proofpoint.

DATA SHEET

Proofpoint Emerging Threats Intelligence

Enhance your Security Tools with Visibility, Research and Analytics

KEY BENEFITS

- Stay on top of the dynamic threat landscape with daily rule updates
- Block attacks and campaigns before they do harm
- Increase the ROI of your network security with a simple and easy-to-consume malware-focused ruleset
- Adopt a proactive security posture based on real intelligence
- Ensure your prevention devices are performing as they should by looking for indicators of post-compromise activity
- Enrich existing log data with a global perspective on suspicious IP addresses and domains
- Enforce security policies based on threat categories that matter to you

Proofpoint Emerging Threat (ET) Intelligence is the industry's most timely and accurate source of threat intelligence. It combines actionable information, including up-to-the minute IP and domain reputation feeds, with a database of globally observed threats and malware analysis. And it gives your security team the intelligence they need to stop malicious attacks and the context to investigate them.

Today's advanced attacks are launched with increasing frequency by cyber criminals who have many different motives. Some focus on making a profit, and some engage in espionage. The tools they use in these attacks have things in common. But each campaign uses botnets, proxies, attack vectors and command and control systems in a unique way. This makes it nearly impossible to keep pace with changes in the threat landscape.

Our team of dedicated threat researchers and analytics systems at Proofpoint ET Labs do the work—so you don't have to. We provide 100% originally sourced threat intelligence on malware delivery, command and control, botnets, credential phishing, ransomware and coin-mining, attack spread and exploit kits.

Our threat intelligence comes from direct observation that is updated in real time. This provides you with the actionable intelligence to combat today's emerging threats. If you don't have an extensive IT infrastructure, you can complement your security controls with ET Intelligence-agnostic threat feeds.

Actionable threat intelligence

ET Intelligence provides you with actionable threat intelligence. This feeds into your firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS). And it also feeds into log and event management systems (SIEMs) and authentication systems. These dynamic feeds, which have been observed by our ET Labs team, identify IPs and domains involved in suspicious and malicious activity.

Features include:

- Separate lists for IP addresses and domains
- IP and domains classified into over 40 different categories, which are assigned a confidence score

- Scores that indicate recent activity levels and reflect aggressive aging
- Hourly updated lists and scores that are depreciated aggressively
- Multiple formats, including TXT, CSV, JSON, BRO IDS and compressed

Use our global threat database and reputation feeds

It's not enough to just know what types of threats exist. To prevent attacks and reduce risk, you also need to understand the historical context. You need to know where attacks originated, who is behind them, when they launched the attacks and what methods they used and why. And all the elements of your network security infrastructure can work more effectively with timely threat intelligence. This includes firewalls, next-generation firewalls (NGFWs), unified threat management (UTM) appliances, security information and event management (SIEM) platforms, authentication systems and more.

ET Intelligence gives you on-demand access to current and more than eight years of historical metadata on IPs, domains and related threat intelligence. This helps you with incident investigation and threat research.

You can use the ET Intelligence Global Threat Database to:

- Access current and historic threat intelligence—searchable by IP address, domain, malware MD5, SHA256, ET signature ID and message text
- Use search results to discover related information for pivot and drill-down activities, providing a forensic data trail for faster incident investigation
- Investigate incidents
- Connect specific attack campaigns to billions of IoCs
- Search and view attacks and actors all over the world in real time
- Research malware with views into the network traffic produced when malware executes
- Integrate into SIEM for additional context to investigations

You can use reputation feeds to:

- Block connections to and from high-risk IP addresses in firewalls, NGFWs, IPS/IDS and UTM, making these devices more effective
- Raise challenges for suspicious IP addresses in risk-based authentication systems
- Enrich event and log data in SIEM platforms
- Power your predictive analytic systems
- Locate compromised assets and discover the extent of internal infections

Enhance existing processes, data and tools

ET Intelligence improves your processes, data and tools with timely and accurate threat intelligence. Our fully verified intelligence provides you with deeper context. And it integrates seamlessly with your security tools to enhance your decision making.

Here are some typical use cases:

- **Human analysts:** Analysts can use the ET Intelligence web interface for threat discovery and research based on IoCs they have seen
- **Security enforcement:** A firewall, IDS, proxy or other breach detection system can use ET Intelligence Reputation Lists to incorporate the threats into the system in order to actively block malicious inbound and outbound connections
- **Threat hunting:** Leverage the ET Intelligence Reputation Lists in a SIEM, TIP or incident response platform to uncover malicious activity based on logs (for example, in your SIEM) and events your security appliances or incident response (IR) platforms detect
- **Incidence Response:** With ET Intelligence Reputation Lists, identify threats lurking in your environment and remove potential false positives when correlated with other sources
- **Enriching home-grown solutions:** Leverage the application programming interface (API) of the ET Intelligence web interface to help you enrich your SIEM, TIP and IR platforms with contextual information beyond what reputation lists provide

Today, defenders must guard many fronts. But attackers only need to find a single opening. Current protections may not be enough. When used proactively and with context, actionable threat intelligence can mean the difference between a major breach and a minor intrusion.

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**.