Proofpoint ETPro Subscription Overview

Overview

Proofpoint ETPro ruleset subscribers get access to Emerging Threats daily ruleset, along with support for content downloads. The ETPro ruleset is reserved for commercial subscribers and qualified organizations performing short-term evaluations.

Published Content Details

The ETPro Ruleset is a compressed file that subscribers can download with an authorization code. The file includes:

- IDS/IPS rules files
- License files
- IDS/IPS engine configuration files

IDS/IPS rules files

Each rule file, named and organized by a rule category, contains text-based ETPro "signatures" for that category. Each signature is written in syntax designed for either the Suricata or Snort intrusion detection and prevention system (IDS/IPS), depending on which version is downloaded. One signature appears per line, with author and license metadata commented out.

The current ruleset includes more than 60,000 signatures with active and inactive rules. Here's an example of a rule signature:

```
alert tcp $EXTERNAL_NET any --> $HOME_NET 21 (msg:"GPL FTP CWD ..."; flow:to_
server,established; content:"CWD"; nocase; content:"..."; distance:0; pcre:"/^CWD\
s[^\n]*?\.\.\./smi"; reference:bugtraq,9237; classtype:bad-- unknown; sid:2101229; rev:8;)
```

Syntax details are available at:

- Suricata: **https://suricata.readthedocs.io/en/suricata-5.0.0/rules/index.html**
- Snort: **https://www.snort.org/**

All signatures are configured to "alert" upon publish. Some signatures may be commented out upon publish, which prevents them from producing an alert when run on an IDS/IPS platform. For intrusion prevention, use a rule manager to convert this field to "drop."

See *Appendix A: ETPro Category Descriptions* for a list of categorical rules files and their descriptions.

License Files

The text-based ETPro Ruleset license files detail rights reserved within the BSD, GPL Version 2.0 and Emerging Threats licenses.

IDS/IPS Engine configuration files

The IDS/IPS configuration files include:

- Supported Snort output processing
- Alert classification
- Signature reference mapping
- An example snort.conf file
- An example Suricata 1.3 YAML file

Support

ETPro support for OEM subscribers is detailed in *Appendix B: Support*.

Delivery

We normally publish the ETPro ruleset each weekday evening, with emergency rulesets and updates issued at other times as warranted. We publish an average of 20 to 40 new rules, updates and removals each day.

The ruleset is available for download at the following URL:
http: //rules.emergingthreatspro.com/<your auth code here>/<engine version>/etprorules.tar.gz
or
https://rules.emergingthreatspro.com/<your auth code>/<engine version>/etprorules.tar.gz

When using this URL, replace `<your auth code>` with the 16-digit code supplied at purchase and `<engine version>` with the Snort or Suricata engine version you use. Detailed instructions for downloading the ETPro ruleset are available here:
https://rules.emergingthreatspro.com/PRO_download_instructions.html

Content and Coverage

The ETPro Ruleset is designed as a best practice and standalone set of rules. More than 40 categories cover threat characteristics, including:

- Network behaviors
- Informational events
- Exploits
- Vulnerabilities
- Malware command and control
- Phishing
- Unwanted applications
- SCADA network protocols
- Exploit kit activity

Rule category content is covered in *Appendix A: ETPro Category Descriptions*.

Our comprehensive collection of signatures allows operators to select categories appropriate for any deployment scenario.

The ETPro ruleset includes the entire ETOpen ruleset. Signature identifiers (SIDs) of ETOpen signatures are the same as those in the ETPro .tar archive. For those reasons, the operator must not run an ETPro package (set of rules files) at the same time as an ETOpen package.

The ETOpen ruleset represents about 40% of a the full ETPro package of more than 60,000 rules. The ETOpen ruleset relies on contributions from security professionals around the world. This crowdsourced approach makes intelligence an invaluable source of free, community-supported intelligence.

To ensure that the quality of the ETOpen ruleset matches that of ETPro Emerging Threats checks each ETOpen rule before publishing it. Maintaining quality standards of the ETOpen ruleset allows Emerging Threats customers—along with the wider cybersecurity community—to benefit from a collective intelligence that provides a global view of threat conditions.

While the ETOpen ruleset is invaluable, it differs from ETPro rules in a few critical ways.

ETOpen: a solid foundation of collective threat intelligence

ETOpen is collective intelligence vetted and organized into IDS/IPS rules by the Emerging Threats research team.

Rule submissions come from all over the world. They cover all types of threats, threat conditions, Common vulnerabilities and exposures (CVEs), information events and more. Emerging Threats adds value to this source of information by ensuring that submissions detect what their author intended and that they place a reasonable workload on the detection engine. If both goals are met, the rule is accepted into the ETOpen ruleset SID range of 2000000–2599999.

This system works well. But as a crowdsourced effort, ETOpen has no consistent content or threat focus. Additions are made on a best-effort basis.

ETPro: exclusive rulesets for modern threats

ETPro is different. It is the product of a proprietary process designed to protect against modern malware. Most of the content produced every day by ETPro stems from this process, which includes:

- Collecting millions of malware samples every day
- Separating new unique samples from already-known samples
- Detonating new samples in many different virtual environments to observe network traffic
- Matching the captured network traffic (pcap) against existing Emerging Threats protections
- Creating new protections when network traffic in virtual as gone went undetected
- Quality assurance of new protections on live traffic worldwide to ensure it can be published with confidence the same day

This fast-acting system of collection, analysis, rule creation and publishing is highly effective against modern malware threats. Emerging Threats can detect and protect against malware campaigns that last only hours. Our process allows us to offer protections as dynamic as the today's ever-shifting threat landscape.

ETPro can help detect:

- Exploit kit activity
- Exploit delivery
- Spyware operation and command and control
- Host-based Trojan network activity and command and control
- Remote access Trojans
- Anomalous user agents
- Distributed denial-of-service (DDoS) tools and operation
- Crimeware
- Covert channels

These are the types of tools most actively used by both advanced attackers and cyber criminals. They're also our focus for ETPro. That's because we understand that exploits are often unseen on the network and that most of these tools have an Achilles' heel—their interactive command-and-control component.

This knowledge, combined with a keen understanding and connections to the cyber underground, enables our research team to fingerprint actors, tools and campaigns instead of trying to write a signature for every unknown and known exploit.

To be effective, network-based intrusion-detection signatures require massive sample collection, analysis at large scale and daily updates. Updates that occur only weekly or less often are usually obsolete on arrival.

Emerging Threats does not sell a network security appliance. That means we can efficiently focus our expertise on threats and rule content with a relatively small team. We give modern malware challenges priority, extending and enhancing foundational security offered by ETOpen, General Public License (GPL) rules and Microsoft CVE coverage through the Microsoft Active Protections Program (MAPP).

CVE Coverage

The complete ETPro Ruleset offers over 7,900 rules that reference a CVE. We cover CVEs vulnerability. We cover CVEs in both the ETOpen and ETPro ruleset.

Our focus is on MAPP coverage in the ETPro ruleset though the malware collection, analysis and protection process described in the section ETPro: exclusive rulesets for modern threats.

But we don't ignore CVEs and other coverage types. We cover CVE under the following circumstances:

- No ETOpen submission exists.
- The vulnerability is being exploited in the wild.
- The vulnerable software is widely used and we are able to quickly determine a network exploit vector.
- We get data as part of MAPP.

Still, no organization can cover all vulnerabilities. That's especially true if the exploit is not visible on the network and the vulnerability not known.

Focusing on attackers' strength—their ability to create new exploits for unknown vulnerabilities—is an untenable strategy for even the most promising security technologies. That's why we focus instead on the weaknesses in the intrusion "kill chain," where the attacker's Achilles' heel is exposed—such as command-and-control activity and other behaviors.

Our approach means that we can focus on the most serious threats, not on producing signatures for every obscure application and proof-of-concept exploit.

GPL Signatures

The ETPro ruleset has incorporated the best of the following:

- The original Snort GPL signatures (those prior to VRT, SIDs 3464 and lower)
- The old community ruleset (SIDs 100000000+)
- The ETOpen ruleset

If you prefer the ETOpen ruleset without the Snort GPL and community signatures, use the "open-nogpl rules."

The old GPL rules that we believe are worth maintaining are being migrated to a new SID range, 2100000–21003464. (SID 300 from the GPL set, for instance, will move to 2100300.) The move will allow the ETPro ruleset team to convert to multiple platforms and maintain them with other versions that do not maintain multiple engines—without creating conflicts in the process.

Documentation

ETPro rule subscribers are entitled to documentation content for each rule delivered. Today, this covers the content of each rule in its native IDS engine syntax, along with all available revisions. Currently, only a searchable repository of the ETOpen ruleset is available. This searchable repository is available at: **https://threatintel.proofpoint.com/.**

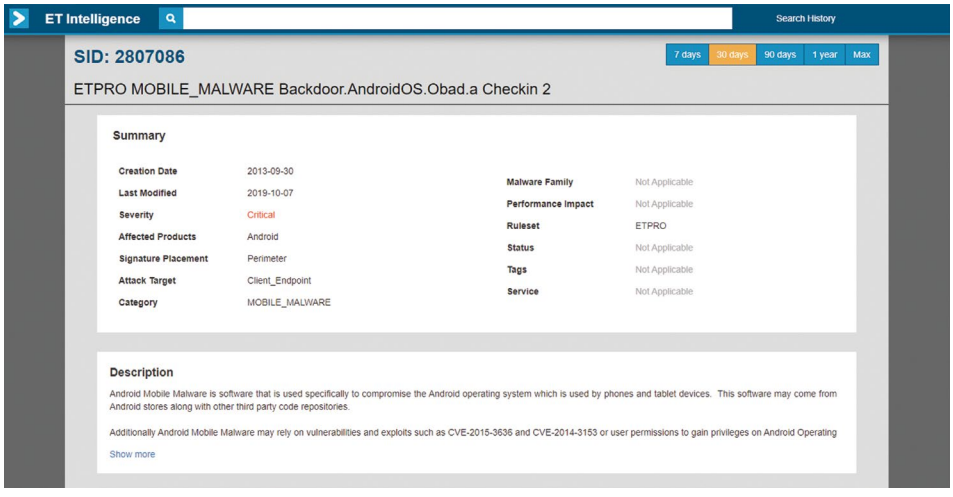

Figure 1: Example documentation.

Note: The ETPro documentation system is being updated and upgraded.

Documentation is provided both within the signatures as metadata and in the SID-Description.json file, which provides the documentation in JSON format. Our current documentation includes the following metadata, and we may add more over time:

- SID
- Message
- Creation Date
- Last Update Date
- Category
- Severity
- Detailed Description
- Affected Products
- Attack Target
- Deployment
- Malware Family
- Threat Actor
- Deprecated-Reason
- Tag
- Reference

A Rule SyntaxA sample of this format is in *Appendix C: Sample Documentation*.

ETPro subscribers can also login to the Threat Portal at **https://threatintel.proofpoint.com** to search for ETPro signatures.

PCAP files and samples are available to ETPro subscribers on a limited basis. You can request them through customer support.

Rule Feedback

You can submit rule feedback through email support (**support@emergingthreats.net**), our feedback portal or our feedback application programming interface (API). We review feedback promptly and incorporate it into the ruleset as needed. Our community's active participation, including your feedback, improves the rulesets and helps ensure that customers receive the highest quality signatures.

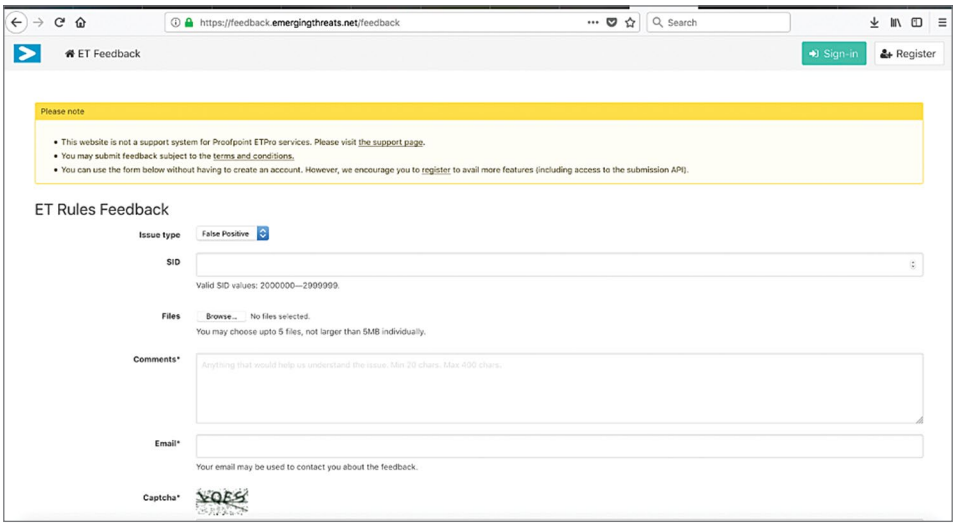

Figure 2: The feedback portal.

Vulnerability Research

Emerging Threats does not provide a vulnerability research service. If we cover a vulnerability, we do so only to digest research quickly and deliver a rule to our customers for the fastest possible protection.

Along with the signatures themselves, this documentation will be the only data delivered to subscribers. We do not provide proof-of-concept code, vulnerability details, vulnerability reports or other vulnerability-related information.

Appendix A: ETPro Category Descriptions

Activex — Attacks and vulnerabilities (such as CVE) related to ActiveX.

Adware-PUP — Identifies signatures that are not explicitly malware but might indicate the presence of software used for ad tracking or other unwanted spyware-related activity. **Note:** This category appears in Suricata 5.0+ rulesets.

Attack Response — Responses that indicate an intrusion, including LMHost file download, certain banners, Metasploit Meterpreter kill command detected and so on. These are designed to catch the results of a successful attack. Evidence such as "id=root" or error messages that indicate a potential compromise.

Botcc (Bot command and control) — These are autogenerated from several sources of known and confirmed active botnet and other command-and-control hosts. Updated daily, primary data source is Shadowserver.org. Bot command-and-control block rules generated from shadowserver.org, SpyEye Tracker, Palevo Tracker and ZeuS Tracker. Port grouped rules offer higher fidelity with destination port modified in rule.

Botcc Portgrouped — Same as **Botcc** but grouped by destination port.

Chat — Indicates traffic related to numerous chat clients, internet relay chat (IRC), and possible check-in activity.

CIArmy — Collective Intelligence-generated IP rules for blocking based upon **www.cinsscore.com**.

Coinmining — Indicates activity that uses computing resources for mining cryptocurrency such as Bitcoin. Most of these signatures detect malware that performs coinmining, but may track legitimate—though possibly unwanted—software that performs such activity. **Note:** This category appears in Suricata 5.0+ rulesets.

Compromised —A list of known compromised hosts, confirmed and updated daily. This set can vary from one hundred to several hundred rules depending on the data sources. The ruleset is a compilation of several private but highly reliable data sources. **Note:** Snort does not handle IP matches well in terms of workloads. If your sensor is already running at full capacity, this set will add significant load. We recommend using just the botcc rules in a high-load situations.

Current Events — Active and short-lived campaigns. The category covers exploit kits and malware that will be aged and removed quickly due to the short-lived nature of the threat. It includes high-profile activity that we don't expect to be active for long, such as fraud campaigns related to natural disasters. These are rules that we either don't intend to keep in the ruleset for long or need to test before they are considered for inclusion. Most often, these will be simple signatures for the Storm binary URL of the day, signatures to catch Class IDs (CLSIDs) of newly found vulnerable apps when we don't have any detail on the exploit.

Decoder-events — Suricata-specific rules for logging normalization events related to decoding.

Deleted — Rules removed from the ruleset.

DNS — Rules for attacks and vulnerabilities related to the domain name system (DNS). The category also includes rules that indicate DNS abuse for activities such as tunneling.

DOS — Denial-of-service attempt detection. This category is intended to catch inbound DoS activity and outbound indications of such activity.

Drop — IP-based rules to block Spamhaus "drop" listed networks. It includes a daily updated list of the Spamhaus DROP (Don't Route or Peer) list, primarily known professional spammers. Details at: **http://www.spamhaus.org**.

Dshield — IP-based rules for Dshield-identified attackers. It includes the DShield's very reliable list of the top attackers, updated daily. More info at **http://www.dshield.org**.

Exploit — Exploits that are not covered in specific service category. It includes rules to detect direct exploits for Windows, Veritas, and so on. Other types of exploits, such SQL injection, have their own category.

Exploit-Kit — Exploit kit signatures used to detect activity related to exploit kits, their infrastructure, and delivery. **Note:** This category appears in Suricata 5.0+ rulesets.

FTP — Rules for attacks, exploits, and vulnerabilities related to file-transfer protocol (FTP). Also includes basic non-malicious FTP activity, such as logins, for logging purposes.

Games — Rules to identify gaming traffic and attacks. World of Warcraft, Starcraft, and other popular online games have signatures here. We don't label these games malicious, but they may not be wanted in all environments.

HTTP-Events — Rules to log HTTP protocol specific events, typically normal operation.

Hunting — These rules may be noisy and match on legitimate traffic or require performance-intensive matching. Bu when hunting for threats within an environment, they often provide indicators that are useful when matched with other signatures.

ICMP — Rules for attacks and vulnerabilities related to Internet Control Message Protocol (ICMP). Also included are rules detecting basic activity of the protocol for logging purposes.

ICMP_info — Rules to log ICMP protocol specific events, typically normal operation.

IMAP — Rules for identifying attacks and vulnerabilities related to the Internet Message Access Protocol (IMAP). Also included are rules detecting basic activity of the protocol for logging purposes.

Inappropriate — Identifies pornography and other activity unsuitable for the workplace. **Note:** These rules tend to rely heavily on regex patterns, which often means high workloads and frequent false positives. Run only if needed.

JA3 — Supported by the Suricata 5.0+ ruleset to fingerprint malicious secure sockets layer (SSL) certificates based on parameters that are in the SSL handshake negotiation by both clients JA3 and by the Servers JA3S. These signatures tend to result in more false positives but can be useful for threat hunting and in malware-detonation environments.

Malware – Malicious software that has clear criminal intent. The category includes malware that is in transit, active, infecting, attacking, updating and other activity we detect on the wire. You should prioritize this ruleset. **Note:** This category was the Trojan category in Snort 2.9 and in Suricata 4.0 and earlier.

Misc. — Miscellaneous rules for rules not covered in other categories.

Mobile Malware — Specific to mobile platforms: malware and spyware related, no clear criminal intent.

Netbios —Identifies attacks, exploits and vulnerabilities related to Netbios. Also includes rules to detect basic activity of the protocol for logging.

P2P — Rules to identify peer-to-peer (P2P) traffic and attacks. Includes torrents, eDonkey, BitTorrent, Gnutella, LimeWire and so on. We don't label these malicious, but they may not be appropriate for all networks and environments.

Phishing –Detects credential-phishing activity, including landing pages that seek credentials and actual credential submissions. **Note:** This category appears in Suricata 5.0+.

Policy – Application identification category. Includes signatures for applications such as Dropbox and Google apps and so on. Also covers off-port protocols and basic data loss prevention (DLP), such as credit card and Social Security numbers. Included in this set are rules for activities often prohibited by company or organizational policy, such as social networks, online shopping and so on.

POP3 — Rules to identify attacks and vulnerabilities related to the Post Office Protocol version 3 (POP3) protocol. Also included are rules detecting basic activity of the protocol for logging.

RBN and RBN malvertisers (Russian Business Network) — IP based rules to identify the Russian Business Network. **Note:** This ruleset has been obseleted and removed. It is no longer used. It is included as a rule file to inform users of its removal.

RPC — Remote procedure call (RPC)-related attacks, vulnerabilities and protocol detection. Also included are rules detecting basic activity of the protocol for logging purposes.

SCADA — Signatures for supervisory control and data acquisition (SCADA) attacks, exploits, vulnerabilities and protocol detection.

SCADA_special — Rules written for Snort Digital Bond-based SCADA preprocessor.

SCAN — Rules to detect reconnaissance and probing such as Nessus, Nikto, port scanning and so on. These rules can provide early warnings of potential malicious activity.

Shellcode – Remote shellcode detection. Remote shellcode is used when an attacker seeks to target a vulnerable process running on another machine on a local network or intranet. If executed, the shellcode can give the attacker access to target machines across the network. Remote shellcodes normally use standard TCP/IP socket connections to give the attacker access to the shell on the target machine. Such shellcode can be categorized based on how this connection is set up. If the shellcode can establish this connection, it is called a "reverse shell" or a connect-back shellcode because it connects back to the attacker's machine.

SMTP — Rules for attacks, exploits and vulnerabilities related SMTP. The category also includes rules to detect basic activity of the protocol for logging.

SMTP-events — Rules that log Simple Network Management Protocol (SMTP) operations.

SNMP — Rules for attacks, exploits and vulnerabilities related to SNMP. Also includes rules detecting basic activity of the protocol for logging.

SQL — Rules for attacks, exploits and vulnerabilities related to Structured Query Language (SQL). Also included are rules detecting basic activity of the protocol for logging.

Stream-events — Rules for matching Transmission Control Protocol (TCP) stream-engine events.

TELNET — Rules for attacks and vulnerabilities related to the Telnet service. Also includes rules detecting basic activity of the protocol for logging.

TFTP — Rules for attacks and vulnerabilities related to the Trivial File Transfer Protocol (TFTP) service. Also includes rules detecting basic activity of the protocol for logging.

TLS-Events — Rules for matching on Transport Layer Security (TLS) events and anomalies.

TOR – IP-based rules for the identification of traffic to and from Tor exit nodes.

Trojan — Malicious software that has clear criminal intent. Rules here detect malicious software that is in transit, active, infecting, attacking, updating and whatever else we can detect on the wire. You should prioritize this ruleset. **Note:** This category is deprecated in the Suricata 5.0 ruleset and is now included in the Malware category.

User Agents — User agent identification and detection.

VOIP — Rules for attacks and vulnerabilities related voice-over-IP (VOIP) environments. Session Initiation Protocol (SIP), h.323, Real-time Transport Protocol (RTP) and so on.

Web Client — Web client-side attacks and vulnerabilities.

Web Server — Rules for attacks and vulnerabilities against web servers.

Web Specific Apps — Rules for specific web applications.

WORM — Traffic that indicates network-based worm activity.

Appendix B: Support

Emerging Threats will provide customer support and rule-maintenance services described in this section at no additional cost to ETPro customers.

Customers are responsible for installing and testing the ETPro ruleset with assistance as requested through the customer support mechanism.

Emerging Threats will exercise commercially reasonable efforts to correct any reproducible malfunction in ETPro that prevents the rules from performing within operating specifications. Customers are responsible for installing and testing of any such fixes with assistance from Emerging Threats.

Customers agree to provide Emerging Threats reasonable access to all necessary personnel to answer questions or resolve reported problems.

Appendix C: Sample Documentation

```
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"ETPRO
MALWARE Observed Malicious SSL Cert (Unk/Xenon CnC)"; flow:from_
server,established; tls_cert_subject; content:"CN=mannolaze.xyz";
nocase; fast_pattern; endswith; tls_cert_issuer; content:"C=US,
O=Let's Encrypt, CN=Let's Encrypt Authority X3"; metadata:
former_category MALWARE; classtype:domain-c2; sid:2840512; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_
Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_
Malicious_Cert, signature_severity Major, created_at 2020_01_20,
performance_impact Low, updated_at 2020_01_20;)
```


```
"2840512": {
 "name": "Observed Malicious SSL Cert (Unk/Xenon CnC)",
 "metadata: former_category": "MALWARE",
 "attack_target": "Client_Endpoint",
 "tag": "SSL_Malicious_Cert",
 "affected_products": "Windows_XP/Vista/7/8/10/Server_32/64_Bit",
 "classtype": "domain-c2",
 "url_reference": "",
 "cve_reference": "",
 "creation_date": "2020-01-20",
 "rev": "2",
 "signature_deployment": "Perimeter",
 "last_modified_date": "2020-01-20",
 "category": "MALWARE",
 "severity": "Major",
 "ruleset": "ETPRO",
 "malware_family": null,
 "type": "SID",
 "performance_impact": "Low",
 "sid": "2840512"
},
```

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.

1210-001-01-02 8/21