FORCEPOINT
POWERED BY Raytheon

Datasheet

Threat Protection Cloud

PREPARE FOR THE MOST ADVANCED, TARGETED ZERO-DAY THREATS AND APTS

Mass market threats have given way to more tailored, targeted attacks. The Forcepoint™ Threat Protection Cloud provides additional defenses for the most advanced, targeted Zero-day threats and APTs that attack through Web or Email channels. Forensic reporting and phishing education feedback strengthen proactive defensive measures.

WHY FORCEPOINT™ THREAT PROTECTION CLOUD?

The Forcepoint Threat Protection Cloud offers unrivaled protection enhancements to Forcepoint Web and Email security defenses. Integrated behavioral sandboxing results are considered along with other Forcepoint ACE analytics to counter innovative, emerging evasion techniques and ensure accurate identification of threats. Networked and mobile users enjoy real-time feedback regarding suspicious email communications, even when working remotely. And detailed sandbox forensics and phishing reports provide insights to help organizations assume a more proactive security posture against future attacks.

FORCEPOINT THREAT PROTECTION CLOUD ENHANCES DEFENSE IN FIVE AREAS:

1. **File Sandboxing for Web**
   Monitor Web traffic for real-time code analysis in a behavioral sandbox for Advanced Threat identification.

2. **File Sandboxing for Email**
   Intercept attachments in real-time for additional threat analysis in a behavioral sandbox.

3. **Email URL Sandboxing**
   Have suspicious links in email reassessed when they are accessed, not just when the email arrives.

4. **Detailed Forensic Reporting**
   Use sandbox results to guide any necessary response or proactive measures against future attacks.

5. **Phishing Education and Reporting**
   Increase phishing awareness at both the user and network levels to drive effective change.

BEHAVIORAL SANDBOXING FORENSICS

Forcepoint Threat Protection Cloud provides an online sandbox environment for safely testing potential malware. Using ACE analytics, all activity is monitored and documented in a detailed report including:

- The infection process and post-infection activity.
- System-level events and changes to files, processes, registry, etc.
- Network communications, including connections/methods used and destination.

Observed behavior is correlated with known threats to provide valuable, actionable insights.

POWERFUL FORENSICS

- Allows safe execution of suspicious code away from network resources.
- Research-grade sandbox used and managed by Forcepoint researchers.
- Detailed forensic reporting provides actionable insights.
- Graphical breakdown of the attack flow linked to every process and event.

Your Needs – Forcepoint Solutions

INTEGRATE WITH LEADING FORCEPOINT TRITON SOLUTIONS

Forcepoint Image Analysis is available as an optional add-on module for TRITON AP-EMAIL and AP-DATA solutions.

SECURE WEB AND EMAIL AGAINST ADVANCED MALWARE

Working with TRITON AP-WEB and AP-EMAIL, suspicious code is triggered in an isolated behavioral sandbox, allowing it to execute safely, yet reveal any malicious intentions. Intercepted in-line, IT is alerted of newly revealed threats in real time, along with a detailed forensic report.

ACTIONABLE INFORMATION FROM FORENSIC REPORTING

The sandbox forensic report provides details of both infection and post-infection activity that can be used to fine tune defenses against attacks, as well as identify and possibly recover infected systems.

INTEGRATED DEFENSES FOR MAXIMUM EFFECTIVENESS

Sufficient clues to a truly advanced, targeted attack may not exist solely in well-crafted malicious code. Therefore, Forcepoint Threat Protection results are also considered in context with an ACE analysis of the delivery vehicle (Web or Email).

ADVANCED EMAIL LINK DEFENSES

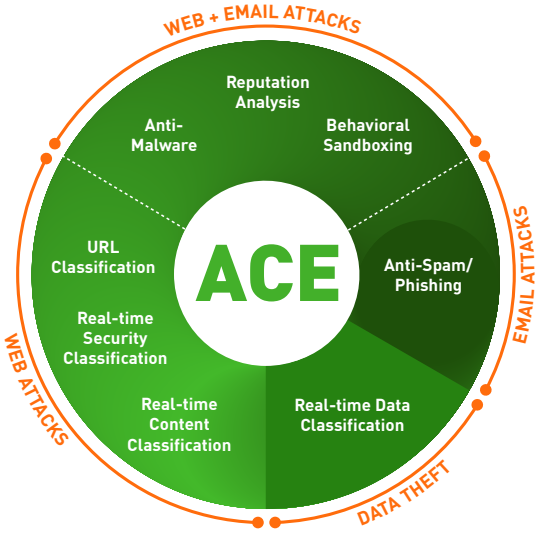
Suspicious URLs are modified such that when a user clicks the link in a message from any device (e.g., laptop, smart phone, tablet), the URL is analyzed in real time before allowing access. Despite other benefits, this is invaluable when a website is compromised well after the link is originally delivered via email.

PERSONALIZE PHISHING FACTS

Both users and IT staff are provided with customized information. User education and feedback alert users to risks, while IT reports can identify trends that may indicate a need for policy, process or other changes.

"Malware today is targeted, polymorphic and dynamic. It can be delivered via Web page, spear-phishing email, or any other number of avenues."

— IDC, Worldwide Specialized Threat Analysis and Protection 2013-2017 Forecast and 2012 Vendor Shares, August 2013



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_MODULE_THREAT_PROTECTION_CLOUD_EN] 100010.012616

FORCEPOINT
TRITON® APX