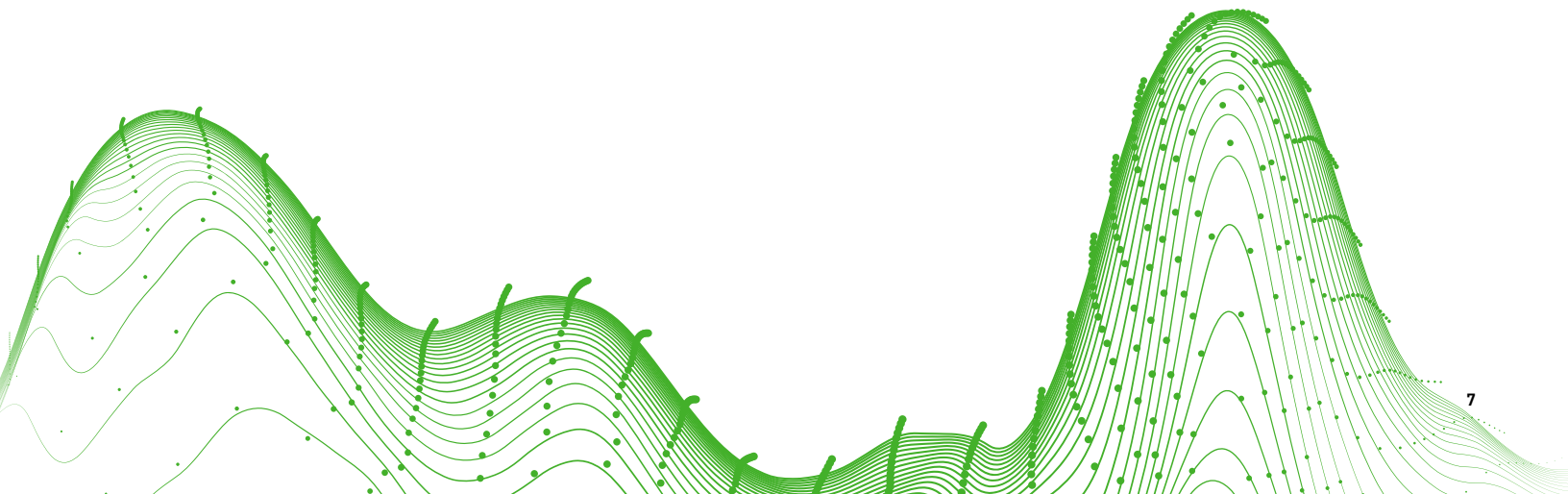
TRITON Architecture

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_EMAIL_EN] 400003.011416

FORCEPOINT
POWERED BY Raytheon