INTRODUCING THE INDUSTRY'S ONLY CLOUD SECURITY SOLUTION

SPECIFIC TO EACH VERSION OF EACH APPLICATION, NOT TO THREATS

Increasingly, more and more applications and services (aka workloads) are moving from data centers to cloud-based platforms. Microservices are becoming prolific and are the accepted way to build applications. This is forcing organizations to re-architect how they do security. Traditionally, security is part of the network (e.g., firewalls, web application firewalls, intrusion prevention systems). Now, network & operating system security is the responsibility of cloud platforms. The customers' security has to focus on the one thing they own now – the application. This is the area of focus of ShiftLeft.

ShiftLeft's two-pronged approach unifies build-time and runtime security together. With its proprietary technology, ShiftLeft extracts the security relevant aspects from the application every time it changes and generates the application's **Security DNA**, which is used to inform and drive the runtime protection. With ShiftLeft, security is built from the get-go to protect the application from known vulnerabilities, unknown vulnerabilities (that only become known once exploited), and data leakage.

SECURITY DNA

The Security DNA of an application is the sum of everything in its code that impact its security. Some key elements are: the execution space of code (what it does and does not do), the flow and treatment of data, the way the application communicates with the outside world, dependencies used, and vulnerabilities.

BENEFITS

- **Detect threats without impacting continuous delivery:** ShiftLeft protects applications in runtime by relying on the single source of truth - the code itself
- **Protection from key OWASP top-10 risks:** Catch vulnerabilities during **build time,** and protect anything that falls through the cracks automatically at **runtime**
- **Prevent data leaks:** Solve for hard to address scenarios like when a developer unintentionally writes sensitive data to a 3rd party API. Admit it. It happens.
- **Enable safe OSS usage:** Find out if your open source software usage is causing contextual vulnerabilities: Is data being serialized when the library in use is expecting no serialized data?
- **Reduce MTTR:** By identifying the specific line of code that caused the issue in runtime, eliminate costly debugging so the teams can focus on what matters most, building great software.

THE SHIFTLEFT APPROACH

- Extract Security DNA of microservice
- Configure microagent based on Security DNA
- Instrument and protect microservice with microagent.

> "With its DevOps and SecOps friendly solution that blends security knowledge of code from buildtime to runtime data from production, ShiftLeft solves a real problem for customers without slowing them down."
>
> – Florian Leibert, CEO & Cofounder at Mesosphere.

FIGURE 1 | *A Screen From ShiftLeft Dashboard*

FEATURES

- **Create Security DNA for every version of every workload:** Security DNA is all things in your code that impact the security of the code – what the code does, flow and treatment of data, dependencies used, and vulnerabilities. It changes as new versions of code are released, so your code is always protected.
- **Track the spread of sensitive data:** ShiftLeft maps how all sensitive data is flowing in-transit from applications to data sinks, and whether it is being securely handled, down to the line of code.
- **Runtime Microagent:** Security DNA informs the agent of where the vulnerabilities lie and which code paths to monitor every time the code changes - allowing for a high performance solution while eliminating false positives.
- **Multi-tenant SaaS with elegant interface:** Customizable interface designed specifically to enable collaboration between Developers, DevOps, and Security.
- **Seamless integration:** Built for automation, instant out-of-box experience. Infrastructure and OS agnostic. Integration with Continuous Integration tools e.g. Jenkins, Travis CI, Circle CI; popular Java runtimes e.g. Oracle JVM 1.6+, OpenJDK 1.6+.

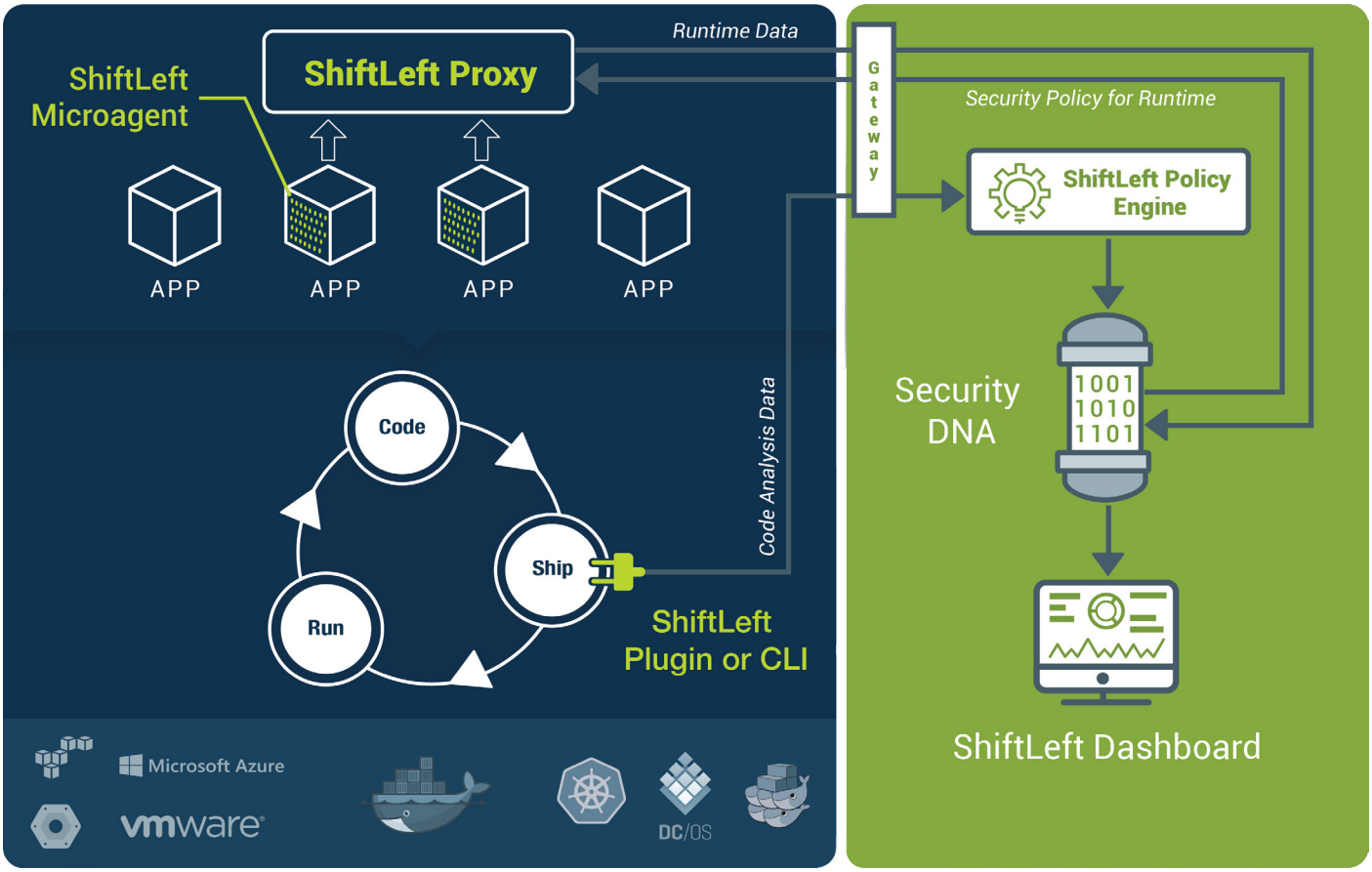

FIGURE 2 | *ShiftLeft Integration into Your Environment*

ShiftLeft has two integration points: At build-time (for ingesting code for analysis) and at runtime (for monitoring runtime behavior).

BUILD-TIME

For build-time integration, a customer downloads the **ShiftLeft plugin for Jenkins** (*.hpi file) , installs it, and enables it per project. The plugin is triggered on a successful completion of the project build. After detecting the build type, the plugin fetches external dependencies associated with the project, composes an archive file, and uploads it to a gateway server in the ShiftLeft cloud along with the organization ID and token metadata. All data payloads from the gateway server to the ShiftLeft core system are encrypted and signed by the organization's private key. Likewise all data stored in the ShiftLeft cloud is encrypted and signed by the organization's key. The encryption key is regularly rotated. When the Jenkins plugin is done sending the archive file to the ShiftLeft gateway server, it triggers the code analysis pipeline for generating the security DNA of that build.

For different CI/CD systems, such as Travis or Circle CI, ShiftLeft CLI can be used to generate the required metadata and upload the package to the ShiftLeft cloud.

RUNTIME

For runtime integration, a customer runs the ShiftLeft Proxy and the ShiftLeft Microagent in their environment.

The **ShiftLeft Microagent** is provided as a JAR file that is attached to the deployment using a single command that includes the JAR path and the ShiftLeft gateway server address where runtime events and alerts are sent. If using a deployment configuration tool such as Chef, Puppet, Ansible, Terraform, etc., simply place the command in the configuration file where the application is being provisioned for deployment. The Microagent monitors the application in runtime and sends events and metrics to the ShiftLeft gateway server via the **ShiftLeft proxy**.

The microagent is inactive until the application starts. Once started, the microagent will establish connectivity with the proxy through a series of ping-pong tests. Once connectivity has been established, the microagent pushes data to the proxy, the proxy aggregates the data and pushes it to the ShiftLeft gateway server that manifests in the ShiftLeft dashboard.

The proxy is a Linux executable that can be installed on most Linux x64-bit distributions. Typically the proxy is installed on an existing jump host. All traffic between microagents and the proxy, and between the proxy and the ShiftLeft gateway server, is encrypted using HTTPS. The maximum number of microagents that can connect to a single proxy is 1,000.

SUPPORTED APPLICATIONS AND PLATFORMS

ShiftLeft is built for production environments supporting the following tools and platforms:

Languages and Runtimes	Java 6+, Oracle JVM 1.6+, OpenJDK 1.6+
Continuous Integration Tools (for build-based integration)	Jenkins 1.625.3+* (with ShiftLeft Plugin), Travis CI or CircleCI (with ShiftLeft CLI)
Infrastructure	Agnostic (Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Digital Ocean, Virtual Machines (VMware ESX, KVM, Xen, Hyper-V), Bare Metal)
Container Engine	Agnostic (Docker, rkt)
Container Orchestration	Agnostic (Docker Swarm, Kubernetes, Mesos/Marathon)

– Recommended Jenkins 2.6+

LET'S GET STARTED

SIGN UP FOR A FREE TRIAL AT: **GO.SHIFTLEFT.IO/SIGN-UP**