proofpoint.

SOLUTION BRIEF

Splunk Integration: Proofpoint On-Demand Email Security App and Add-On

Accelerate Response with a Consolidated View of Advanced Threats

REQUIREMENTS FOR PROOFPOINT ON-DEMAND EMAIL SECURITY APP

- Proofpoint Email Protection version 8.10 or later
- Splunk Enterprise version 6.5 or later
- Splunk Common Information Model (CIM) Add-On version 4.8 or later
- Proofpoint On-Demand Email Security Add-On for Splunk 1.0.2 or later
- Proofpoint TAP SIEM Modular Input 1.0.1 or later

REQUIREMENT FOR ENABLING PROOFPOINT ON DEMAND EMAIL SECURITY ADD-ON

- Proofpoint Email Protection version 8.10 or later
- Proofpoint On-Demand Log API key
- Splunk Enterprise version 6.5 or later
- Splunk Common Information Model (CIM) Add-On version 4.8 or later

REQUIREMENTS FOR PROOFPOINT TARGETED ATTACK PROTECTION (TAP) SIEM MODULAR INPUT

- Current URL Defense or Attachment Defense license
- Splunk 6.5 or later

As part of our partnership with Splunk, we offer you enhanced visibility into your email activities, advanced threats and data exfiltration. The Proofpoint On-Demand Email Security App for Splunk provides you with an executive dashboard and reporting capabilities. These features help you pinpoint your security issues and respond quickly. And the app enhances our On-Demand Email Security Add-On, giving you rich, visual data you can act on.

Accelerate Threat Response with a Single Dashboard View

If your security team is standardized on the Splunk platform for threat research and incident response, now you can act faster. Proofpoint email security information is now displayed within the Splunk interface (see Figure 1). With an at-a-glance view of your security events and affected users, your security team can respond to security incidents more quickly. And with security information all in one place, they can quickly contain the spread of an attack.

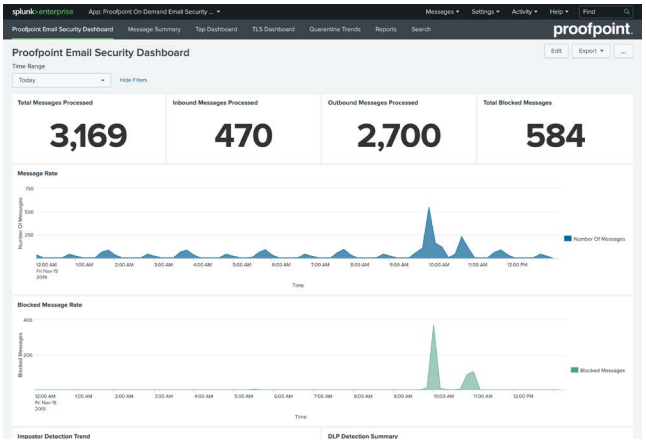

Figure 1: Email Security Dashboard

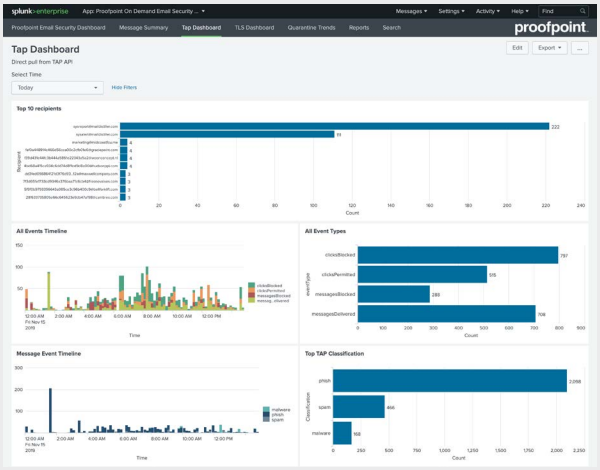

Figure 2: TAP Dashboard

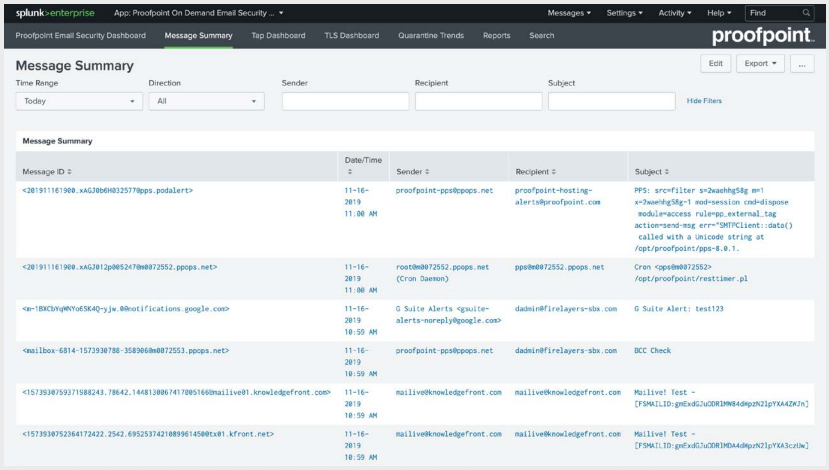

Figure 3: Sample search using On-Demand Email Security Add-On

Get Complete Visibility into Advanced Threats

With the Proofpoint On-Demand Email Security App for Splunk, your security team gets complete visibility into today's advanced threats. It's integrated with Proofpoint Email Protection and Proofpoint Targeted Attack Protection (TAP). And it gives you a consolidated view into your email-borne threats. These include ransomware, email fraud, credential phishing, targeted attacks and more.

Consolidate Reporting Easily

Proofpoint On-Demand Email Security Add-On uses Proofpoint on Demand (PoD) log API to download the logs. It extracts filter and mail logs and maps them to the Splunk CIM model. This makes it easier to create dashboards, reports and alerts using standard Splunk searches. The email security data feeds automatically correlate with Splunk Enterprise, Splunk Enterprise Security Reporting and other sources. This helps your security team zero in on malicious insiders and on other difficult-to-detect activity. And your admins can create customized queries to search and analyze email logs with other sources of data (Figure 3).

The Proofpoint TAP Modular Input Add-On integrates TAP seamlessly into your Splunk deployment. Your security operation teams can simplify their workflow by ingesting TAP events for the following scenarios into Splunk:

- Blocked or permitted clicks to threats recognized by Proofpoint URL Defense
- Blocked or delivered messages that contain threats recognized by URL Defense or Proofpoint Attachment Defense

The Proofpoint On-Demand Email Security Add-On, On-Demand Email Security App and TAP Modular Input are available for free download on Splunkbase.

LEARN MORE

For more information, visit **proofpoint.com/us/technology-partners/splunk**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.