

# APX DLP Modules

**GAIN VISIBILITY, CONTROL AND SECURITY OF INBOUND AND OUTBOUND SENSITIVE DATA BY EXTENDING ENTERPRISE DLP CAPABILITIES TO YOUR WEB AND EMAIL CHANNELS**

**From a damaged reputation to regulatory fines and penalties, a data breach can have devastating consequences for your organization. And as workforces become more mobile, it's critical that you get visibility into the sensitive data coming and going to and from your network.**

**To stop data theft, demonstrate compliance and safeguard your brand and intellectual property, your IT defenses must work outside your organization. You must secure your sensitive data in Web and Email channels for your mobile workforce working off network. Extending full Enterprise DLP capabilities to your defenses gives you the ability to do that on both Web and Email channels and much, much more.**

## **WHY FORCEPOINT™ WEB & EMAIL DLP MODULES?**

Forcepoint Web DLP and Email DLP Modules leverage highly accurate, industry-leading technology to quickly and easily meet compliance and regulatory requirements by extending full enterprise-class DLP capabilities to Web and Email channels. They provide real-time and historical visibility into the transmission of sensitive data at all times. With a number of unique capabilities, such as OCR (Optical Character Recognition) and custom encryptions identification, Forcepoint takes enterprise-class DLP to a new level.

- Extensive out-of-the-box library of templates enables you to quickly set up and deploy policies to identify and stop data theft of your critical data.
- Easy-to-use wizard to deploy DLP Web and Email modules with your existing staff has never been easier.
- Gain visibility to data inbound and outbound from your network through Web and Email channels
- Prevent "drip-DLP", the low and slow data theft of credit card numbers or other records one or two at a time.
- Stop Insider Threats with behavioral analytics that identify and flag those who may present a risk to your organization.
- OCR (Optical Character Recognition) exposes text within an image to prevent data going out hidden in screen shots, photos and other images.
- With TRITON® AP-EMAIL, apply DLP policies to Microsoft® Office 365 traffic to secure sensitive data while embracing new technologies.
- Remediate sensitive data, enabling you to audit, block, allow, alert, notify, quarantine\*, or encrypt\* when found. [\*for Email DLP Module only]



**SOLUTION THAT QUICKLY DEPLOYS AND SECURES MY CRITICAL DATA FROM LEAVING MY NETWORK VIA WEB AND EMAIL CHANNELS**

With an extensive library of out-of-the-box templates and policies, Forcepoint quickly gets you up and running securing your sensitive data.

**NEED TO BE ABLE TO MANAGE WITH EXISTING STAFF**

Forcepoint TRITON® architecture is a fully integrated combining reporting, data management and policy management all into one user interface for your Web, Email, Data, Cloud, and Mobile solutions.

**IDENTIFY AND EDUCATE HIGH RISK USERS**

Behavioral analytics identify and flag those who may present a risk to the organization based on bad habits or even disgruntled employees.

**DON'T KNOW WHAT DATA IS LEAVING MY NETWORK OR HOW**

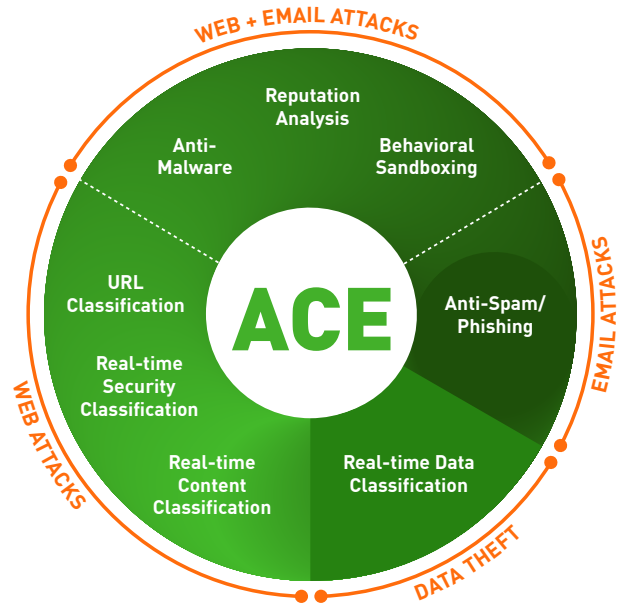
Get visibility into the sensitive data coming and going via your Web and Email channels with Forcepoint Web and Email DLP.

**VISIBILITY INTO THE SENSITIVE DATA LOCATED IN IMAGES FROM SCANNED LEGACY FILES**

Forcepoint Optical Character Recognition (OCR) can see text inside images and enforce policies to prevent sensitive data found in scanned images from leaving your network.

**HAVE TO ENSURE REGULATED DATA DOES NOT LEAK OUT OF MY NETWORK IN SMALL BATCHES**

Stop the low and slow data leakage with Forcepoint Drip DLP. By looking at the cumulative events over time, it detects “drip” theft of one record or credit card number at a time.



**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.

**CONTACT**

[www.forcepoint.com/contact](http://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.

[DATASHEET\_MODULE\_DLP\_EN] 100007.011416

**FORCEPOINT**  
TRITON® APX