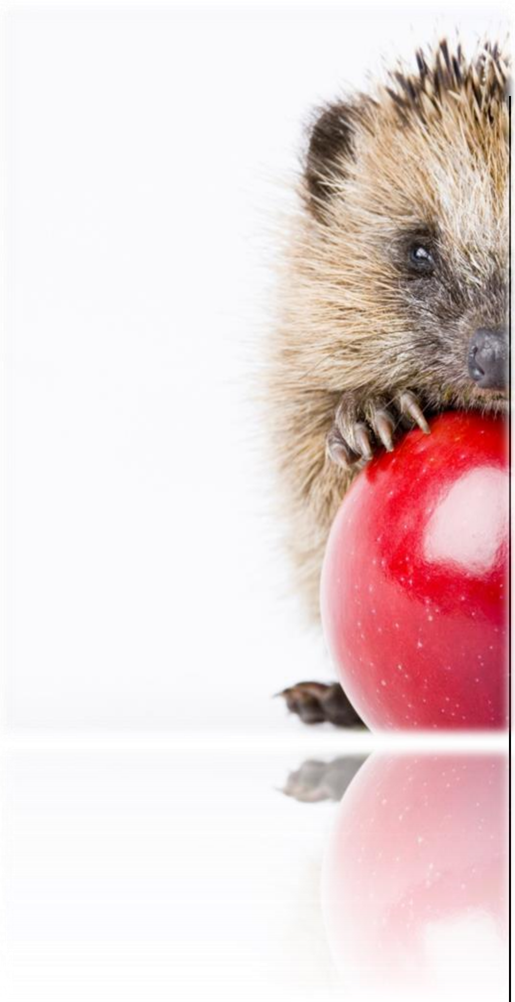


Threat Protection®

Guaranteeing the **availability** of your services.

The availability of online services influences everyday activity, directly impacts the business and forges the image of many companies and organizations. It turns out to be a critical quality metric for any Internet service and content provider, for any hosting or cloud provider. With this in mind, **DDoS attacks** (Distributed Denial of Service), targeting infrastructures, servers and applications, are an ever-growing threat to the legitimate operation of these critical services because of their intensity, frequency and sophistication.

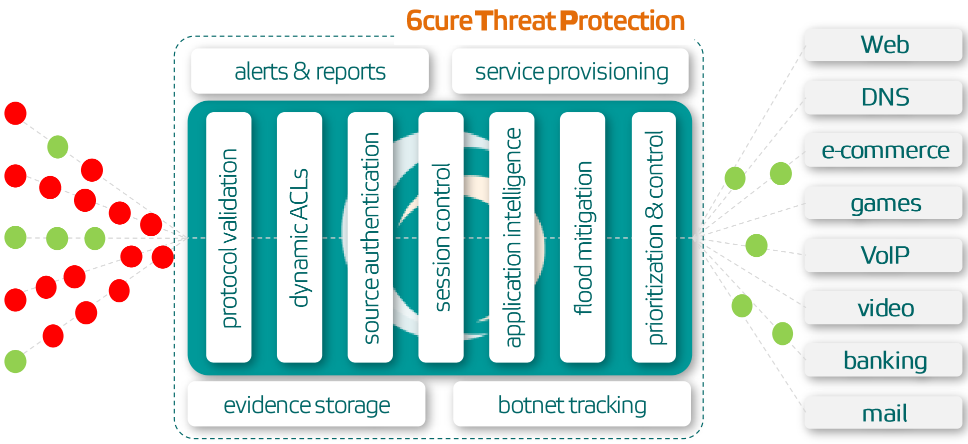
6cure Threat Protection®, the result of more than ten years of R&D in the DDoS mitigation, is the only European solution providing **comprehensive, effective and differentiated protection against DDoS.**

DDoS protection

The *6cure Threat Protection* (6cure TP) solution is able to **eliminate malicious traffic** targeting critical services **in real time** all the while **preserving** the integrity and performance of legitimate flows. 6cure TP uses patented algorithms identifying and filtering even the most complex DDoS attacks, up to application level, and therefore ensuring the normal flow of authorized requests to protected services.

Differentiated multi-service protection

DDoS attacks can simultaneously target a range of services, ranging from equipment and infrastructure services (e.g. routers, DNS), network capacity (bandwidth) and/or application resources (web, commerce and online games, voice, video, messaging).



The detection, analysis and filtering architecture of the 6cure TP solution enables **several levels of protection for each service** requiring specific protection, in a parallel manner, giving it the ability to deal with very large attacks (n x 10Gbps) by applying **differentiated protection policies.**

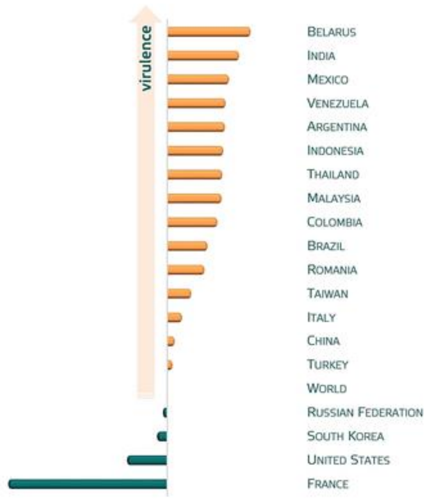
Identification and elimination of malicious flows

6cure TP relies on a set of algorithms to instantly identify and isolate malicious flows targeting a service, and to **preserve the legitimate flows**. Its unique algorithms include the detection of protocol anomalies, behavioral anomalies, and application session anomalies (dynamics and kinetics of individual sessions, intersessional coordination).

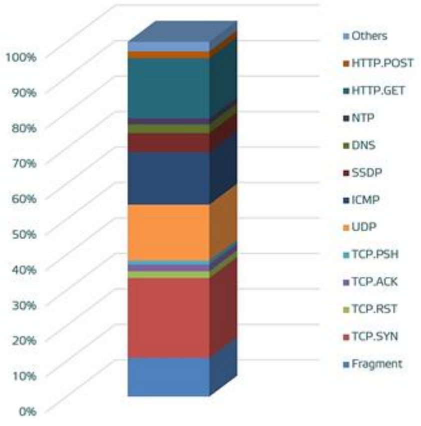
Its ability to establish behavioral profiles allows the solution a continuously adapt without repeated updates of rules or signatures and optimizes its exploitation.

"The 6cure Threat Protection solution provides unrivaled selective traffic-sorting capabilities. Traffic can be cleaned in real-time, with intelligent filtering capabilities that far exceed the capabilities of firewalls and other IPSs, ineffective against the majority of DDoS attacks on our clients and infrastructure. »

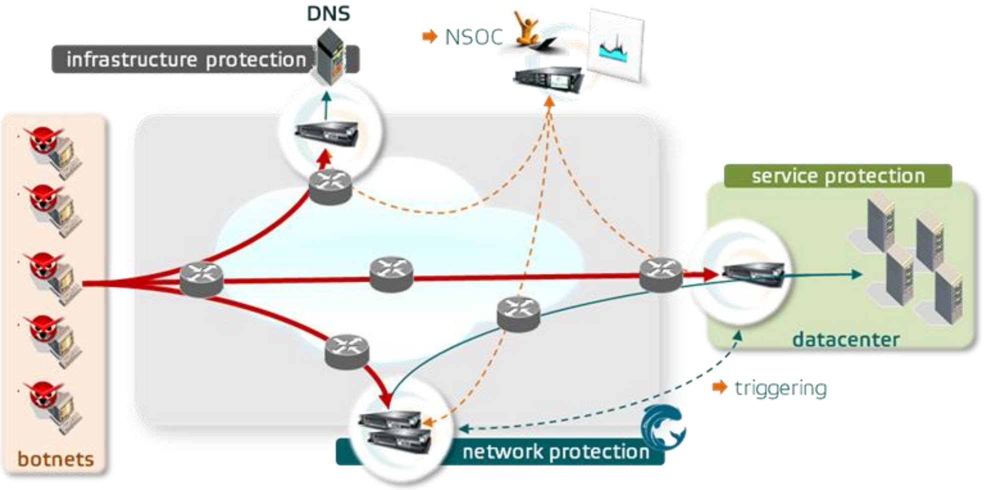
Thierry Baritaud, Security Marketing Director, Orange



Virulence of the origins of attacks filtered by 6cure TP - 2017.



Types of attacks filtered by 6cure TP - 2017.



TP deployment modes.

Diverse implementation possibilities

Inline or off-ramp

6cure TP can be positioned inline in front of a data center to protect customer or critical infrastructure services.

6cure TP can also be deployed within a network infrastructure to attract malicious traffic and re-inject legitimate flows. As such, 6cure TP has capacity for both BGP announcements and use of MPLS/GRE tunnels.

Standalone/farm modes

Each 6cure TP unit has significant filtering capabilities, which allow it to be effective, even in standalone mode. For redundancy and/or increased capacity, 6cure TP units can be stacked in a cluster, allowing them to process of several tens of Gbps of traffic.

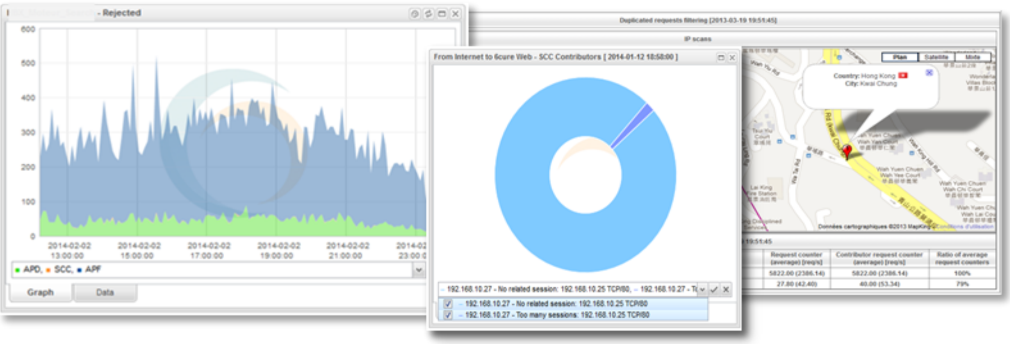
Hybrid protection: Cyblex™ anti-DDoS service platform

The 6cure TP units deployed to protect critical services can immediately alert upstream DDoS protection services, such as those provided by ISPs or the Cyblex™ solution provisioned by 6cure, supervised by a 24/7 security operations center.

The hybrid protection allows to guarantee the availability even when the attack volume exceeds the Internet access link bandwidth, while providing a full visibility of the traffic in real time.

Virtualization

The 6cure TP solution is available as a virtual machine (VM) for different hypervisors (VMWare™, Oracle VirtualBox™, KVM, Xen Server) for fast and controlled deployment in virtual environments.



Duplicated requests filtering [2013-03-19 19:51:45]

From Internet to 6cure Web - SCC Contributors [2014-01-12 18:58:00]

- 192.168.10.27 - No related session: 192.168.10.25 TCP/80, - 192.168.10.27 - T

☑ - 192.168.10.27 - No related session: 192.168.10.25 TCP/80

☑ - 192.168.10.27 - Too many sessions: 192.168.10.25 TCP/80

	Request counter (average) [req/s]	Contributor request counter (average) [req/s]	Ratio of average request counters
	5822.00 (2386.14)	5822.00 (2386.14)	100%
	27.80 (42.40)	40.00 (53.34)	79%

Real time visualization of malicious flows and filtering detail with geolocation.

Effectiveness against polymorphic attacks

6cure TP offers an unrivaled diversity of protections against a wide variety of attacks and malicious phenomena based on several levels of detection and filtering.

- protocol validation: bogon filtering, protocol compliance (malformed packets), protection against TCP/IP attacks (flags) and by fragmentation
- dynamic access control: black/white-lists, spam filtering, filtering and monitoring based on IP geolocation and reputation, filtering unwanted domains (dangerous or illegal content)
- source authentication: IP anti-spoofing, protection against amplification attacks, Web clients validity check, protection against the ripping of contents (Web), SIP sources authentication ...
- session control: protection against "slow" attacks (e.g. Slow Loris, Slow Read), filtering of redundant, orphan or coordinated sessions (identification of botnets) and backscatter traffic, optimized handling of flash crowds
- application intelligence: compliance of application protocols (Web, DNS, voice, video), invalid request filtering, DNS protection (e.g. Poison Cache), Web (e.g. Killer Apache), video/voice (e.g. VoIP message processing attack), level 7 ACLs: DNS domain filtering, LOPPSI, URL filtering…
- flood mitigation: TCP floods (flags), ICMP floods, application floods (e.g. HTTP GET, HTTP POST, DNS A, DNS MX, DNS ANY, SIP call requests), UDP reflection/amplification (DNS, NTP, SSDP, TS3, Memcached ...), "hit & run", "slow drip" attacks, botnet identification, protection against scans (IP, TCP, UDP, DNS sub-domains, URLs…)
- prioritization & control: identification of excessive contributors, detection of behavioral anomalies (massive influx of requests, isolated flows), preservation and protection of legitimate flows and authenticated sources, full traffic captures and/or by service

Reporting & provisioning

The 6cure TP solution comes with a centralized management console which makes it possible to configure all instances deployed on an infrastructure, to receive alerts, produce periodic and real-time reports, and provides the solution's user interfaces.

Alerts & reports

The centralized management console groups together all real-time alerts and periodic reports produced by the 6cure TP units. It makes it possible to quickly visualize and categorize the attacks in progress, to identify the stakeholders of these (sources, targets), to evaluate the effectiveness and possibly to modify the countermeasures applied, and to obtain detailed views (instant zooms, log, filters by source, target, type of attack ...) and to recover the captures executed on the services involved.

Protection provisioning

Operators and service providers have access to provisioning API on the 6cure TP management console, enabling them to declare and activate, in a few seconds, a service for a new customer to be protected as well as obtain the corresponding reports and alerts to integrate them e.g. into their own administration portal for their customers .

Complete offer

6cure proposes its technology on the basis of two models.

The token model allows scaling up the deployment and costs based on the number of protected services and/or the volume of legitimate traffic. Particularly suitable for service providers (hosting, MSSP, etc.), this model enables value propositions to be constructed and offered to their customers.

The integrated model, intended for operators and large companies, provides complete freedom to define and build protections adapted to the operating environment.

For each model, 6cure provides a wide range of professional services: integration, operation, 24/7 support and maintenance, and consulting and expertise.

6cure TP-10000. (Non contractual photo)

Technical specifications

Model	TP-1000	TP-2000	TP-4000	TP-10000	TP-20000	TP-40000
Deployment	Inline, derivation (simulation/protection/automatic)					
Protection	Protocol validation, dynamic ACLs, source authentication, session control, application intelligence, flood mitigation, prioritization & control					
Functions	Identification & tracking of malicious sources (botnets) Traffic capture per service (forensics), configurable retention					
Management	Centralized management console, filters, customizable views, alerting (IDMEF, SNMP, syslog, e-mail, SMS), reporting & provisioning					
Dimensions	4.28 x 48.3 x 73.4 cm (1U)			8.73 x 48.2 x 75.6 cm (2U)		
Power supply	Dual Hot-Plug Redundant Power Supply (AC or DC) 750W					
Environment	5ºC to 40ºC at 5% to 85% RH					
Storage	2x 300GB (system) - 1.2 TB (captures)			2x 200GB SSD (system) - 7.2 TB (captures)		
RAM/CPU	16 GB / 3.2GHz (8 cores)			64 GB / 3.2GHz (16 cores)		
Interfaces	4x1G (management) 2-8x1G (processing)			2x1G 2x10G (management) 2-8x10G (processing)		
Options	SSL Protection, Intelligent Bypass, Intensive Capture, Reference Update Security Service					
Capacity (bps)	up to 1G	2x1G	4x1G	10G	2x10G	4x10G
Flow (pps)	1.3M	2.2M	3.5M	10M	15M	30M
Cluster	✓	✓	✓	✓	✓	✓
Services	50	100	100	250	250	500
Latency	< 1 ms (99.99%)					
Responsiveness	< 1s					

6cure
secure your business

France

Tel. +33 826 387 373
contact@6cure.com

www.6cure.com

6cure Simplified Joint Stock Company with a capital of €114,900 - RCS Caen 520 799 487 - France.