sea

Secure Evolutive Application

borderless security

Relevance

- Everybody is already familiar with dangers of security issues. They are already spoken about too often
- Most modern hosting providers should implement many security features and functions, which are hard to implement and direct
- Often they run into constant issues such as fines, government regulations and other compliance problems

Main Benefits

Providing best-in-class security service means:

- Being a step ahead of your competitors
- Gain additional Revenue Per User because of a useful new service
- Gain additional trust from your subscribers, improve your reputation and prestige
- Prevent issues with clients and regulatory bodies (lawsuits, fines, reputation losses), like:
  - Shutting down a whole datacenter because of massive DDoS attack
  - Blocking a provider’s IP-address range because of some clients become part of a botnet
  - Legal issues due to regulatory requirements violation (those, which a provider is responsible for)

sea

How it works?

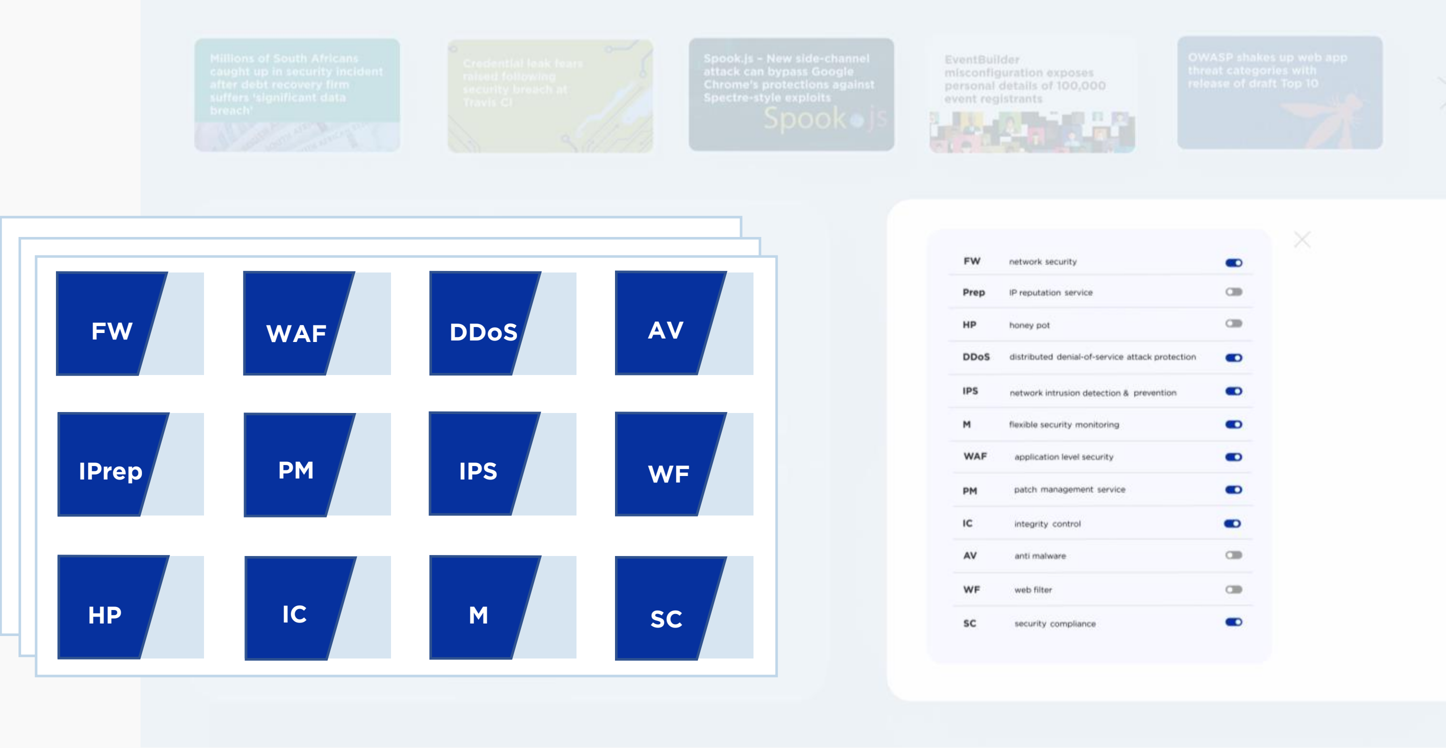
There are number of security modules

FW	FireWall (network security)
WAF	Waf Web application firewall
DDoS	distributed denial-of-service attack protection
AV	anti virus (malware)
IPrep	IP reputation service
PM	patch management service
IPS	network intrusion detection & prevention
WF	web filter
HP	honey pot
IC	integrity control
M	flexible security monitoring
SC	security compliance

sea

How it works?

The client is able to activate/deactivate needed module sets at any time. Thus effectively allowing customers to build optimal vsecurity solutions. Customers pay a subscription fee only for services used and receive comprehensive reports showing module usage and efficiency



Millions of South Africans caught up in security incident after debt recovery firm suffers 'significant data breach'

Credential leak fears raised following security breach at Travis CI

Spook.js – New side-channel attack can bypass Google Chrome's protections against Spectre-style exploits

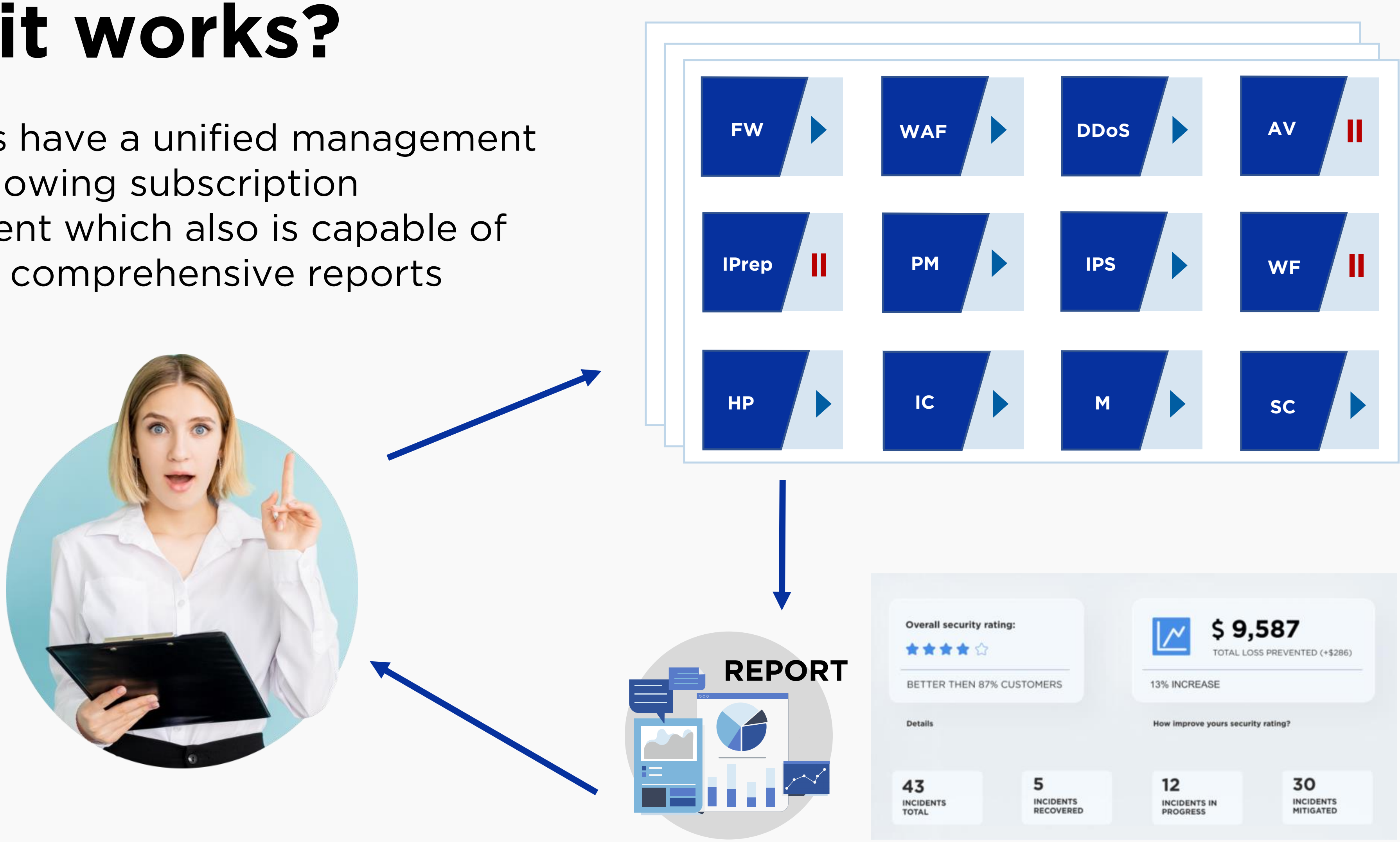
EventBuilder misconfiguration exposes personal details of 100,000 event registrants

OWASP shakes up web app threat categories with release of draft Top 10

FW	network security	●
Prep	IP reputation service	○
HP	honey pot	○
DDoS	distributed denial-of-service attack protection	●
IPS	network intrusion detection & prevention	●
M	flexible security monitoring	●
WAF	application level security	●
PM	patch management service	●
IC	integrity control	●
AV	anti malware	○
WF	web filter	○
SC	security compliance	●

How it works?

Customers have a unified management console allowing subscription management which also is capable of producing comprehensive reports



Overall security rating:

★★★★☆

BETTER THEN 87% CUSTOMERS

$ 9,587

TOTAL LOSS PREVENTED (+$286)

13% INCREASE

Details

How improve yours security rating?

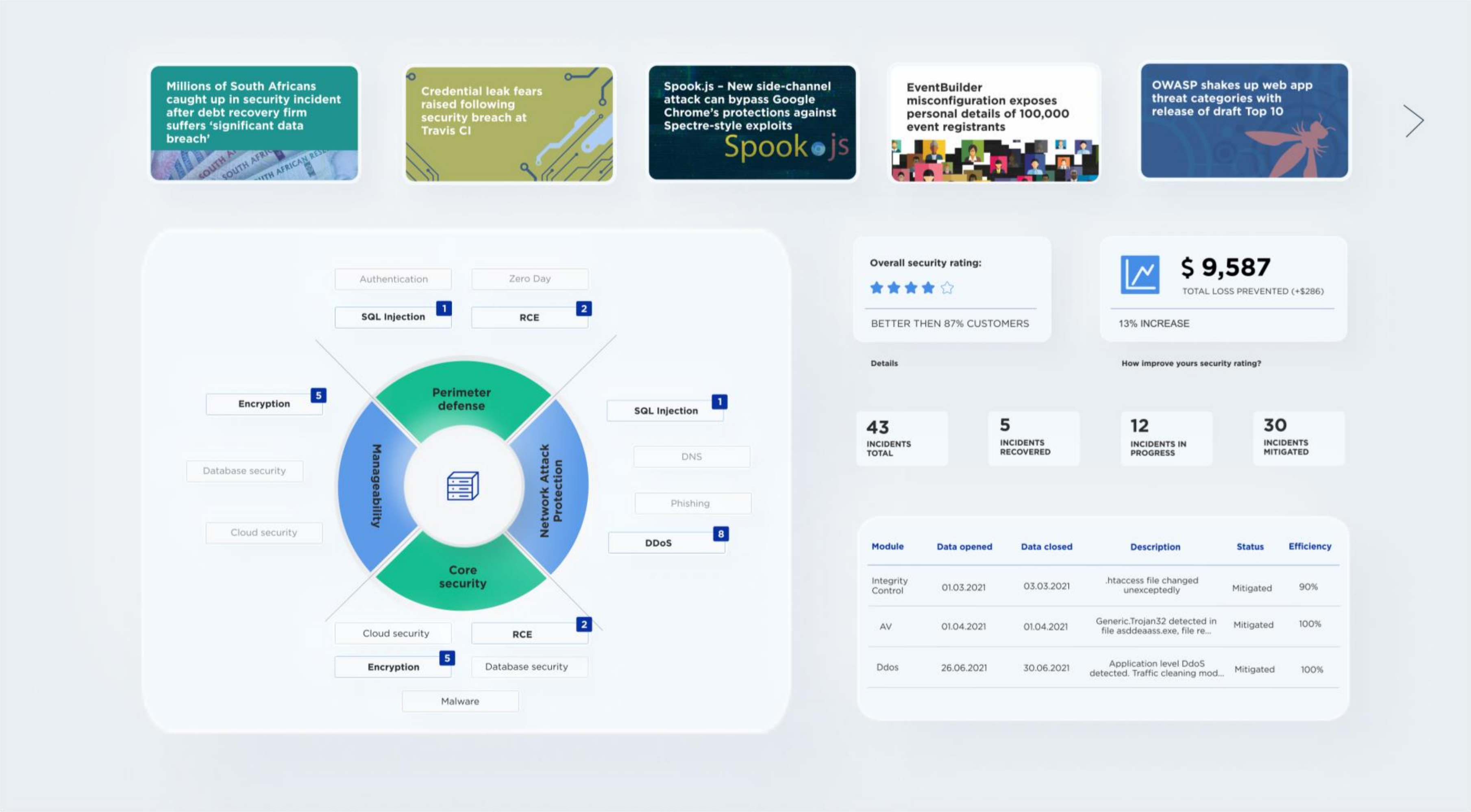
43 INCIDENTS TOTAL

5 INCIDENTS RECOVERED

12 INCIDENTS IN PROGRESS

30 INCIDENTS MITIGATED

Management console screenshot example



Millions of South Africans caught up in security incident after debt recovery firm suffers 'significant data breach'

Credential leak fears raised following security breach at Travis CI

Spook.js – New side-channel attack can bypass Google Chrome's protections against Spectre-style exploits

EventBuilder misconfiguration exposes personal details of 100,000 event registrants

OWASP shakes up web app threat categories with release of draft Top 10

Overall security rating: ★★★★☆

BETTER THEN 87% CUSTOMERS

$ 9,587

TOTAL LOSS PREVENTED (+$286)

13% INCREASE

Details

How improve yours security rating?

43 INCIDENTS TOTAL

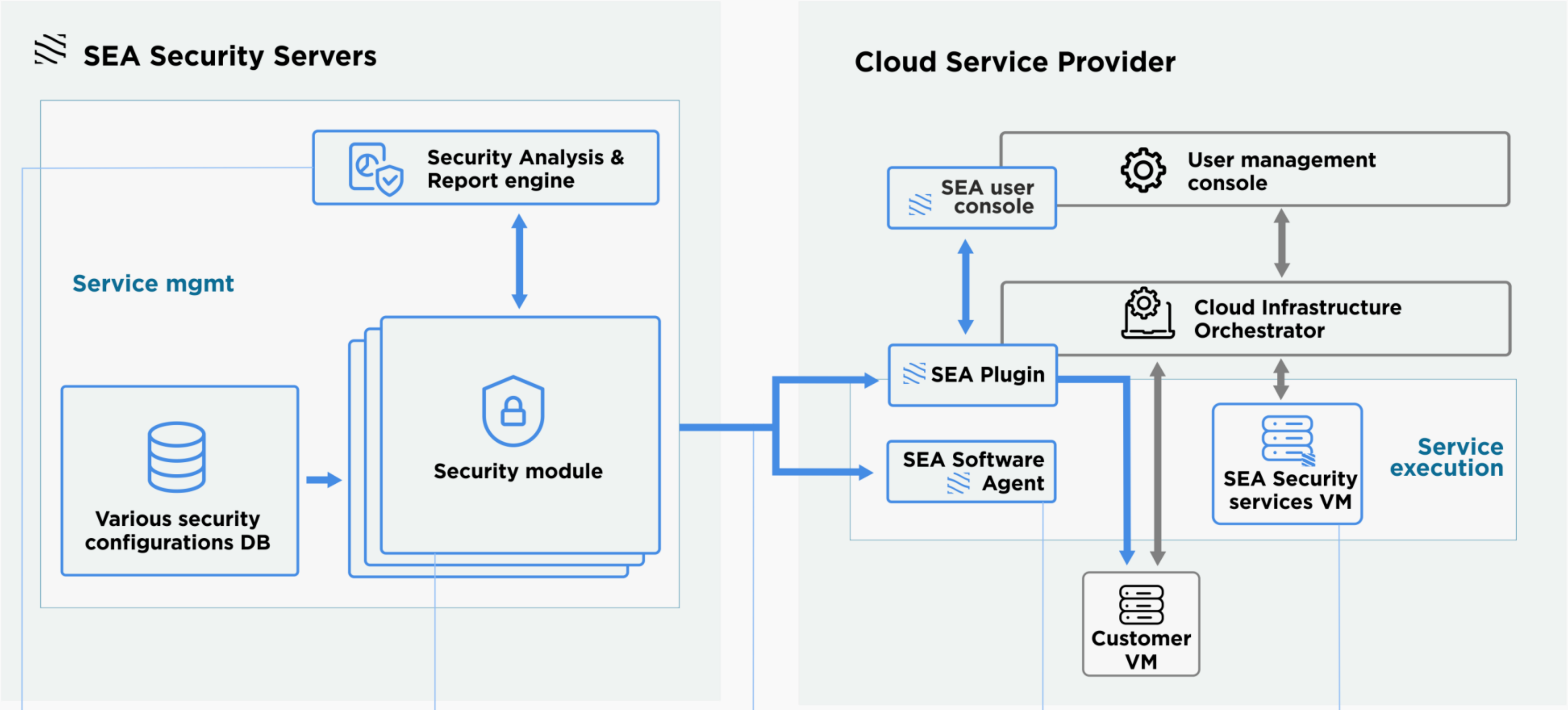
5 INCIDENTS RECOVERED

12 INCIDENTS IN PROGRESS

30 INCIDENTS MITIGATED

Module	Data opened	Data closed	Description	Status	Efficiency
Integrity Control	01.03.2021	03.03.2021	.htaccess file changed unexceptedly	Mitigated	90%
AV	01.04.2021	01.04.2021	Generic.Trojan32 detected in file asddeaass.exe, file re...	Mitigated	100%
Ddos	26.06.2021	30.06.2021	Application level DdoS detected. Traffic cleaning mod...	Mitigated	100%

Architecture



Various on demand reports for CSP & end-user:

- Billing
- SEA security modules usage
- Incident report

- SEA Agents & Plugin configs
- security logs collection

VM Security hardening:

- Remote access protection
- Secure Storage configuration
- Secure boot & vTPM
- FDE (on demand)
- VM guest additions patching
- VM config integrity protection
- SEA Agent automatic installation

Security function enforcement:

- malware protection
- integrity control
- patch mgmt.
- security monitoring
- vulnerabilities check

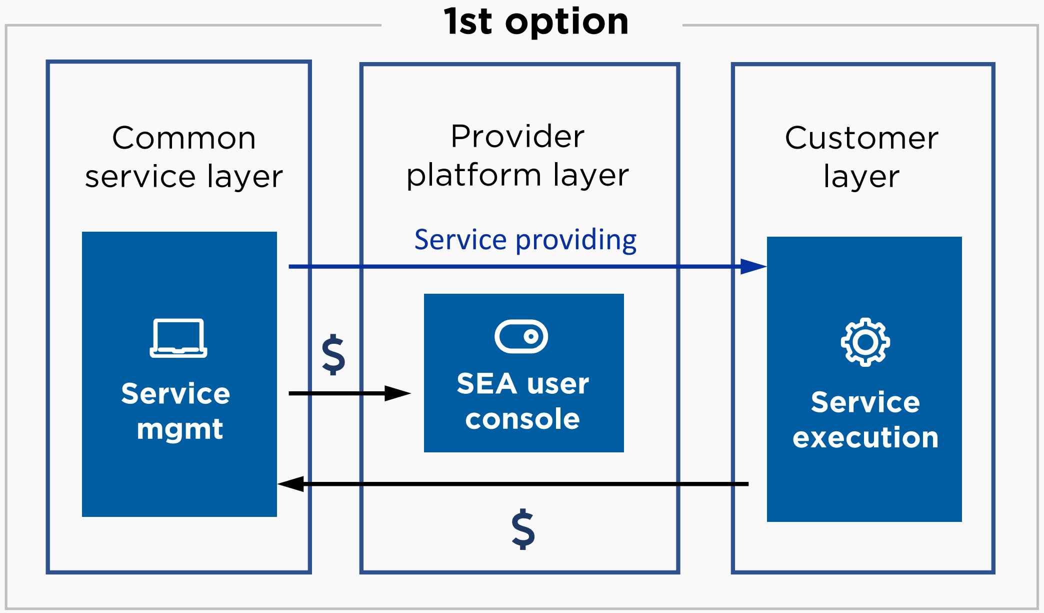
Rule cache & network security services:

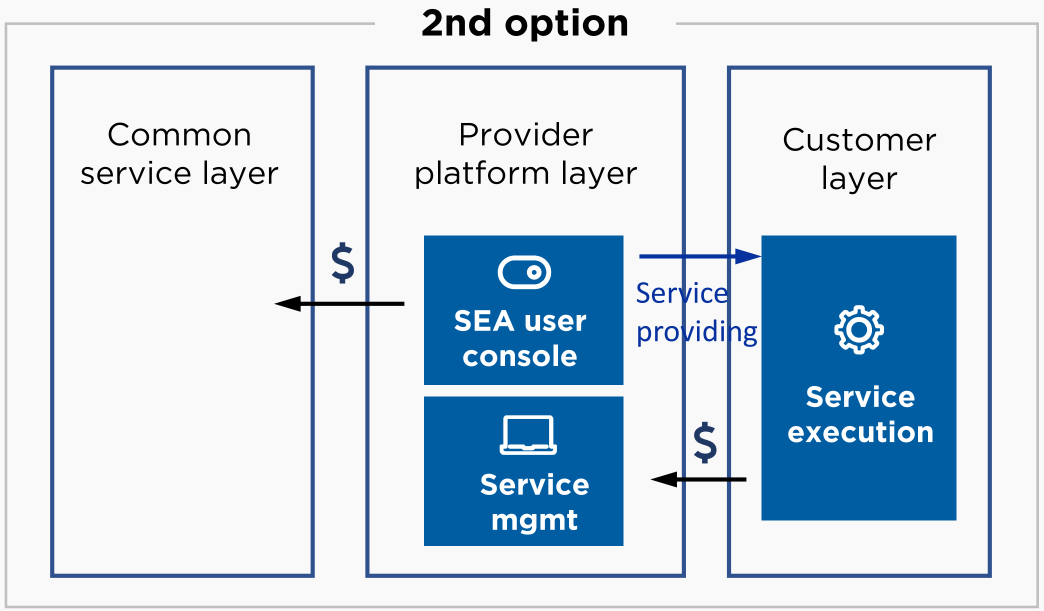
- FW Rules
- WAF Rules
- IP reputation DB cache

Business model

Options:

- The Hosting Provider can receive a subscription fee, paying for common service or the Provider can gain an agent fee from each subscription that is sold (different fee calculation methods are available: time of usage, subscription volume, technical characteristics) - this option can be used as a trial period. The Hosting Provider's role is to just deliver our security services
- The Hosting Provider's role is to maintain all management functions of our security services (including customer's account) and to implement total billing and platform integration. You can install our solution directly into your platform





Advantages

- Billing and customer account integration
- Easy installation, integration and usage
- Centralized multi tenancy support (flexible - fully depend on client’s requirements)
- Full set of security tools (not only malware protection)
- Subscription efficiency evaluation (comprehensive report). Security proof (using BAS techniques)
- Use-as-you-grow + Pay-as-you-go
- Zero impact on performance
- Trial period and flexible business models
- Security assessments for all required regulatory compliances