FORCEPOINT
POWERED BY Raytheon

Datasheet

APX TRITON® RiskVision™

GAIN VISIBILITY INTO NEXT GENERATION ADVANCED THREATS AND DATA THEFT

Defending against today's cyber threats requires enhanced scope and scalability to fully understand the effectiveness of current defenses. Forcepoint™ TRITON® RiskVision™ is a network monitoring appliance that provides unparalleled visibility into Advanced Threats, highlighting infected systems, call home communications, blended attacks and data exfiltration; uncovers Advanced Threats via sandboxing and many other real-time techniques; delivering actionable data in ready-to-use dashboards and reports.

WHY TRITON RISKVISION?

TRITON RiskVision is an unmatched threat monitoring solution. It combines real-time advanced threat defenses, global security intelligence, file sandboxing and data loss/data theft detection into a single appliance that is easy to deploy via a network TAP or SPAN port. TRITON RiskVision provides immediate visibility into Advanced Threats, data exfiltration and infected systems.

REAL-TIME DEFENSES, GLOBAL THREAT AWARENESS, SANDBOXING AND DLP

TRITON RiskVision unifies four key defenses into one platform:

- Forcepoint ACE uses seven defense assessment areas with over 10,000 analytics to provide real-time threat analysis of web and email traffic.
- Forcepoint ThreatSeeker® Intelligence Cloud unites over 900 million endpoints and analyzes 3-5 billion requests per day, providing global threat awareness and vital defense analytics to ACE.
- Forcepoint TRITON ThreatScope™ sandbox analyzes behavior of web downloads and email attachments to uncover Advanced Threats and communications and provides actionable forensic reporting.
- Data loss prevention (DLP) detects data exfiltration for registered data, criminal-encrypted uploads, and password file data theft.

FILE SANDBOXING & FORENSICS

- Integrated web download and email attachment file sandboxing for behavioral analysis and forensic reporting with actionable insights.

CLOUD APPLICATION VISIBILITY POWERED BY SKYFENCE

- Identify critical data threats from "shadow IT" by uncovering high risk cloud application usage and those users putting your data at risk.
- Identify safer alternative cloud applications.

INTEGRATED DLP DEFENSES

- Content and context aware DLP detects data exfiltration related to theft or loss.
- Data theft features include detection of data loss via outbound email, web communication including webmail, and cloud app usage.

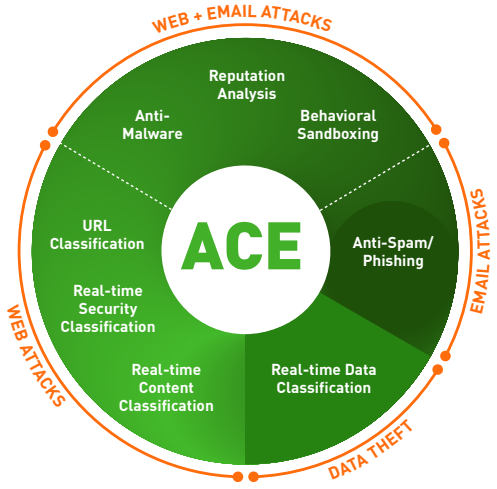
ADVANCED THREAT & DATA THEFT DETECTION

- ACE real-time defenses for advanced threat and data theft detection.
- More than 10,000 analytics enable defenses against undetected threats.

GLOBAL THREAT AWARENESS

- Security intelligence from the ThreatSeeker Intelligence Cloud.
- Analyzes up to 5 billon web, email and social networking requests per day.
- Facebook partnership provides insight into social media lures and threats.

YOUR NEEDS	FORCEPOINT SOLUTIONS
Advanced threat intelligence that works with existing countermeasures	Extensible threat intelligence platform channels threat intelligence into existing security controls for zero-latency defenses against Advanced Threats.
Visibility into cloud application usage and IT compliance	Identifies critical data threats from "shadow IT" by uncovering cloud application usage and those users putting your data at risk.
Visibility into Advanced Threats and data theft/data loss incidents	TRITON RiskVision combines real-time advanced threat defenses, global security intelligence, file sandboxing and data loss/data theft detection into a threat monitoring solution that provides insight into threats unseen by traditional defenses.
Advanced Threat detection beyond traditional defenses	ACE goes beyond anti-virus defenses by using seven defense assessment areas in a composite scoring process that uses predictive analysis. Multiple real-time content engines analyze full web page content, active scripts, web links, contextual profiles, files and executables. ACE leverages over 10,000 analytics derived from the ThreatSeeker Intelligence Cloud.
Detection of data theft and data loss within multiple channels	Advanced DLP defenses detect data theft and data loss. Advanced data theft defenses include detection of custom encrypted uploads, password file data theft, and slow data leaks (drip DLP) and geo-location destination awareness.
Sandboxing of files and objects to detect Advanced Threats, with actionable forensic reports	ThreatScope web file sandboxing provides behavioral analysis to uncover Advanced Threats and communications, plus detailed forensic reporting. An advanced threat dashboard provides forensic insight on who was attacked, what data was attacked, where the data was destined, and how the attack was executed. Security incidents include data theft capture when possible, with the ability to export forensic details to SIEM systems.
Ready-to-deploy appliance provides immediate visibility	TRITON RiskVision deploys on Forcepoint V10000 appliance via a network TAP or SPAN port deployment alongside TRITON management and reporting servers. Please refer to the latest V-Series datasheets for hardware specifications. Integrates with leading SSL decryption products.



THE FORCEPOINT DIFFERENCE

ACE

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

ABOUT FORCEPOINT

[DATASHEET_RISKVISION_EN] 100005.020216

FORCEPOINT
TRITON® APX