proofpoint

ET Pro Rule Set

Highlights

- Keep pace with dynamic threat landscape with daily rule updates.
- Block attacks and campaigns before they damage your organization.
- Increase the ROI of existing network security systems with simple and easy-to-consume malware-focused rule set.
- Enforce custom security policies based on threat categories that matter to your organization.
- Improve fidelity and reduce false positives from existing intrusion detection / prevention systems (IDS/IPS) and next generation firewalls.
- Available in SNORT® or Suricata IDS/IPS format.

Even today's most sophisticated attack prevention systems cannot stop everything. When attackers get through, you need to know immediately, so you can limit the damage. The only way to know is to deploy technology designed to detect when attackers have bypassed these systems.

Proofpoint ET Pro is a timely and accurate rule set for detecting and blocking advanced threats using your existing network security appliances, such as next generation firewalls (NGFW) and network intrusion detection / prevention systems (IDS/IPS). Updated daily and available in SNORT and Suricata formats, ET Pro covers more than 40 different categories of network behaviors, malware command and control, DoS attacks, botnets, informational events, exploits, vulnerabilities, SCADA network protocols, exploit kit activity, and more.

Why Proofpoint ET Pro?

Today, advanced cyber attack campaigns are perpetrated by a variety of actors with motives ranging from profit to espionage. While the basic tools used to execute these attacks have common elements and are often derived from fewer than 20 known exploit kits, each campaign is unique in its use of bot nets, proxies, attack vectors, and command and control systems.

Given the dynamic nature of these campaigns, it has become nearly impossible for enterprises to keep pace with the changing threat landscape. That's where Proofpoint comes in.

Serious security professionals have very few high-quality options available for network detection rules. At Proofpoint ET we leverage our massive international malware exchange, an automated virtualization and bare metal sandbox environment, a global sensor network, and over a decade of anti-evasion and threat intelligence experience to develop and maintain our ET Pro rule set.

There are five requirements for producing quality network-based detection in the face of a constantly evolving threat landscape:

- Early access to the latest malware samples from around the world.
- An automated sandbox environment, capable of evaluating millions of new malware samples per day and capturing the resulting network behavior.
- Dedicated focus on detecting the interaction between the compromised organization and the attackers' command and control systems.
- Unwavering commitment to writing and testing high-fidelity detection signatures to minimize false positives.
- Daily updates.

The Proofpoint ET Pro rule set delivers on all five.

Network-Based Advanced Threat Detection

Security teams are often dissatisfied with their network IDS/IPS and NGFW deployments due to the overwhelming number of false positives and their inability to notify them when an actual breach takes place. This is because standard IDS/IPS signatures are designed to detect exploits against known vulnerabilities in hosts on the network – even if the systems are patched and not actually vulnerable. Yet, these security platforms are ideally positioned on the network to monitor for malware activity, including stealth communication to and from the remote command and control sites.

ET Pro features include:

- Emphasis on compromises missed by traditional prevention methods.
- Support for both SNORT and Suricata IDS/IPS formats.
- Over 26,000 rules in over 40 categories.
- 10 to 30+ new rules are released each day.
- Includes ET Open. ET Pro allows you to benefit from the collective intelligence provided by one the largest and most active IDS/IPS rule writing communities. Rule submissions are received from all over the world covering never seen before threats—all tested by the Proofpoint's ET Labs research team to ensure optimum performance and accurate detection.
- Very low false positive rating through the use of state-of-the-art malware sandbox and global sensor network feedback loop.
- Extensive signature descriptions, references, and documentation.

Proofpoint Layered Security

Individual security systems can be effective at blocking certain types of threats, but without complete coverage, compromise is inevitable.

- Deploy ET Pro real-time detection logic in your IDS/IPS/NGFW.
- Get actionable intelligence and global context for detecting advanced threats with ET Intelligence.
- Investigate attacks seen in email-based attacks via Targeted Attack Protection and Proofpoint Enterprise Protection.
- Dive deeper into advanced threat forensics reported by URL Defense Service and Attachment Defense Service.
- Investigate and block threats with Threat Response.
- Use intelligence to extend the ability to safeguard sensitive and confidential data with Proofpoint Enterprise Privacy.

Focused Coverage

While the Proofpoint ET Pro offers complete coverage for numerous threats, it offers unrivaled network-based detection logic to identify Malware command and control communications, known bad landing pages, bot nets, communication with drive by sites and other advanced threats – using your existing IDS/IPS or NGFW platform.

ET Pro bolsters your network security platforms with high-fidelity detection of advanced threats, including:

- All major malware families covered by command and control channel and protocol.
- Detection across all network-based threat vectors, from SCADA protocols, Web Servers, to the latest client-side attacks served up by exploit kits.
- The most accurate malware call-back, dropper, command-and-control, obfuscation, exploit-kit related, and exfiltration signatures the industry can offer.
- Comprehensive rule set also includes regularly prescribed CVE updates, including MS MAPP & Patch Tuesday updates.

Platform Independent

The Proofpoint ET Pro rule set is available in multiple formats for use in a variety of network security applications. The formats include various releases of SNORT and Suricata IDS/IPS platforms. It is the only rule set that is specifically written for the Suricata platform to take full advantage of next generation IDS/IPS features. The ET Pro rule set is optimized to make the best use of the feature set and version of each IDS/IPS engine it supports.

The ET Pro rule set:

- Runs transparently on systems supporting the current and earlier versions of SNORT.
- Is the only ruleset optimized for the next generation Suricata open source IDS/IPS engine.

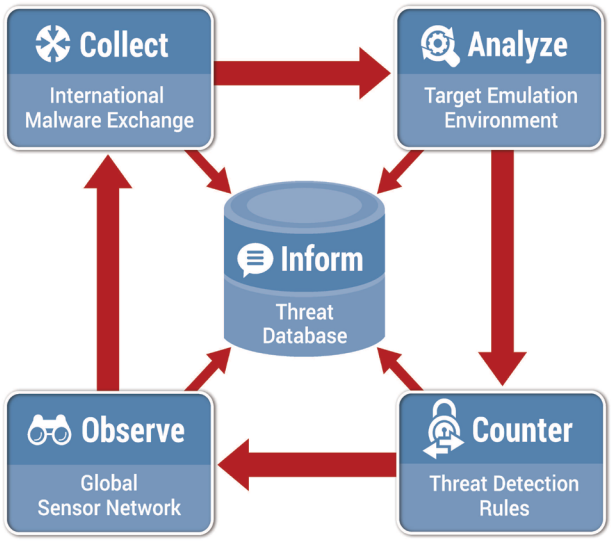
Proofpoint can also create custom OEM versions ET Pro for integration into proprietary network security appliances.

Created by the Malware Experts at ET Labs

The team of dedicated threat researchers at Proofpoint ET Labs do the difficult work so you don't have to. The result is a comprehensive set of signatures for detecting advanced malware and other threats on your network.

Built upon a proprietary process that leverages one of the world's largest active malware exchanges, victim emulation at massive scale, and a global sensor feedback network, Proofpoint ET Pro is updated daily to provide organizations with actionable intelligence to combat today's emerging threats.

- Proofpoint ET Labs manages one of the world's largest private malware exchanges with over 40 global participant organizations.
- ET Labs analyzes approximately 200,000 new unique malware samples every day in a proprietary network sandbox to create new signatures.
- ET Pro is the only IDS/IPS rule set from a research team proven to keep pace with dynamic nature of today's threat landscape.
- Leverages the ET Open community for extended coverage of vulnerabilities and other threats observed by independent security practitioners around the world.



Contact Proofpoint Today

The modern threat landscape is a lopsided battleground, where defenders must guard many fronts while attackers only need to find a single opening. Every day, organizations are threatened with thousands of cyber attacks resulting in serious security breaches that result in billions of dollars in lost revenue and damaged reputation. Subscribers to the ET Pro rule set can detect and identify malicious threats before they cause extensive breaches and data exfiltration.

About Proofpoint

Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.

892 Ross Drive
Sunnyvale, CA 94089
1.408.517.4710
www.proofpoint.com