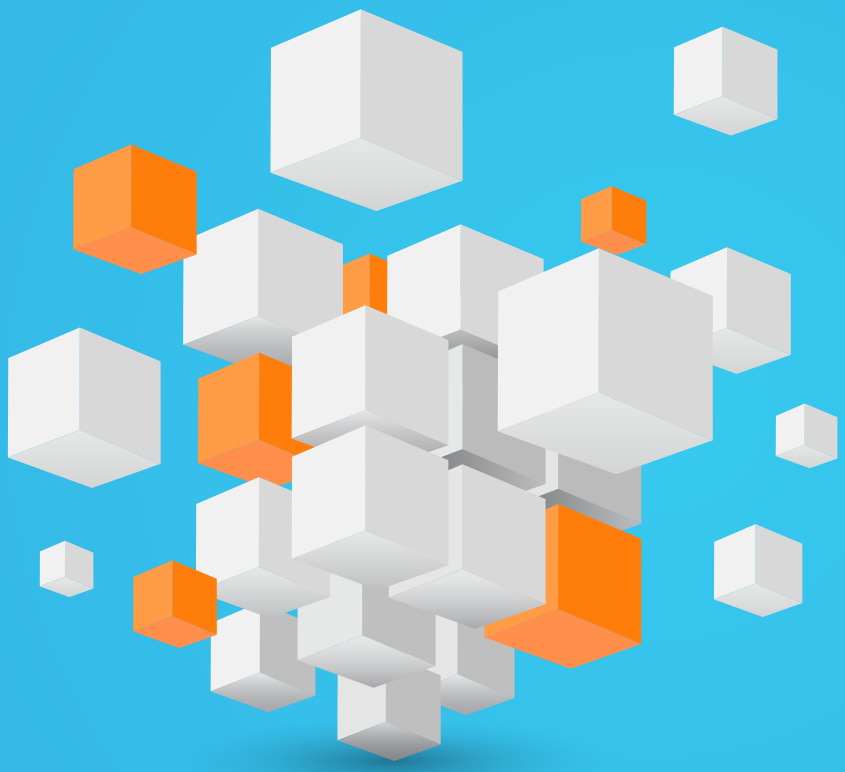


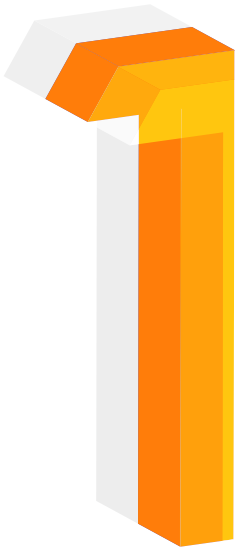
# The SIX PRINCIPLES of a GOOD SERVERLESS SECURITY SOLUTION

Presented by PURESEC

**As pioneers in the world of serverless security, we asked ourselves this important question:**

# What makes *A GOOD* SERVERLESS SECURITY SOLUTION?

We formulated these **six principles of a good serverless security solution** based on decades of experience in the cybersecurity and application security industry and hundreds of hours spent learning about the needs, environments and serverless security challenges of our design partners:



## A good serverless security solution is serverless

The defining features of a serverless architecture are: no server management, flexible scaling, high availability, and no idle capacity. A serverless security solution wouldn't be worth much if it didn't also follow these concepts. It would essentially neuter and negate all of the benefits of the serverless architecture.

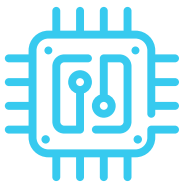
# 2 A good serverless security solution is platform & environment agnostic

Serverless is a software architecture, not a product tied to a specific technology, infrastructure or vendor. A good serverless security solution secures serverless applications without assuming anything about the environment or infrastructure in which they operate.

Serverless is not a synonym for public-cloud FaaS. A good serverless security solution addresses many other serverless scenarios, including:

**Serverless applications deployed on private clouds** (e.g. OpenWhisk, Oracle FN, ..)

**Serverless applications deployed on IoT devices** (e.g. AWS Greengrass)



**Serverless applications used in Edge computing environments** (e.g. AWS Lambda@Edge, Kuhirō)

**Local or offline integration testing for serverless applications,with security already in place**

Serverless functions are event-driven. Each serverless architecture features its own event type, event-data format and other event-related intricacies. Some serverless architectures even offer custom-defined events. A good serverless security solution provides protection without having to rely on any specific protocols or event message formats.

# A good serverless security solution is future-proof

Serverless is a new technology. You don't have to be clairvoyant to predict that hundreds of new attack vectors, vulnerabilities and exploits will be discovered and published in upcoming years. A good serverless security solution doesn't assume anything based on current knowledge. It provides behavioral-based protection that learns and adapts over time.

# A good serverless security solution is high-performing and lightweight

Serverless functions are essentially nanoservices. They are small, lightweight and often execute for only a few milliseconds. A good serverless security solution has minimal impact on performance or size.

For example, any security solution that attempts to send data out of the immediate serverless execution environment is bound to inflict an unacceptable performance penalty. It can't be considered platform agnostic, as it assumes that data can be routed out of the serverless environment and back into it. It won't work effectively with an IoT device running a serverless function or a serverless application deployed in an isolated environment with no access to the Internet.

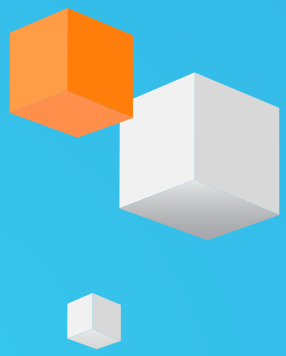
# A good serverless security solution provides high accuracy, without compromising security

Serverless functions are often used for back-end data processing tasks, some of which are business critical. When a failure occurs, there often isn't any instant feedback like the one that exists in a user facing environment, such as a web application. A good serverless security solution provides highly accurate protection that never has a negative security impact.

# A good serverless security solution is low touch and unobtrusive to its users

The key components of a successfully deployed security solution are ease-of-use, minimal maintenance and invisibility to users/consumers. A good serverless security solution never interferes with developer deadlines or forces DevOps / DevSecOps to change the way it likes to operate. It is seamless, providing security with as little disturbance to the regular serverless application lifecycle as possible.

# So what is SSRE? (Serverless Security Runtime Environment)



Just like any other type of software, your serverless functions may be vulnerable to application layer attacks. If your functions contain vulnerabilities, malicious users and hackers will quickly find and exploit them in order to tamper or steal sensitive data, damage your application, deny service from other users and so forth. In order to withstand such attacks, your serverless functions require a solution for protecting them against application layer attacks.

Since no traditional application security products fulfill all six principles mentioned earlier, we defined a brand new category of application security solutions that provide the best, most suitable security protection for serverless architectures. We named it “Serverless Security Runtime Environment,” or SSRE for short.

**SSRE** is a trusted, secure execution environment for serverless functions. It generates a runtime environment that protects serverless functions from external malicious activity while also protecting the applications that contain the serverless function. SSRE provides platform agnostic “secure once, run anywhere” application layer protection that never requires re-applying security when a function moves to a new serverless environment or technology. It offers a high level of visibility into function execution so organizations can perform effective security event analysis. SSRE is lightweight, fast and proportional to the functions it protects. And most importantly, SSRE is serverless.

PureSec is the world’s first and only vendor to provide a full-fledged SSRE solution. PureSec Tesseract fulfills all six principles of a truly effective serverless security solution.

We encourage you, our reader, to evaluate your current security solutions, or any solution you’re considering, to determine if they truly fit serverless architectures and follow these six principles of a good serverless security solution.

PURESEC

Visit us at puresec.io