Advanced Threat Protection

PRODUCT BRIEF

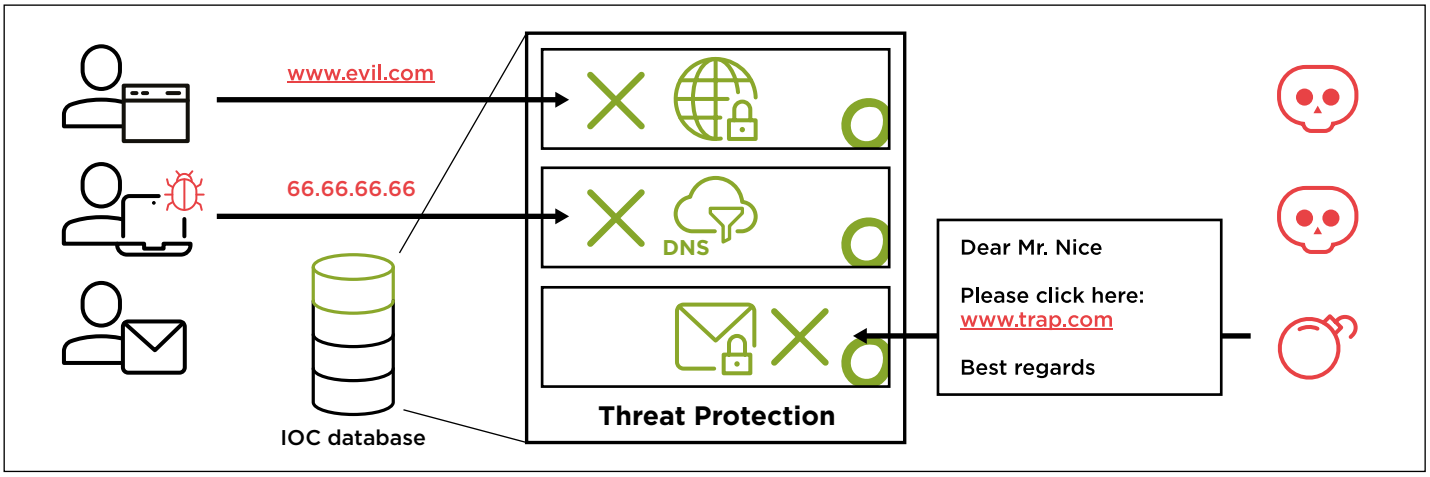
Quickly detecting and blocking access to zero-day malicious entities

Keep pace with attackers

Malware, phishing and ransomware require having rapidly updated protection
Most of the successful cyberattacks start with browsing a compromised website or receiving a malicious email. Quickly changing environments for such distribution of malware, phishing, ransomware and adware/spyware make it indispensable to have your protection against it updated very fast.

High quality threat intelligence feeds to protect from 0-day threats
Threat Protection is the platform at Open Systems to block malicious URLs, domains and IPs. It aggregates different threat intelligence feeds which deliver known indicators of compromise (IOCs) in real time. With Advanced Threat Protection (ATP), your protection level can be enhanced significantly by adding more protection layers and high quality, commercial intelligence feeds for 0-day threats.

Threat Protection – unified threat intelligence for web and email security



For consistent protection, Secure Web Gateway, DNS Filter and Secure Email Gateway use the knowledge from a centralized threat protection platform.

Why do you need Advanced Threat Protection by Open Systems?

Because speed matters

Most phishing and web threats are designed to cause damage in a short time while awareness is low. Therefore, ATP includes commercial 0-day threat intelligence feeds which are designed specifically to catch 0-day threats quickly.

High quality threat intelligence

ATP aggregates third-party databases including commercial threat intelligence feeds which deliver verified malicious URLs, domains, and IP addresses in real time. These feeds combine information from various sources to classify the URLs and domains.

Threat intelligence management

The used threat intelligence feeds are curated by Open Systems engineers and security specialists to always have a powerful and first-class quality set of feeds covering different attack vectors from various threat intelligence vendors.

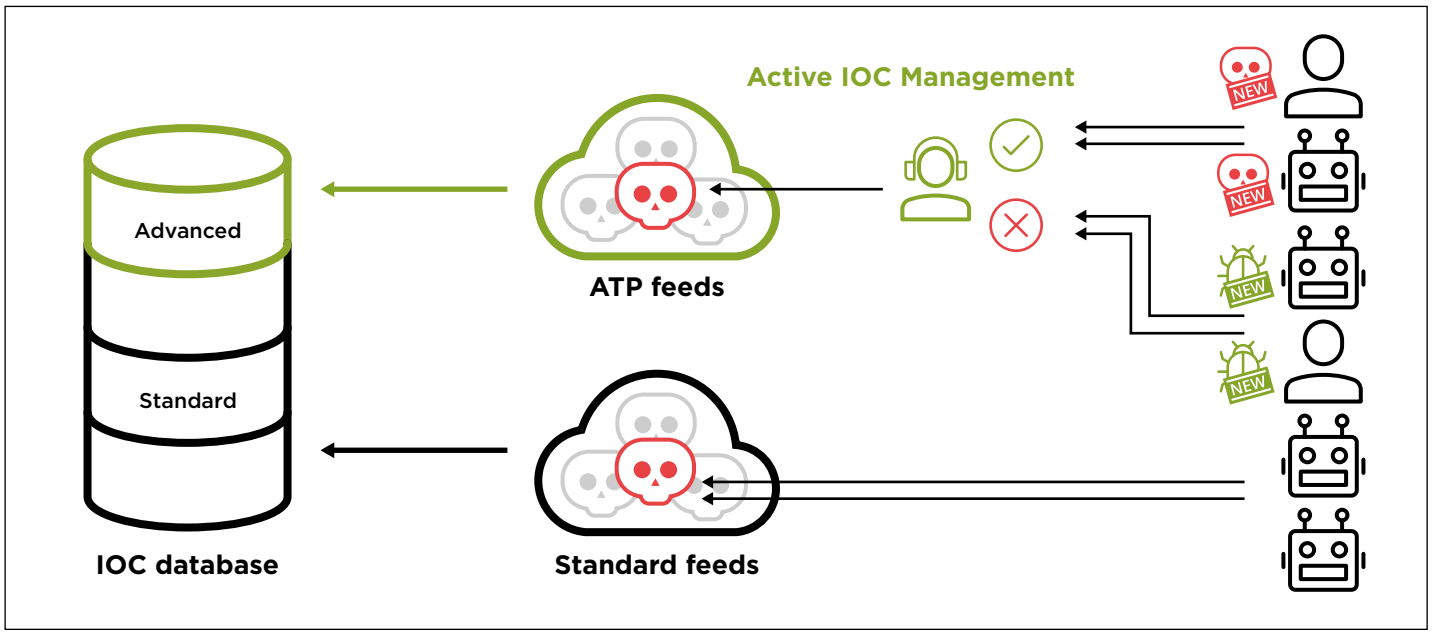
Advanced Threat Protection – How it works

Add commercial threat intelligence for 0-day, high quality protection

Advanced Threat Protection offers additional, commercial 0-day threat intelligence feeds from well-known security solution providers, as an add-on to the basic Threat Protection which is included in our Secure Web Gateway, DNS Filter and Secure Email Gateway. These feeds combine information from various sources to classify the URLs and domains.

- In-house spam traps and honey pots
- Hosting companies and registries
- Law enforcement and internet governing bodies
- Enterprise businesses and internet service providers
- Independent security researchers and volunteers

High quality and 0-hour threat intelligence feeds through active IOC feed management



Fast

- Always the latest and greatest IOC information
- Including 0-day or even 0-hour/0-minute IOCs
- Automatically updated in the central IOC database for real-time protection

Specific

- Granular, specific threat information in the form of URLs instead of IPs/domains
- Diverse sourcing of IOCs: email vendors and MTAs, DNS servers, ISPs, security community etc.

Reliable

- Very low false-positive rate even for quickly changing threats
- Regular, automated and human reviews of IOCs
- Reporting functionality and 24x7 support

opensystems

Open Systems is a secure access service edge (SASE) pioneer that enables organizations to connect to themselves, to the cloud, and to the rest of the world. With cloud-native architecture, secure intelligent edge, hybrid cloud support, 24x7 operations by level-3 engineers, and predictive analytics, the Open Systems SASE delivers a complete solution to network and security.

Learn more at **open-systems.com** |