IMPERVA – PORTFOLIO SHORT

Imperva is a cybersecurity software and services company that provides protection for enterprise data and application software. The company is headquartered in San Mateo, California. Imperva essentially operates in three areas: Data Security, Application Security and Edge/Network Security and has a Professional Services department. The company's mission is "Protecting Data and all paths to it".

Data Security Portfolio:

The Data Security space is all about solutions that enable companies to secure their data. One of the two main motivators behind Data Security projects is to ensure a company's compliance with regulations. The other is to increase the security of the organization's data by monitoring its use on an ongoing basis and detecting anomalies.

Main use cases:

- Data Classification. Recognizing where data is stored and its relevance. Classification works within data in databases and in other repositories, such as files.

- Data Activity Monitoring (DAM). Generate a full audit of access to any data to ensure regulatory compliance and the ability to investigate suspected data leaks.

- User Right Management. Applying the principle of Least Privilege in relation to data access. Ensuring that everyone has a minimum set of permissions to valuable data.

- Advanced analytics examining the use of data in the organization as follows:

    - Behavioral analysis of data access, that is, learning normal user behavior and detecting anomalies based on default and custom build models.
    - Pattern-based analysis, which is the analysis of data usage against vendor-supplied signatures and detection of malicious behavior.
    - Analysis against custom rules, that is, the ability to apply custom definitions of undesirable behavior and generate incidents if such are observed.

- Compliance. In particular: GDPR, PCI DSS, HIPPA, etc. Regulated data processing like PII requires data access monitoring.

- Data Masking - the secure use of production-like data in development environments without the risk of processing the original, valuable data in unsecured environments.

- Incident Response - supporting data incident response through automation and integration with other security systems (Runbooks, SOAR).

- Supporting automated processes, including support for Data Subject Request Access within the data processed by the organization.

Key features of the solution:

- Integration with databases using an agent or agentless (e.g., native auditing).
- Support for databases in the local Data Center as well as in the cloud (PaaS and IaaS).
- Support for data in databases as well as in files (unstructured data).
- The solution is available as hardware, virtual machines, and a cloud service.

Application Security portfolio:

The Application Security area is dedicated to protecting web applications at various levels. The main and most popular functionality is WAF (Web Application Firewall), which comes in the form of a cloud service as well as software/hardware that the customers can install in their infrastructure. The offering is complemented by RASP (Runtime Application Self-Protection), which offers protection through direct integration with the web application.

Main use cases:

- Protecting the web application from known and unknown attacks that are commonly used in the context of web applications.
- Protecting applications from DoS and DDoS attacks at the application level that aim to overload the application server.
- Content Delivery Network (CDN) features. Accelerate application performance by optimizing site content and caching content at access points around the world.

- Managing traffic generated by bots (good or bad bots), in particular, prevention of:
  - web-scraping - automatic reading of page content like prices, products, etc.
  - spamming – posting of a significant amount of worthless data.
  - carding and card cracking – various abuses related to credit cards.
  - server overload and lack of visibility into customer behavior.
- Protect the identity of the company's customers by detecting and neutralizing attacks aimed at taking over customer accounts (Account Takeover attacks).
- Protect and control the browser environment by managing the code executed on the browser side and reducing the risk of browser-side data interception (like Magecert attacks).
- Protecting APIs from abuse, in particular:
  - API Discovery - scanning (self-learning) APIs.
  - Enforcing protection through the application of a positive security model.
  - Scanning the interfaces themselves to detect their weaknesses.
  - Visibility of sensitive data exposed by APIs.

Key features of the solution:

- Application protection available at all levels: in the cloud, on-prem and on application level.
- The possibility of applying a positive and negative security model.
- For the cloud service, a network of more than 60 access points spread around the world.

- Dynamic use of reputational information collected by Imperva.
- Flexible licensing of all components.
- A solution created with low TCO in mind.
- SOC team working 24/7/365.

Edge/Network Security Portfolio:

The Edge/Network Security area is centered around the issue of DDoS attacks. Attacks can be carried out on different network layers and on different application protocols. Imperva has four main products in its portfolio that protect entire Data Centers (network DDoS protection), individual servers (single IP DDoS protection), web applications (web application DDoS protection) and DNS servers (DNS DDoS protection).

Main use cases:

- Protecting networks from DDoS attacks. These are volumetric attacks, often distributed, aimed at overloading the network infrastructure and consequently blocking access to application servers.
- Protecting web applications from DDoS attacks. We're referring to application attacks, which aim to overload the application server itself by sending an excessive number of application requests. The consequence of a successful attack is blocking access to application servers.

Key features of the solution:

- A network of more than 50 scrubbing centers spread around the world.
- 3 second SLA to neutralize the attack.

- SLA for 100% service availability when the service is properly configured.
- SOC team working 24/7/365.

SOFTPROM — VALUE ADDED IT DISTRIBUTOR

Softprom is a leading Value Added IT Distributor in the CIS and Eastern Europe markets which is trusted by more than 1200 partners. The company was founded in 1999 and today is represented in more than 30 countries.

OUR MISSION

Increase customers effectiveness by providing high-quality IT-solutions and services.