defenselayers

CHALLENGE

Easiness of data exchange and integration among applications in the cloud come at a tremendous cost – increased threat of cybersecurity attacks and data breaches. It is estimated that global costs related to cybercrime will exceed 2 trillions of US Dollars, according to Juniper Research's The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation report. In 2018 serious cases of data hacks were reported. Cybercrime can affect organizations on numerous levels and aspects including data destruction, , data and IP theft, stolen money, productivity and reputation loss, as well as business disruptions. All organizations that make use of cloud applications will have to address evolving cybersecurity challenges including massive data breaches, ransomware attacks targeting the cloud, improper use of AI Technology, attacks on IoT devices. The biggest challenge is a severe cybersecurity talent gap. According to Forbes in 2021 there will be 3.5 Million cybersecurity job posts that will remain unfilled. Shortage of talents suggests higher costs to keep up with cybersecurity standards.

SOLUTION

Taking into account issues of increasing cybersecurity threats and lack of necessary number of cybersecurity and compliance specialists, Defenselayers Plug&Play Cybersecurity&Compliance Platform offers a solution which brings significant level of automation of cybersecurity and compliance processes of software development and maintenance and therefore allows to lower costs related to application security and to shorten time to market. Both are significant to businesses in order to achieve and maintain competitive advantage.

Using application container technology we provide a novel solution which allows to deploy each business application in a specially secured container, assuring safe exploitation of the application itself, as well as protection of data used by it.

Defenselayers Plug&Play Cybersecurity&Compliance Platform is a tool dedicated to cybersecurity management. It also guarantees compliance with main formal regulations (e.g. GDPR, NIS, PCIDSS). The product is a result of many years of experience acquired in the area of cybersecurity and compliance, as well as convergence of different technologies developed over the last years. It is all bundled in one complex solution, which however remains transparent to the customer.

Defenselayers provides a novel solution that addresses the following customer pains/problems:

- Shortage of cybersecurity and compliance specialists
- Once you find necessary specialists they are very expensive to recruit and/or engage
- Customers spend a lot of money/too much money because of necessity to implement cybersecurity best practices and compliance regulations (like GDPR, NIS, PCIDSS, etc) into their software
- Customers are in constant risk of paying huge penalties if they do not comply with certain regulations e.g. penalties for non-compliance with GDPR can reach even tens of millions of Euros
- Customers spend a lot of money on tools which monitor cybersecurity threats in their applications

In order to address the above listed problems Defenselayers delivers cybersecurity and compliance as a service dedicated to applications in a computing cloud. In central Defenselayers infrastructure top-level cybersecurity and compliance specialists (our team members) continuosly monitor the market for new cybersecurity threats and changes in regulations. Defenselayers platform produces a container equipped with cybersecurity and compliance features which customers can use for encapsulating their own applications. Such container connects to Defenselayers' central infrastructure and therefore remains constantly updated while new cybersecurity threats emerge and new changes in regulations occur.

Using Defenselayers' secure container customers acquire the following benefits:

Money savings on:

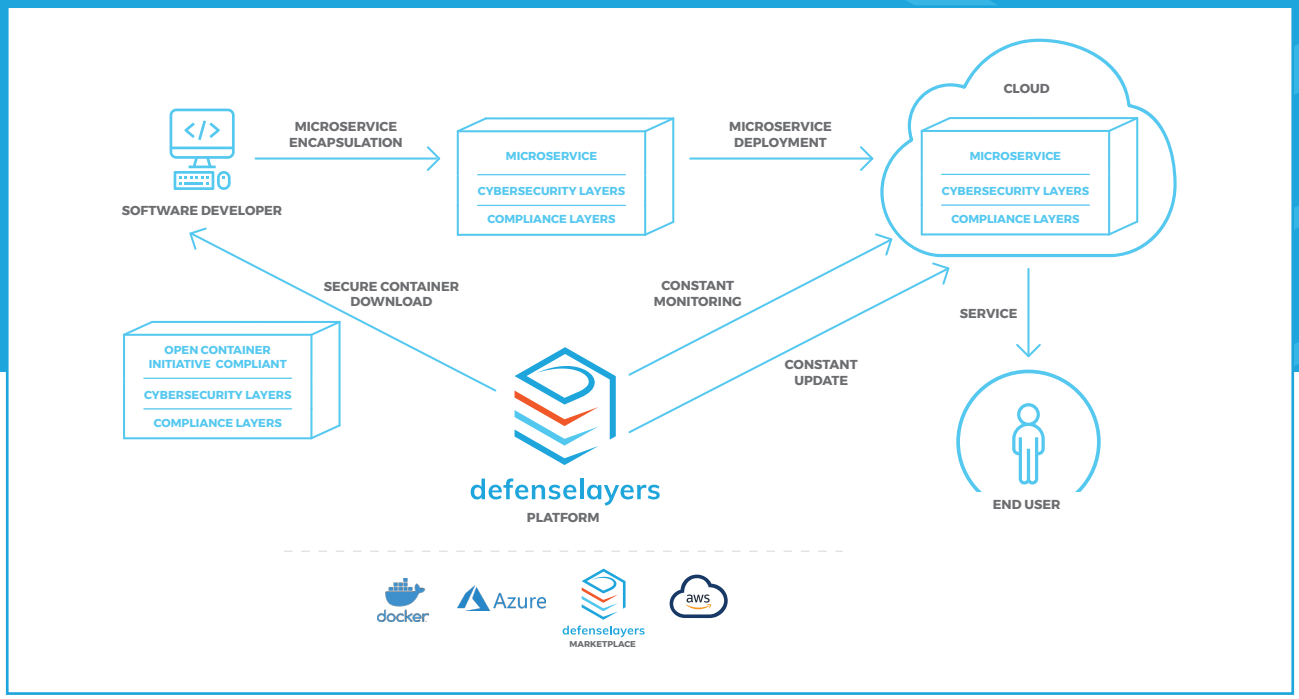
- Cybersecurity resources - these competences are provided by Defenselayers as an electronic service in the Software-as-a-Service model
- Software development costs, as most of cybersecurity and compliance elements will also be provided as a service
- Cybersecurity tools during software development and operations - Defenselayers application container's continuous update eliminates need of additional tools use.
- Potential penalties associated with risk of non-compliance with regulations.

Time necessary for developing new application (time-to-market) will be shorter as cybersecurity and compliance part will be automatically given as a service.

INNOVATION & EXCELLENCE

Containerization these days begins to replace virtualization and, according to both Forrester 451 Research and Gartner, it is currently a leading technology trend. Application container world market is estimated to grow 40% a year.

Defenselayers Plug&Play Cybersecurity&Compliance Platform is the answer to market trends: businesses moving into a cloud, while technology of microservices and containers gain wide acceptance. The product fits within the model of modern methodologies of software development and operation in cloud environment (DevSecOps). Defenselayers Secure Container is compliant with Open Container Initiative Standard (unified application containers standard accepted by all container orchestration tools and public cloud service providers including Azure, AWS, Google, etc) and it is equipped with preinstalled layers responsible for assuring container cybersecurity and compliance. At the same time Defenselayers central infrastructure monitors and keeps these layers constantly updated. This is why we call it out-of-the-box security.



Defenselayers Plug&Play Cybersecurity&Compliance Platform assures:

- Cybersecurity standards & best practices automatically implemented
- Regulations automatically implemented
- Cybersecurity and compliance layers constantly kept updated

Defenselayers reduces complex and expensive cybersecurity services into plug&play, commodity which can be used on a mass scale.

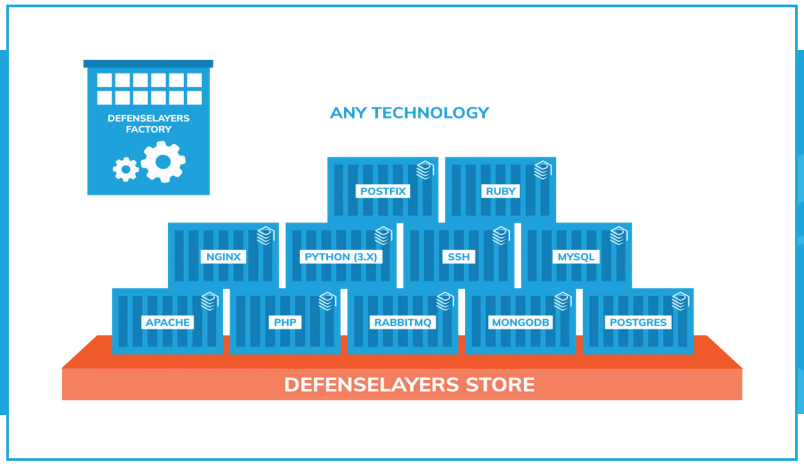
defenselayers

Did you know that 99% of commercial software programs include at least one open-source component? This is what Synopsys found in their latest "2020 OPEN SOURCE SECURITY AND RISK ANALYSIS REPORT" (https://www.synopsys.com/software-integrity/resources/analyst-reports/2020-open-source-security-risk-analysis.html). Moreover what they found is that 75% of audited codebases contain open-source components with known security vulnerabilities, out of which 49% was classified as high-risk.

Apart from reducing software development costs and addressing cybersecurity talent gap issue, Defenselayers solves another crucial problem - the problem of trust. Defenselayers Secure Technology Stack is a set of technologies pre-encapsulated in Defenselayers Secure Containers, which are prepare with particular emphasis to cybersecurity and compliance aspect. In this way organizations can have one place with different technologies that they can trust.

Secure Technology Stack

Defenselayers provides your microservices with out-of-the-box secure containerized technology stack just by one click.



Defenselayers Factory

Defenselayers Factory is an advance automation engine enabling us rapid manufacturing of Defenselayers Secure Containers while reacting to dynamic changes in threat and vulnerability landscapes immediately. Defenselayers Factory are supported with Atlas – our unique vulnerability knowledge database which is supported by multiple external sources such as National Vulnerability Database, GitHub, Alpine Linux, PyPi and many others as well as our own deep experience. Atlas is not just an ordinary database, as thanks to its API our analyst can do best of breed threat detection research. This allows us to react quickly and undertake actions protecting our customers before real attackers can reach their systems.

When it comes to naming the advantages of using Defenselayers Secure Containers over the competitors, we would call the most important two: the containers' preparation process, and the compliance assurance. In a closer look:

The preparation process

One of the main requirements of safe IT operations - and many regulations, by the way - is to embed security from the very first step of the production process. It might be called security-by-design/default in terms of Secure Development Lifecycle or privacy-by-design/default in terms of GDPR but they all mean the same: engaging the security measures as early as possible and composing them into the very foundation of your product. And follow it, Defenselayers Secure Containers have been made safe, out-of-the-box.

This is done by Defenselayers Factory which prepares, selects and assembles only the secure components, configuring them in a safe product in the following sequence:

- Hardening the executables by recompilation of main components, removal of insecure modules and insecure features; this is to make us sure we don't use the poisoned apples for the apple pie
- Removal of insecure components (as well as getting rid of unused ones – in general: the less to maintain, the better); our expertise in this case is to recognize the insecure

- Configuration of the included components with security in mind: shell, network services, daemons etc. must fulfil the strict security requirements (which make part of our unique know-how)
- Safeguarding the access, which includes: removal of default accounts, securing application accounts, hardening the variables' settings, tightening the filesystem's access rights and limiting files' permissions with UMASK
- Vulnerability and malware scanning, which - besides being strongly advised by most of the best practices and strictly required by many regulations – gives us the assurance of being free from built-in flaws
- Building-in the integrity protection mechanism for each binary and configuration set to avoid sneaking-in
- Listing all the container's components within the manifest which makes monitoring easy

This is totally different from competitors who usually give the tools for securing the containers after they are deployed, causing lots of troubles with missing dependencies, lost functionality, conflicting access rights etc.

Compliance assurance

One of the basic needs business explicitly requires from IT is to shorten time-to-market and time-to-money which seems to be crucial source of advantage over competitors.

Surprisingly, the compliance issues appear to be the second most time-consuming task in the IT operations nowadays. This is the result of many regulations aimed in stakeholders' security: GDPR (clients' privacy), SOX and corresponding EU-countries regulations (business security), PCI DSS (payment security), NIS (state security) etc. – they all require IT and its products to conform to strict security rules, in order to sustain the business, protect individual rights and so on.

Todays' market products aimed in container security do not address the compliance issues at all or in a way that shortens time-to-market only seemingly, ignoring the consequences of deploying non-compliant products "temporarily", until the safeguards are built in post-factum.

From the other hand, Defenselayers Secure Containers embrace the idea of security-by-design/default and are built with compliance as *sine qua non*.

Naming few compliance requirements to be met with Defenselayers:

- GDPR-compliance by:
  - embracing privacy-by-design/default with safe components and configurations called by art. 25
  - obligatory testing and vulnerability management with test-before-release procedure (art. 32 1 c-d)
  - incident management enabled with tight integrity control at Defenselayers Factory (art. 33, 34)
- NIS directive by:
  - incident management enabled with tight integrity control at Defenselayers Factory (art. 14)
  - Vulnerability and patch management supported by Safe Containers production cycle (art. 14, 16)
- PCI DSS by:
  - Security and hardening as required in Cardholder Data Environment (CDE) supported by Safe Containers production cycle (req. 3, 4)
  - Integrity control at Defenselayers Factory (req. 6)
  - Vulnerability and malware scanning embedded in the Safe Containers production cycle (req. 5, 6, 11)
  - Effective patching within the initial stage of each container's assembly (req. 11)
  - Enabling only secure encryption protocols/algorithms (req. 3, 4)
  - Embedding only secure system/network/application components (req. 2, 6)
- Financial regulations (SOX and corresponding in EU-countries) by:
  - Utilizing risk assessment for justified yet balanced selection of hardening controls
  - Vulnerability and malware scanning
  - Applying always up-to-date patches
  - Mitigating operating risk by reducing one of the main factors: cybersecurity risk

Defenselayers Secure Containers

For actual list of Defenselayers Secure Containers as well as current plan for new technologies encapsulation, please reffer to www.defenselayers.com/offer.

Scope of Defenselayers Secure Containers Monitoring and Update Service

- Constant monitoring of Defenselayers Secure Containers cybersecurity status
- Providing customers with information about new vulnerabilities
- Providing customers with new versions of Defenselayers Secure Containers free from vulnerabilities

defenselayers