proofpoint.

SOLUTION BRIEF

Proofpoint ET Pro Ruleset

Stay ahead of today's advanced threats with network-based detection



Key Highlights

- Respond to emerging threats faster with daily rule updates
- Block attacks and campaigns before they do harm
- Increase ROI of network security with malware-focused rules that are easy to consume
- Enforce security policies based on threat categories that matter to you
- Improve fidelity and reduce false positives across IDS, IPS, and NGFW
- Available in Suricata and Snort IDS and IPS format

Overview

Proofpoint ET Pro Ruleset is a timely and accurate ruleset for detecting and blocking advanced threats. Updated daily, it covers malware delivery, command and control, attack spread, in-the-wild exploits and vulnerabilities, credential phishing, DDoS, protocol and application anomalies, exploit kits, and SCADA attacks.

Built by Proofpoint ET Threat Research, the ruleset turns real-world malware intelligence into high-fidelity network detection that helps security teams keep pace with fast-changing campaigns across email, web, cloud, social, and lateral network threats.

The challenge

Attackers only need one opening, yet traditional controls can miss subtle signs of compromise. ET Pro Ruleset helps defenders detect threat activity earlier while reducing noisy alerts and improving confidence in network-based detection.

©Proofpoint, Inc. 2026

The Solution: Research-Driven Detection Plus Daily Protection

ET Pro Ruleset delivers on the five requirements for quality network-based detection: early access to malware samples and attacks, global IDS sensor visibility, large-scale sandbox analysis, accurate signature writing and testing, and daily updates.

The result is continuously refreshed detection logic that helps security teams uncover command-and-control communications, malware callbacks, botnet activity, exploit kits, exfiltration, and other advanced network threats.

Network-based advanced threat detection

Modern IDS, IPS, and NGFW deployments are well positioned to monitor malware activity and stealth communications to command-and-control sites, but they need high-fidelity detection to reduce false positives and surface real compromise activity.

Focused coverage

Detect major malware families, bad landing pages, botnets, drive-by sites, exploit-kit threats, callbacks, droppers, obfuscation, and exfiltration across network-based threat vectors.

- Malware delivery
- Command-and-control
- Exploit kits
- Credential phishing
- Attack spread
- DDoS
- SCADA
- Protocol anomalies

Key Capabilities:

- Emphasis on compromises that traditional prevention methods miss
- Support for both Snort and Suricata IDS and IPS formats
- Over 65,000 rules in more than 50 categories
- Between 30 to 50 new rules released each day

Operational Advantages:

- Low false-positive rates through sandbox and sensor feedback
- Extensive signature descriptions, references, and documentation
- ET Open Ruleset community intelligence included
- Regular CVE, MAPP, and Patch Tuesday updates

©Proofpoint, Inc. 2026

Created by the malware experts at Proofpoint ET

Proofpoint ET Threat Research does the hard work, so defenders don't have to. The team combines malware exchanges, victim emulation at massive scale, and a global sensor feedback network in a proprietary research process.

Operational Advantages:

- One of the world's largest private malware exchanges
- 70+ participating organizations around the world
- Approximately 3,000,000 malware samples analyzed every day
- New samples number around 300,000 daily

Detection Lifecycle

Collect
Malware, sensors, community

Analyze
Sandbox and victim emulation

Write
Test accurate signatures

Update
Publish daily rules

Platform independent

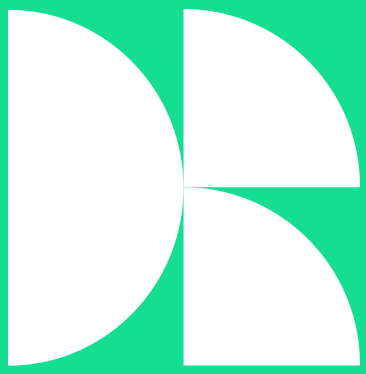
ET Pro Ruleset is available in multiple formats for network security applications. It is optimized for next-generation Suricata and runs transparently on systems supporting current and earlier versions of Snort.

Deployment Fit:

- Suricata-optimized rule content
- Snort-compatible deployments
- Custom OEM versions for proprietary appliances
- Extensive rule descriptions and references

Scale Detection Coverage Without Adding Analyst Noise

By combining daily threat research, broad attack coverage, and accurate detection logic, ET Pro Ruleset helps security teams focus on malicious behavior that matters—so existing IDS, IPS, and NGFW investments can work harder.



Conclusion

Proofpoint ET Pro Ruleset helps organizations detect and block advanced threats before they cause extensive breach and data exfiltration.

With daily updates, malware-focused signatures, and coverage across threat categories from command and control to exploit kits, the ruleset improves network security fidelity while reducing false positives.

By unifying ET threat research, global malware intelligence, sandbox analysis, and platform-independent delivery, ET Pro Ruleset helps defenders keep pace with today's fast-changing threat landscape.

Outcome: stronger detection, less noise, and faster confidence in network threat activity.



Learn More

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

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com

Connect with Proofpoint: LinkedIn

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.

proofpoint.