TRITON® AP-DATA and TRITON AP-ENDPOINT

GAIN VISIBILITY AND CONTROL TO SECURE YOUR DATA

FORCEPOINT
POWERED BY Raytheon

TRITON® AP-DATA and TRITON AP-ENDPOINT

UNRIVALED VISIBILITY AND CONTROL OVER YOUR CRITICAL DATA WHEREVER IT IS – IN THE OFFICE, ON THE ROAD OR IN THE CLOUD

Your critical data is mobile, stored and accessed in cloud services like Office 365 and Box to encourage collaboration around the world. TRITON® AP-DATA is an industry-leading DLP solution with the visibility and control to protect your data, whether it's stored and accessed on mobile devices such Windows and Apple laptops or shared via email and IM.

Protect your sensitive data wherever it lives – on endpoints, in the Cloud or on-premises with TRITON AP-DATA.

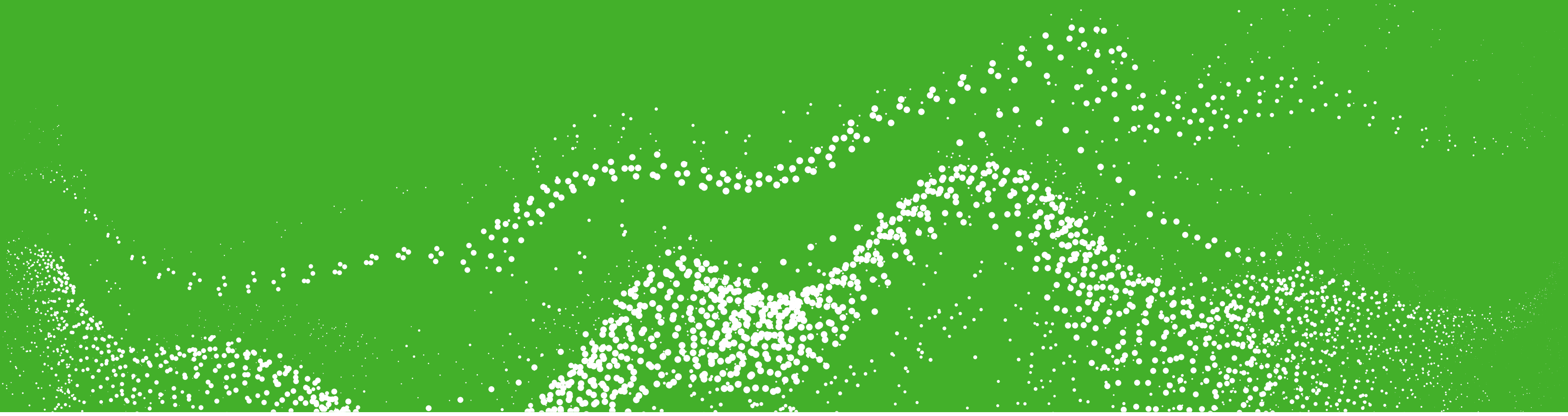
Forcepoint DLP Empowers Your Organization

- Quickly address global and industry-specific regulatory compliance requirements with pre-defined policies that are maintained and updated by Forcepoint's dedicated research team
- Leverage data classification tools to identify and protect your intellectual property no matter where it is stored
- Behavioral policies combine content and context awareness to automatically identify high risk behavior by users, such as forwarding emails to personal accounts or packaging data using encryption for exfiltration purposes
- Easily find and secure files stored on Mac, Windows, and Linux endpoint devices
- Identify and prevent data loss within cloud services like Office 365 and Box
- Implement effective role-based access controls and comprehensive auditing to meet internal and external compliance requirements
- Seamlessly integrate with third party data security solutions from Microsoft, HP, Splunk, IBM, Titus, Boldon James and Citrix
- DLP analytics that use data modeling and statistical analysis to automatically identify user behavior presenting the highest risk of data loss or theft, allowing your security operations team to leverage Forcepoint's research expertise
- Forcepoint's TRITON architecture lets you unify your security solutions, coordinate defense policies, shares intelligence along multiple points and enjoy centralized management of your data security

Key Features

- **Incident Risk Ranking** uses advanced data analytics to provide your security operations team with a stack ranked report on the top data security risks within your organization
- **Integrated OCR** identifies sensitive data and IP markers within images such as CAD designs, scanned documents, MRI's and screen shots
- **Drip DLP** considers cumulative data transmission activity over time to discover small amounts of data leakage
- **Behavioral-based policies** combine content and context awareness to automatically identify when sensitive data is being put at risk by users
- **Our unique PreciseID Fingerprinting** can detect a partial fingerprint of structured (database records) or unstructured data (documents) on Mac and Windows endpoints – whether an employee is working in the office or off the network
- **Automatically encrypt data** being transferred onto removable storage devices to enable secure data sharing with partners
- **Email-based incident workflow** makes it easy to distribute an incident for review and remediation to data owners and business stakeholders without having to provide access to the DLP management system
- **Detect and prevent** sensitive data being sent out of the organization via email, web uploads, IM and cloud service clients - includes Native SSL decryption for both network traffic and on the endpoint
- **Deploy DLP Components** in Microsoft to apply DLP policies in Microsoft Office 365

> **“TRITON data security was the strongest solution we found to stop and prevent data leakage.”**
>
> — Amir Shahar, Information Security Manager,
> Cellcom Israel Ltd.



TRITON AP-DATA Capabilities

EMBRACE INNOVATION WITH CONFIDENCE

Meeting your customer needs and remaining competitive requires innovation and enabling your workforce to adopt new technologies. Forcepoint’s DLP solution, TRITON AP-DATA, extends data security controls into enterprise cloud applications and to your endpoints. This allows you to safely leverage powerful cloud services like Microsoft Office 365, Google for Work and SalesForce.com, as well as protect your sensitive data and intellectual property on Windows and Mac laptops, both on and off the network.

Forcepoint enables the secure sharing and collaboration of data within the organization and outside to trusted partners with policy-based encryption of sensitive data transferred onto removable storage devices that are automatically decrypted on endpoints running AP-ENDPOINT.

EASE THE BURDEN OF DEPOLOYMENT AND MANAGEMENT

We offer the most precise and accurate Enterprise DLP polices with the easiest policy deployment of any DLP vendor. Our out-of-the-box global policy library and user-friendly wizard uses region and industry filters to recommend a set of DLP policies to quickly secure your intellectual property and regulated data, all in a single template. Forcepoint is also the first DLP provider to give you behavioral-based policies that combine content and context awareness to automatically identify when sensitive data is being put at risk by users. Email-based incident workflow makes it easy to distribute an incident for review and remediation to data owners and business stakeholders without needing to provide access to the DLP Management system. Satisfy auditors with standardized reports while enabling you to customize reports as needed.

COMPLETE DATA PROTECTION WITH THE INDUSTRY’S MOST ADVANCED TECHNOLOGIES

A malicious screen shot saved as a .jpeg, medical images, bank images or legacy records scanned and stored as images present blind spots for traditional DLP solutions - but not for TRITON AP-DATA.

With Forcepoint’s OCR (Optical Character Recognition), you can reliably identify and secure sensitive data within an image. This unique ability allows you to control the flow of sensitive information in screen shots, fax pages, smart phones and table photos, as well as in documents such as checks, receipts and scanned legacy files, protecting you from advanced attacks and the insider threat of data theft.

Gain greater visibility to see advanced data theft tactics such as custom encryption to obfuscate data or data sent in small volumes to avoid detection.

LINK DATA MOVEMENT WITH USER BEHAVIOR FOR COMPLETE DATA PROTECTION

Forcepoint is the first vendor to integrate our advanced DLP solution with SureView® Insider Threat to provide context around data policy violations and to document users’ intent. This industry-leading combination provides you with context around user attempts to transfer sensitive data. An “over-the-shoulder” view with DVR capture and playback provides the needed context into user activity and your data, identifying the early warning signs of a system being hijacked, stolen credentials, a rogue user, or one just making mistakes.

TRITON AP-DATA and TRITON AP-ENDPOINT Components

The combination of TRITON AP-DATA (AP DATA DISCOVER and AP-GATEWAY) with AP-ENDPOINT extends Forcepoint's Enterprise DLP controls to the channels that present the greatest risk to your data: Web, email, cloud applications and endpoints. Forcepoint is the only vendor that provides Enterprise-class policies and technology to secure integrated channels (Web and email) and carry those policies and reports over to an Enterprise DLP solution, while providing you with the industry's most advanced technology to secure your critical data. PreciseID Fingerprinting can detect even a fragment of structured or unstructured data residing on-premises, in the Cloud, or on a Windows or Mac endpoint, on or off the network.

TRITON AP-ENDPOINT DLP

Forcepoint TRITON AP-ENDPOINT DLP protects your critical data on Windows and Mac endpoints on and off the corporate network. PreciseID Fingerprinting enables you to detect even a fragment of structured or unstructured data on an endpoint off the network. Monitor web uploads, including HTTPS as well as uploads to cloud services like Office 365 and Box Enterprise. Full integration with Outlook, Notes and email clients, all while using the same user interface as Forcepoint's Data, Web, Email and Endpoint solutions.

TRITON AP-DATA DISCOVER

TRITON AP-DATA DISCOVER identifies and secures sensitive data across your network, as well as data stored in cloud services like Office 365 and Box Enterprise. With the addition of TRITON AP- ENDPOINT DLP, the power of AP-DATA Discover can be extended to Mac OS X and Windows endpoints on and off the network. Leverage the industry's most advanced fingerprinting technology to ensure your sensitive data is not compromised.

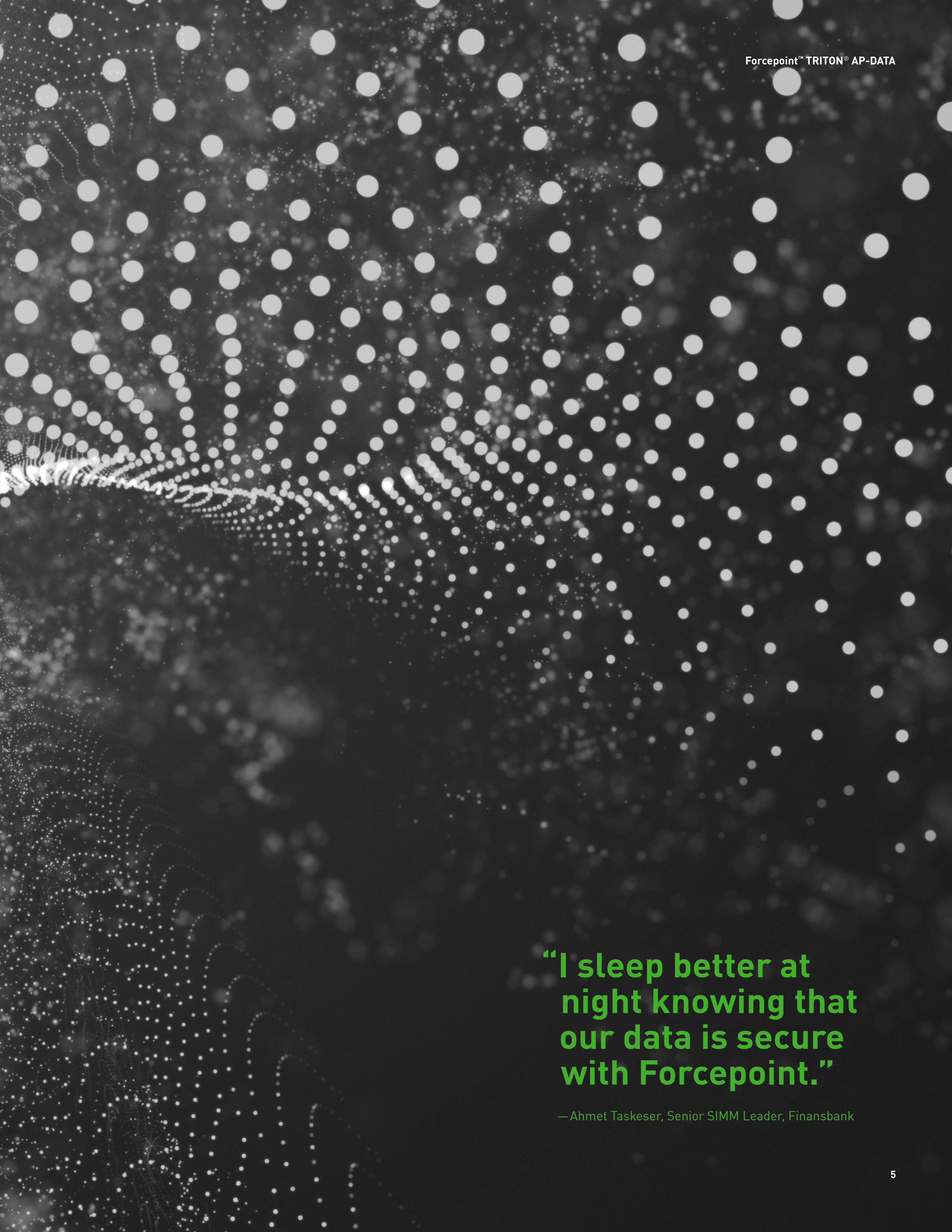
TRITON AP-DATA GATEWAY

It's critical to stop the theft of data in motion through email and Web channels. TRITON AP-DATA GATEWAY helps identify and prevent malicious and accidental data loss from outside attacks or from the growing insider threat. Counter advanced threat evasion techniques with powerful OCR (Optical Character Recognition) to recognize data within an image. Use Drip DLP to stop the theft of data one record at a time and for behavior monitoring for high-risk user identification.

IMAGE ANALYSIS MODULE

To meet regulatory obligations in many parts of the world, or simply to ensure a harassment-free environment, the optional Image Analyses Module identifies explicit images, such as pornography, stored on the organization's network or in motion through email or Web channels.

To request a demo go to forcepoint.com/contact



> “I sleep better at night knowing that our data is secure with Forcepoint.”
>
> — Ahmet Taskeser, Senior SIMM Leader, Finansbank

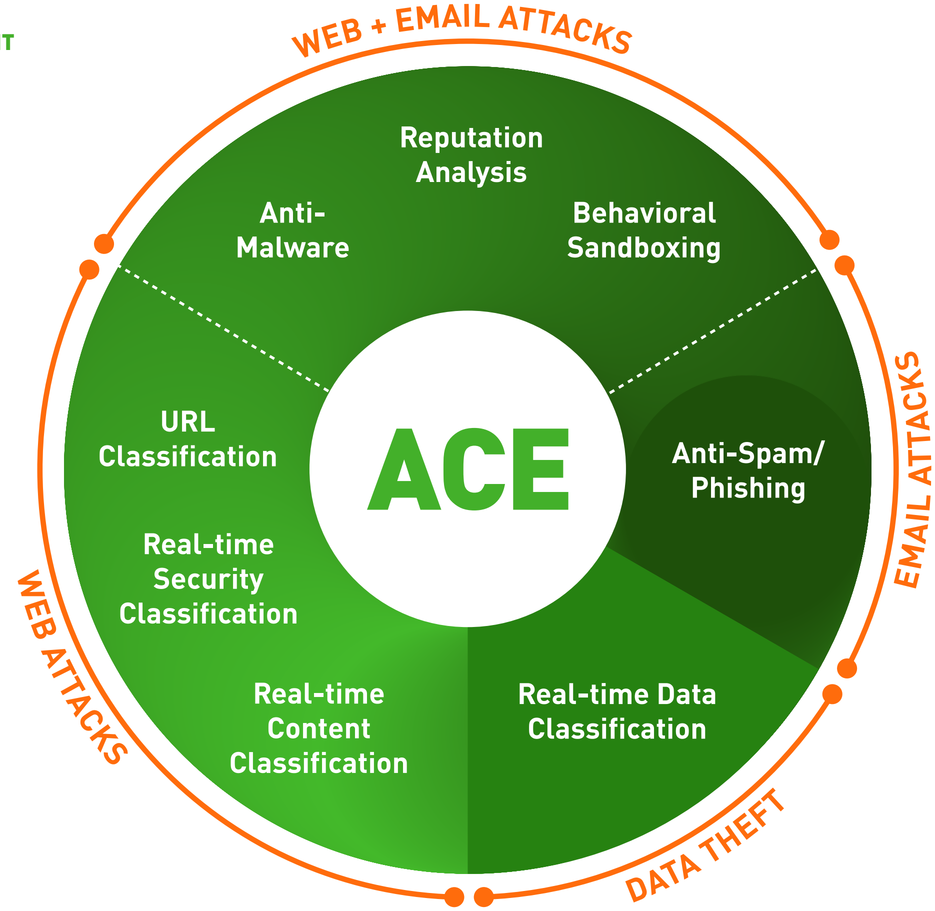
The power behind TRITON® solutions

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-premises, 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

FORCEPOINT
POWERED BY Raytheon