# Solution Brief

## Idappcom Easy Rules Manager & Proofpoint ET Pro Rule sets

### Centralised rule-management support for a multi-vendor, multi-layered network security architecture

Idappcom's Easy Rules Manager, ERM, is a powerful and versatile tool that streamlines and automates the process of updating all IDS/IPS devices across the network with the latest security rules, via a centralised management dashboard. Combined with access to the Proofpoint ET Pro rule set the security operations team can use ERM to rapidly update all SNORT or Suricata based devices, to provide enhanced network protection against the latest cyber-threats.

New and increasingly sophisticated attacks are emerging every day, which means that security professionals need to be continuously assessing and updating their security controls just to keep pace with the latest threats. With potentially hundreds of devices deployed to protect critical nodes in the network as part of a defence-in-depth strategy, the overall network security posture can quickly become compromised when relying on conventional tools and methodologies.

The ERM/Proofpoint package is a vendor-neutral tool that allows SecOps to import, group, edit and test the latest SNORT format rule-sets from Proofpoint prior to simultaneous distribution to any SNORT or Suricata based device located anywhere in their network.

The centralised ET Pro rule-database is updated daily covering more than 40 different categories of network behaviours, malware command and control, DoS attacks, botnets, informational events, exploits, vulnerabilities, SCADA network protocols, exploit kit activity, and more.

- Rapid IDS/IPS policy updates
- Multi-vendor support
- Centralised rule management and deployment
- Group/edit and test 3rd party SNORT rules
- 37,000+ rules in 40 categories, updated daily

## Easy Rules Manager (ERM)

### Developed by Security Professionals for Security Professionals

ERM has been developed by Idappcom's security experts based on direct front-line experience managing complex corporate and military-grade networks and working closely with the industry's leading IPS vendors over a continuous 10-year period. Based on this unrivalled industry knowledge ERM has includes a range of features that reflect the fact that all networks are different and that automated vendor updates can often result in unintended consequences; creating additional workloads needed to filter out the high volumes of false-positives.
ERM ensures that Proofpoint and Idappcom, or other vendor's rules, are correctly and appropriately deployed based on the specific network requirements.

- **Organisation and Sorting**
  ERM allows you to group rules in categories that are appropriate to your network infrastructure.
- **Tuning**
  Most IDS/IPS work with text-based rules files and each rule is identified by a Signature ID. ERM cross-references the text files in each rule-set to save time and avoid duplicated effort in deploying the right rule for each sensor.
- **Filtering and Grouping**
  A good rules deployment policy is one where you only deploy those rules that are necessary on your different subnets, to avoid false positives. ERM allows rules to be filtered and grouped according to a range of custom parameters.
- **Multiple copies of Your Rules**
  Once rules have been grouped and uploaded it is very likely that many rules have been duplicated and deployed to more than one subnet. ERM enables changes made in any single rule to be deployed in more than one location to avoid duplications.
- **User Audit**
  ERM provides a full audit trail for all rule-deployments to help in forensic investigations following a security event. By being able to pin-point which rules were deployed and enabled (or not) analysts can quickly determine the root cause of a problem and simplify the remediation decision making process.

## Proofpoint ET Pro Rule Set

## Built on Decades of Threat Intelligence Experience

Proofpoint is the industry's leading, vendor neutral supplier of SNORT and Suricata format security rule-sets. ET Pro Rule set leverages Proofpoint's massive international malware exchange, an automated virtualisation and bare metal sandbox environment, a global sensor network, and over a decade of anti-evasion and threat intelligence experience to develop and maintain its ET Pro rule set.

### Platform Independent

ET Pro Rule set is available in multiple formats for use in a variety of network security applications. The formats include various releases of SNORT and Suricata IDS/IPS platforms. The ET Pro rule set is optimized to make the best use of the feature set and version of each IDS/IPS engine it supports.

### The ET Pro Rule set:

Runs transparently on systems supporting the current and earlier versions of SNORT.

Is the only rule set optimized for the next generation Suricata open source IDS/IPS engine.

## Key Features

- Emphasis is on fingerprinting actual malware / C2 / exploit kits, and in the wild malicious activity missed by traditional prevention methods.
- Support for both SNORT and Suricata IDS/IPS formats.
- Over 37,000 rules in over 40 categories.
- Between 10 to 50+ new rules are released each day.
- Extensive signature descriptions, references, and documentation.
- Very low false positive rating using state-of-the-art malware sandbox and global sensor network feedback loop.
- Includes ET Open. ET Pro rule-sets benefit from the collective intelligence provided by one the largest and most active IDS/IPS rule writing communities. Rule submissions are received from all over the world covering never seen before threats—all tested by the Proofpoint's ET Labs research team to ensure optimum performance and accurate detection.


Idappcom Ltd. | Unit 6 Rural Enterprise Centre | Eco Park Road | Ludlow | Shropshire | SY8 1FF

T. +44 (0) 203) 355 6804 | www.idappcom.com