Proofpoint ET Pro Ruleset

Keep Up with Today's Advanced Threats with Network-Based Detection

KEY BENEFITS

- Stay on top of the dynamic threat landscape with daily rule updates
- Block attacks and campaigns before they do harm
- Increase the return on investment of your network security with rules that focus on malware and are easy to consume
- Enforce security policies based on threat categories that matter to you
- Improve fidelity and reduce false positives from existing IDS, IPS and NGFW
- Available in Suricata and Snort IDS and IPS format

Proofpoint ET Pro Ruleset is a timely and accurate rule set for detecting and blocking advanced threats. Updated daily, it covers malware delivery, command and control, attack spread, in-the-wild exploits and vulnerabilities and credential phishing. It also detects and blocks distributed denial-of-service attacks (DDoS), protocol and application anomalies, exploit kits and supervisory control and data acquisition (SCADA) attacks.

Why Proofpoint ET Pro Ruleset?

Cyber criminals with many different motives, launch today's advanced attacks with increasing frequency. Some focus on making a profit, while others engage in espionage. The tools they use have a lot in common. But each campaign is different. It uses botnets, proxies, attack vectors and command-and-control systems. This makes it nearly impossible to keep pace with changes in the threat landscape. That's where Proofpoint comes in.

ET Pro Ruleset signature writing is based on real-world threats that surface every day. Most security teams have few good options for network detection rules. For ET Pro Ruleset, we leverage our massive international malware exchange, an automated virtualization and our bare metal sandbox environment. In addition, we take advantage of our global sensor network and more than a decade of anti-evasion and threat intelligence experience. ET signature writers also contribute to other Proofpoint products, such as Email Protection and Targeted Attack Protection. This helps us identify threats from other vectors, such as mobile, social, cloud applications, abuse mailboxes and more. That means we have ET Pro Ruleset coverage for all of these.

Email is the primary attack vector. But not all threats come in through corporate email. Some are web-based attacks, personal email or social media attacks and lateral network spread. Also, there are supply chain attacks and attacks against applications on servers. ET Pro Ruleset helps with all of these.

The five requirements for quality network-based detection are:

1. Early access to the latest malware samples from around the world, a global network of intrusion detection system (IDS) sensors and access to the latest attacks
2. An automated sandbox environment that can evaluate millions of new malware samples every day and capture the network behavior that follows
3. Detecting how a compromised organization interacts with attackers' command and control systems
4. A commitment to writing and testing accurate detection signatures to reduce false positives
5. Daily updates

ET Pro Ruleset delivers on all five.

Network-based advanced threat detection

Your security team may be dissatisfied with their network IDS, intrusion prevention system (IPS) and next-generation firewall (NGFW) deployments. This is due to the overwhelming number of false positives. Plus, these network security solutions often fail to notify your security team when a breach takes place. This is because standard IDS and IPS signatures detect exploits against known vulnerabilities in hosts on the network. This happens even if the systems are patched and not really vulnerable. But these security platforms are well positioned on your network to monitor for malware activity, including stealth communication to and from remote command and control sites.

Features include:

- Emphasis on compromises that traditional prevention methods miss
- Support for both Snort and Suricata IDS and IPS formats.
- Over 65,000 rules in over 50 categories
- 30 to 50 new rules released each day
- Includes ET Open Ruleset. Benefit from the collective intelligence provided by one of the largest and most active IDS and IPS rule-writing communities. We receive rule submissions from all over the world that cover threats that have never been seen before. The Proofpoint ET Labs research team tests these rule sets to ensure the best possible performance and accurate detection.
- Low false positive rates through our state-of-the-art malware sandbox and global sensor network feedback loop.
- Extensive signature descriptions, references and documentation.

Focused coverage

ET Pro Ruleset offers unrivaled network-based detection logic to uncover malware command and control communications. It also detects known bad landing pages, botnets, communication with drive-by sites and other advanced threats using your IDS, IPS or NGFW platform.

ET Pro Ruleset makes your network security more effective with accurate detection of advanced threats, including:

- All major malware families covered by command and control channels and protocols.
- Detection across all network-based threat vectors—from SCADA protocols and web servers to the latest client-side attacks served up by exploit kits.
- The most accurate signatures in the industry for malware call-back, dropper, command and control, obfuscation, exploit-kit related threats and exfiltration.
- A comprehensive rule set that also includes regularly prescribed CVE updates, including Microsoft Active Protection Program (MAPP) and Patch Tuesday updates.

Platform independent

ET Pro Ruleset is available in multiple formats for a variety of network security applications. These formats include various releases of Snort and Suricata IDS and IPS platforms. It is the only rule set that is written for the Suricata platform. And it takes full advantage of next-generation IDS and IPS features.

ET Pro Ruleset makes the best use of the feature set and the version of each IDS and IPS engine it supports. ET Pro Ruleset is the only rule set optimized for the next-generation Suricata open source IDS and IPS engine. Proofpoint is a platinum Open Information Security Foundation (OISF) sponsor and a contributor to the Suricata platform.

ET Pro Ruleset runs transparently on systems supporting the current and earlier versions of Snort.

We can also create custom OEM versions of the ET Pro Ruleset so that you can integrate it into your proprietary network security appliances.

Created by the malware experts at Proofpoint ET Labs

Our team of dedicated threat researchers at Proofpoint ET Labs do the hard work—so you don't have to. As a result, you get a comprehensive set of signatures for detecting advanced malware and other threats on your network.

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

- ET Labs manages one of the world's largest private malware exchanges, with over 70 organizations participating all over the world.
- ET Labs analyzes approximately 3,000,000 malware samples every day in a proprietary network sandbox. New samples number 300,000.
- ET Pro Ruleset is the only IDS and IPS rule set that is research-team proven to keep pace with the dynamic nature of today's threat landscape.
- Leverages the ET Open Ruleset community for extended coverage of vulnerabilities and other threats observed by independent security practitioners around the world.

Contact Proofpoint today

Today, defenders must guard many fronts. But attackers only need to find a single opening. Every day, organizations like yours are threatened with thousands of cyber attacks. These can result in serious security breaches that can cost you billions of dollars in lost revenue and damaged reputation. By subscribing to the ET Pro Ruleset, you can detect and identify malicious threats before they cause extensive breaches and data exfiltration.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance 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**.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. **Proofpoint.com**