proofpoint.

SOLUTION BRIEF

Proofpoint Active Exploits Protection

Stop Exploits at the First Mile—Before They Execute

Key Benefits

- Deliver best-in-class first-mile exploit protection by identifying and stopping exploit activity at the email front door before payload execution or endpoint compromise.
- Prioritise vulnerabilities based on active exploits observed in the wild.
- Reduce exposure before patches are deployed while protecting against exploit-driven malware and command-and-control activity.
- Accelerate investigations with current and historical threat context and continuously updated detection intelligence.
- Prepare for AI- and agent-driven security workflows.

Overview

The speed and scale of exploitation are increasing. New vulnerabilities are being disclosed at a record volume while attackers are weaponising them faster. Traditional vulnerability management and exposure management solutions often prioritise based on severity scores and theoretical risk, but lack visibility into what adversaries are actively attempting to exploit.

Proofpoint Active Exploits Protection changes that model.

By leveraging first-mile visibility into exploit delivery across email and network traffic, Proofpoint helps organisations identify malicious activity before payload execution. The solution combines real-world exploit intelligence, adversary-aware prioritisation and immediate protection capabilities to help security teams focus on what matters most and reduce exposure more rapidly. The result is a more proactive approach to exploit defence, built around preventing attacks earlier in the attack chain.

The Solution: First-Mile Exploit Intelligence Plus Immediate Protection

Proofpoint Active Exploits Protection transforms real-world exploit intelligence into actionable protection and prioritised response. The solution combines adversary-aware exploit intelligence, email- and network-based threat detection, and operational integrations to help organisations identify and stop exploit activity before execution.

With best-in-class first-mile exploit visibility derived from email—where many modern attacks begin—Proofpoint can identify exploit delivery attempts and real attacker behaviour at the earliest stage of the attack chain before payload execution, endpoint compromise or lateral movement occurs.

By leveraging this unique vulnerability intelligence and broad coverage across network- and exploit-driven threats, Active Exploits Protection helps organisations prioritise vulnerabilities based on active exploitation, reduce exposure during patching windows and accelerate investigations with actionable threat intelligence.

Prioritise Active Exploits Over Theoretical Risk

Focus remediation efforts on vulnerabilities tied to active exploitation, not just high CVSS scores.

Active Exploits Protection correlates exploit intelligence with observed attacker behaviour across global telemetry sources to help organisations quickly identify which vulnerabilities present immediate operational risk.

This adversary-aware approach helps security teams reduce noise, improve prioritisation and focus resources on the exposures most likely to be exploited.

Key capabilities include:

- Prioritise asset patching based on actively exploited CVEs
- Distinguish urgent threats from lower-priority risk
- Guide patch prioritisation with clear, actionable threat context, including real-time IP and domain reputation feeds
- Enhance operational focus by aligning prioritisation with real-world adversary activity

Get Immediate Protection While Patching

Patching takes time. Active Exploits Protection helps organisations reduce exposure during that window by providing continuously updated exploit intelligence and enabling immediate protection across email and network traffic.

It provides timely high-fidelity detection logic for advanced threats, including:

- Malware delivery
- Command-and-control communications
- Exploit kits
- Credential phishing
- Attack spread
- Ransomware, botnets
- Protocol and application anomalies
- Coin-mining
- Distributed denial-of-service attacks (DDoS)
- Supervisory control and data acquisition (SCADA) attacks

Key capabilities include:

- Continuously updated exploit intelligence designed to improve protection earlier in the attack chain
- Network-based detection rules for IDS, IPS, NGFW and related security controls
- High-fidelity signatures for malware callback, droppers, command-and-control, obfuscation, exploit kit-related threats and exfiltration
- Daily rule updates to keep pace with the changing threat landscape
- Coverage across major malware families, attack campaigns and network-based threat vectors
- Support for widely used IDS and IPS formats, including Suricata and Snort-compatible deployments

Enrich Security Tools with Global Threat Intelligence

Active Exploits Protection provides actionable intelligence that integrates with a wide range of security tools, including firewalls, IDS, IPS, NGFW, UTM, SIEM, authentication systems, threat hunting platforms, incident response workflows and custom security tools.

The solution delivers reputation and threat intelligence on suspicious and malicious IP addresses, domains, malware, signatures, campaigns and related attack activity.

Key capabilities include:

- Current and historical threat intelligence for IPs, domains, malware hashes, signatures and message text
- IP and domain reputation feeds organised by threat category and confidence score
- Frequent feed updates with aggressive ageing to reflect current activity
- Searchable global threat database for pivoting, drill-down and investigation
- Multiple feed formats for operational integration, including TXT, CSV, JSON, IDS and compressed formats
- API-based enrichment for SIEM, TIP, incident response and internal tools

Improve Detection Fidelity and Reduce Noise

Active Exploits Protection is built from real-world threat observations, malware analysis, global sensor feedback and dedicated threat research. This enables high-fidelity detection while helping reduce false positives in existing network security tools.

Key capabilities include:

- Research-driven detection content based on observed threats
- Malware sandbox analysis that captures network behaviour after execution
- Global sensor feedback to refine detection accuracy
- Signature descriptions, references and documentation to support analyst workflows
- Category-based policy enforcement aligned to organisational priorities

Scale with AI-Driven Workflows

Active Exploits Protection is designed to support modern, intelligence-driven security operations. Future capabilities are expected to provide access to threat intelligence through MCP and agent-based workflows, enabling API- and AI-driven use cases.

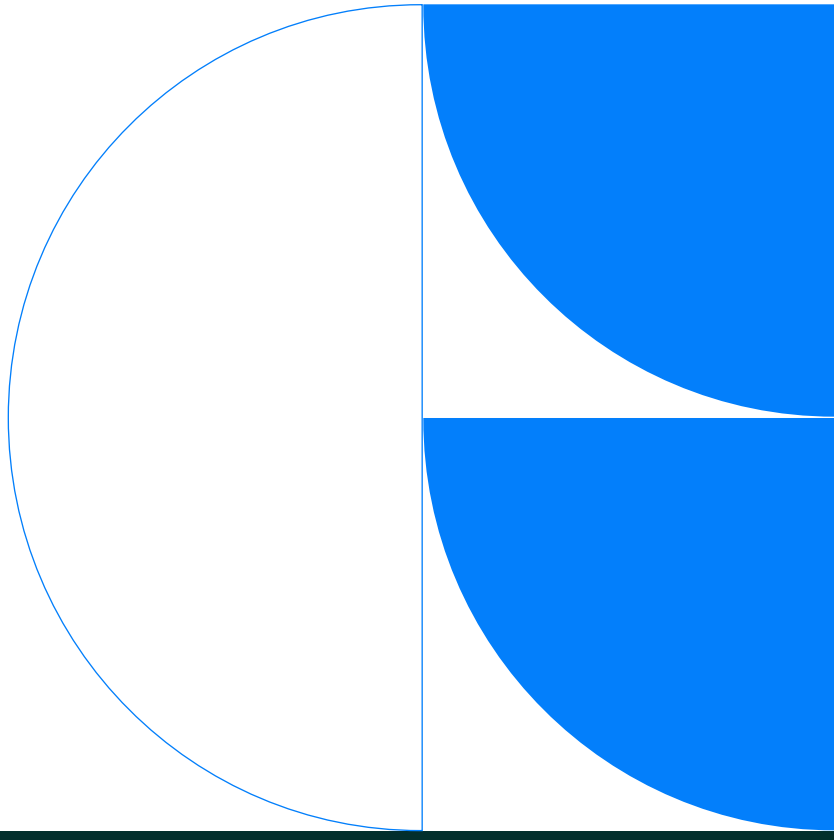
These workflows are intended to help teams embed prioritised threat intelligence directly into automated security operations, accelerate decisions and reduce manual triage.

Summary

Proofpoint Active Exploits Protection helps organisations prevent exploit-driven attacks before compromise by combining best-in-class first-mile exploit visibility derived from email, adversary-aware exploit intelligence and immediate protection capabilities.

Rather than relying solely on vulnerability severity scores or theoretical exposure models, Active Exploits Protection enables security teams to prioritise based on what attackers are actively targeting in the real world.

By unifying prioritisation, protection and investigation, Active Exploits Protection helps security teams focus on what matters, protect immediately and investigate faster.



proofpoint.