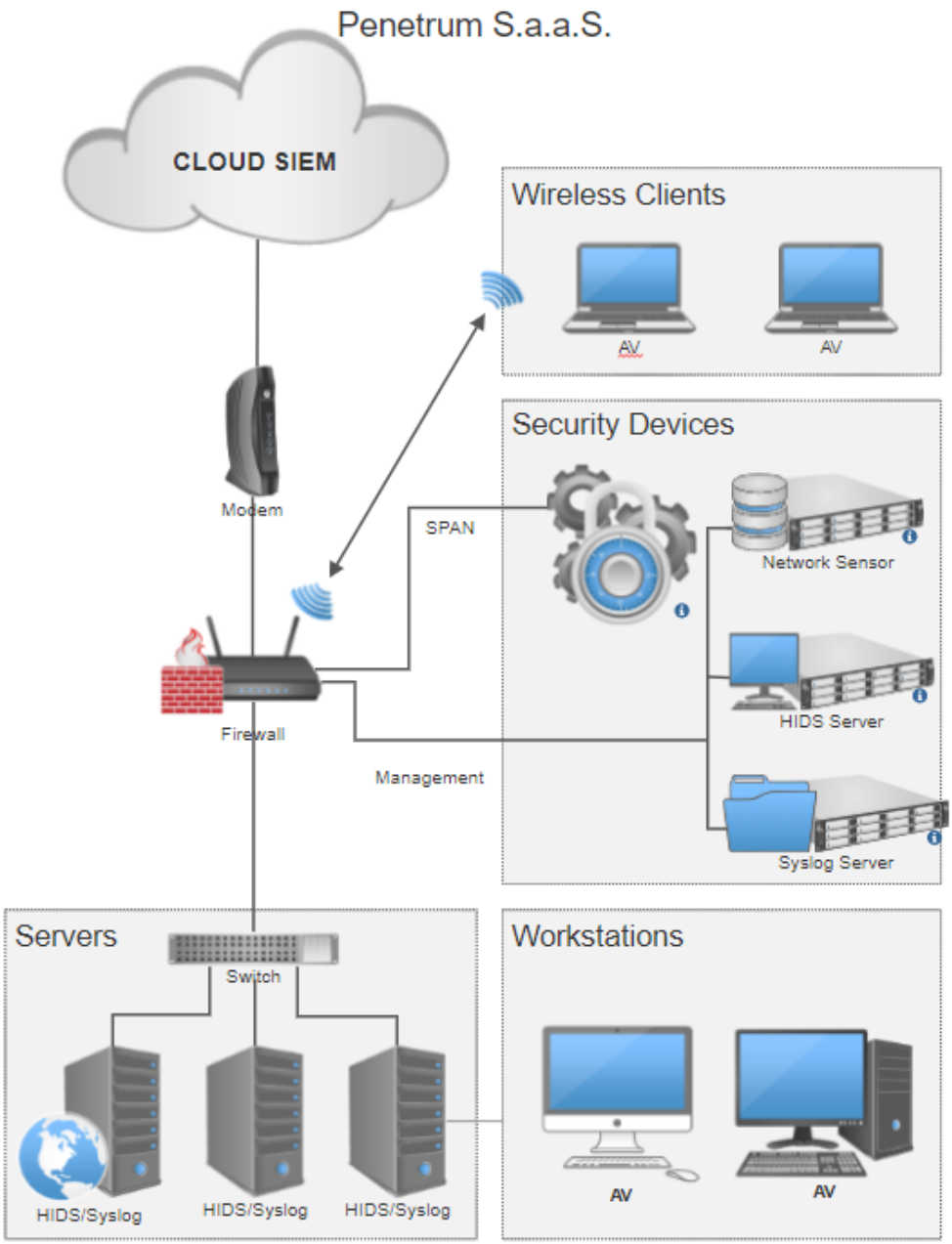
Penetrum LLC.

Penetrum Security as a Service

June 4, 2020

Security as a Service (SaaS) is a business model in which complex security needs may be outsourced to Penetrum while allowing internal IT and security teams to focus on core business competencies. Our security solution eases the financial constraints and burden of inhouse datasecurity while providing a consistent and uniform protection framework as well as security expertise.

Architecture



Core Features

Firewall

- Stateful Packet Inspection
- GeoIP Blocking
- Anti-Spoofing
- Time based rules
- Connection limits
- NAT mapping
- VLAN support (802.1q
- Configurable Static routing
- DHCP
- DNS forwarding

VPN server

- IPsec
- Site to Site
- SSL
- VPN client
- L2tp mobile device VPN
- IPv6 support
- Multi/Split tunnel support
- LDAP capable

Network Sensor

- Full Packet capture
- Protocol Analysis and Metadata
- Signature Based Alerting
- Recursive File Scanning

Host Sensor

- Log based Intrusion Detection
- Rootkit and Malware Detection
- Active Response
- Compliance Auditing
- File Integrity Monitoring
- System Inventory

Core Features

Vulnerability Scanning

- Risk Management
- Asset Discovery
- Network Scanning
- Web Scanning
- Asset Tagging
- Vulnerability Assessment

SIEM

- Multi-stack Monitoring
- Audit logging
- High available, scalable alerting
- Notifications via email, slack, pagerduty or webhooks
- Alerting UI
- Cloud Deployment

Antivirus

- POSIX compliant
- Fast scanning
- Database of over 1 million known bads
- Supports portables executables files

Syslog

- Hardware errors
- Application failures
- Lost contact
- Mis-configuration
- Security auditing

Deployment

On-Premise:

We provide physical and virtual sensors and servers to fit any client or environment. These deployments allow companies to control and maintain systems on their own network. This has the benefit of providing extra services to deter both physical and remote threats.

Cloud:

We can secure AWS, Azure and Google cloud environments. Our external cloud servers provide our clients with easily deployable sensors while maintaining the flexibility to access their security data/devices anytime, anywhere. Although cloud services do not have the benefit of providing on-site security it is a good deployment strategy for those who need to restrict hardware cost or already outsource physical security.

Scaling

Penetrum's SaaS scales with your business needs. Using our various deployment methodologies, you can add or remove both physical and remote sensors, bring on additional cloud services and scale central log management as your business needs change.

Analytics

A common issue when dealing with bulk data analysis is an ability to write and present actionable intelligence derived from the raw information coming from security devices in a readable and well understood manner. Penetrum's analysts present our clients with an understandable threat overview of both active and potential threats.

Our analysts are trained to have:

- Strong understanding of vulnerability management: What are vulnerabilities, how do we find them, and how do we mitigate them?
- Strong understanding of malicious code: Reverse engineering skills; practitioner tactics, techniques and procedures from common
- Motivations
- Strong understanding of basic visualization techniques; especially big data.
- Strong understanding of basic intelligence techniques as applied to cyber.
- Strong understanding of adversary Motivations: cybercrime, cyber hacktivism, cyber war, cyber espionage and the difference between cyber propaganda and cyber terrorism.