IMPERVA®

E-BOOK

Five Security Strategies for DevOps, APIs and Microservices

Content

Secure the Modern Application World

The pressures on IT continue to mount:

- Deliver increased agility so the business can adapt quickly to changes
- Accelerate delivery of applications to the business, customers, and partners
- Boost customer engagement and loyalty with compelling digital experiences
- Gain a sustainable competitive advantage through digital innovation

To meet these challenges, more and more organizations are adopting architectures that use DevOps, containers and microservices as well as automation toolchains and frameworks.

Within this new application landscape, software development has become more complex as the number of touchpoints and integrations increase. This is driving the need for scaled-out, distributed infrastructure. To accelerate delivery of services and products in these distributed architectures, automation is imperative.

At the same time, cybercriminals are increasingly turning their attention to security gaps and vulnerabilities in modern software, both custom and third-party. It's often easier for threat actors to exploit these vulnerabilities than it is to breach hardened components of the infrastructure. Given the speed and volume of development today and the greater complexity of the environment, it's never been more important to secure your applications and data.

Whether your role is CISO, developer, security architect, operations engineer, or a different member of the DevOps team, you need to understand the security implications of today's application landscape. Read on for more insight as well as five strategies for addressing application and data security.

Approximately 60 percent of web applications are "always vulnerable" in the utilities, education, accommodations, retail and manufacturing industries.

"WEB APPLICATIONS SECURITY STATISTICS REPORT, 2016," WHITEHAT SECURITY

Start with DevOps and Get Ready to Shift Left

DevOps Defined

DevOps is a style of rapidly developing and deploying applications through coordinated project management, testing, and development. By tightly integrating and monitoring the development and operations processes, DevOps increases an organization's ability to deliver products and services at a high velocity and with great efficiency.

Why it's Important

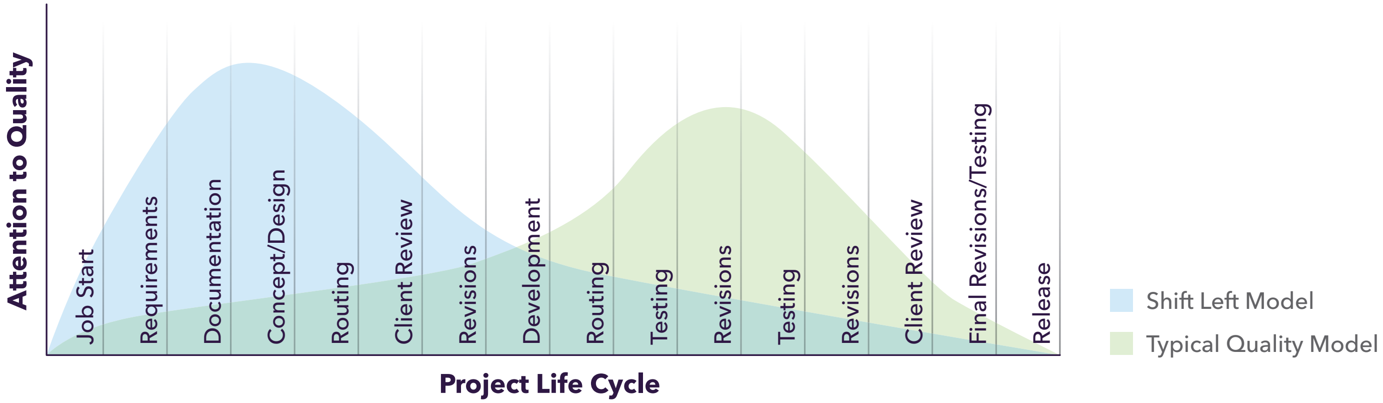
DevOps uses automation and deep, cross-functional integration to dramatically reduce the time to release new applications. It's this speed that enables organizations to get to market faster with applications that deliver value to the business.

What You Need to Know About Shifting Left

The shift-left principle moves tasks that typically come later in a workflow to the left, that is, earlier into the workflow. In software development, the concept of shifting left moves tasks such as testing earlier in the cycle so that these tasks occur in parallel to development activities.

What DevOps and Shift Left Mean for Security

- **The rise of DevSecOps:** The new application landscape is an opportunity to integrate security measures earlier in the development process to improve the security of the code that reaches production. This is called DevSecOps and it's fast becoming the preferred approach to security for modern apps and ecosystems.
- **Continuous security:** The beauty of DevSecOps is that it maintains agility for developers while creating continuous security throughout the development lifecycle, with security professionals integrated as part of the cross-functional team.
- **An improved way to collaborate:** Developers aren't typically security experts and as such need to partner with security practitioners for tools and training that allow them to reliably build and operate secure code and infrastructure. The collaborative DevSecOps culture and tools foster this partnership.



IMPERVA®

Embrace Microservices and Containers

Microservices at a Glance

If you want to develop applications faster, a microservices architecture can help. With microservices, large and complex systems are decoupled into simple, independent projects. Each individual component (a microservice) serves a single purpose or function and operates independently of its peer services and the rest of application.

Why This is Important

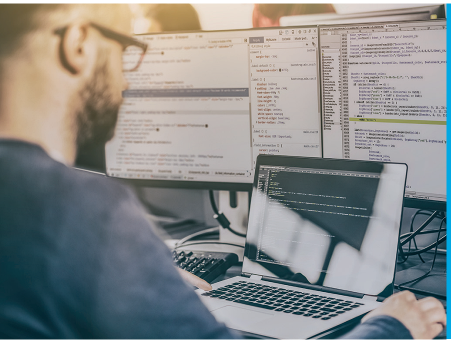
A microservices architecture brings sought-after agility that IT teams need so they can react in days to changes in the business as they occur and not months later.

What You Need to Know About Containers

Software containers accelerate development by enabling applications to be broken down into microservices, which can improve the quality of testing and reduce the complexity of integration and deployment. Containers hold packaged pieces of software that contain all the components (the software, system libraries, and file system) needed to run the service. You can think of containers as application-level virtualization that operates as isolated components on one uniform OS–unlike virtual machines (VMs), in which each application runs on a guest OS and is deployed on top of a hypervisor layer that divides the guest and host OS. The container approach greatly reduces packaging and boot-up time to launch applications.

What Microservices and Containers Mean for Security

- **Same security measures, different environment:** Many of the security solutions—such as web application firewalls (WAFs)—that you currently use for VMs and other application environments still apply to containers. More good news: solutions such as WAFs can protect containers similarly to how they protect VMs.
- **Scalable and dynamic security:** Because containers are ephemeral, being spun up and then decommissioned very rapidly and on demand, you need an application-security solution that can handle these dynamic characteristics using automation.
- **Transitions from VMs to containers:** While securing containers should be similar to securing virtual instance deployments, your application-security solutions should also allow you to easily transition from a virtual environment to one that uses containers, or a combination (i.e., hybrid environment) that leverages both technologies.
- **Granularity:** With containers, you can apply very granular security to the most sensitive microservices running within their own containers without impacting the rest of the services. A WAF with granular and customizable control of each microservice is ideal for this scenario.



CI/CD Defined

Continuous integration (CI) and continuous deployment (CD) are important concepts in today's application development landscape. Continuous integration refers to executing integration testing at every code change. Continuous delivery means deploying every change that passes your tests. Both concepts are often components of an automated software development pipeline.

Understand the Importance of Application Programming Interfaces

APIs at a Glance

Application programming interfaces (APIs) aren't new, but they are increasingly important for exposing specific internal functions of a service or application to the outside world. APIs are essentially plug-and-play services that enable different services, applications, and platforms to communicate with each other in real time. The popularity of microservices architectures is another driver for the increased importance of APIs because all microservices use APIs to communicate with other services and applications.

The API Economy Defined

APIs are essential today for companies looking to monetize data and services to create new revenue streams. Need to provide data to an ecosystem of partners? That's what an API is for. The API economy, as it's being called, refers to using APIs to deliver new digital products and services to the market and enable new business models and channels.

Adding an API Gateway

An API gateway establishes a single entry point for all requests coming from clients, insulating the clients from how an application may be partitioned into microservices, and enabling clients to retrieve data from multiple services with one request.

What APIs Mean for Security

- **A larger attack surface:** Simply put, APIs are an additional attack vector for cybercriminals and can make your microservices and other endpoints vulnerable to the full range of web application attacks. It's possible for attackers to reverse-engineer an API by examining client code or simply monitoring communications.
- **Security for API gateways:** As another potential attack vector, API gateways need layered access control and security defenses. A WAF on the front end helps with access control, bot and DDoS protection, threat detection and filtering. Apart from protecting API gateways from well-known attacks, a WAF can profile API calls and provide user tracking.

Make it All Possible with Public Cloud Computing

While DevOps, microservices, containers, APIs and more can be deployed on-premises, the public cloud is a popular ecosystem for implementing "greenfield" DevOps deployments. Popular public cloud vendors offer a multitude of platform tools catering to lifecycle automation, containers, microservices and API gateways. The public cloud and DevOps are intertwined to deliver a common solution—a scalable, automated environment that allows for greater agility in testing, development, delivery and deployment.

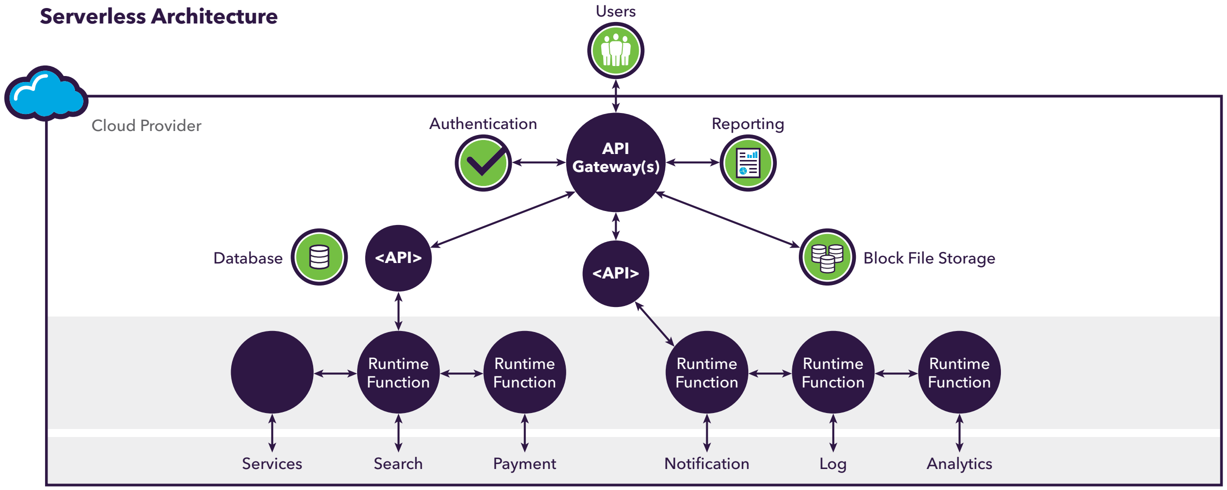
Serverless Computing Defined

Infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) offerings have made the concept of serverless computing possible, where the infrastructure and operating environments necessary for the execution of the application or service are managed by the IaaS/PaaS provider. With serverless computing, DevOps teams don't have to worry about managing the infrastructure the code runs on. The compute resources used to run applications or services are transient, only existing while the application is running. This shifts the focus towards application development rather than network infrastructure management.

What the Public Cloud Means for Security

- **Cloud-ready security solutions:** Your security solutions need to not only secure applications and data in the cloud, they need to be built with the capabilities of the cloud in mind so that they can be integrated and managed as true cloud services.
- **Autoscaling:** Because applications and services running in the cloud can be scaled automatically to support increased usage and performance, your application security needs to autoscale as well to accommodate dynamic changes in cloud resources.
- **Automation:** Security should be a core component in your automated cloud/DevOps environment, with your security solutions supporting automated configuration and deployment through APIs, integrations and templates.
- **Multi-cloud strategy:** Organizations are increasingly taking a multicloud approach to public cloud computing. Choose security solutions that support all the popular public cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Serverless Architecture



Don’t Forget Traditional Applications and Environments

For most organizations, moving to DevOps and modern application architecture such as microservices, public APIs and containers is an evolutionary step. Traditional applications and infrastructure won’t go away in their entirety anytime soon. While some legacy systems might get transitioned to DevOps or retired, some will remain in their current form indefinitely.

In the meantime, organizations are taking what industry analyst Gartner calls a bimodal IT approach, where DevOps (and Agile development) run in parallel with traditional waterfall development. Likewise, microservice and container-based application architectures run in parallel with legacy web and multi-tier applications.

What this Means for Security

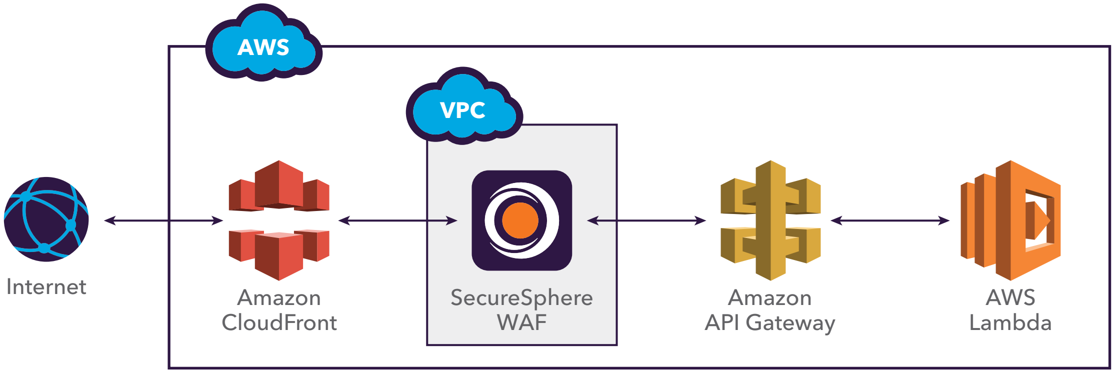
- **Flexible security tools:** Your security solutions must support both legacy applications and ecosystems as well as modern applications. The right solution will make it easier to transition existing applications to new environments without sacrificing security.
- **Same security policies:** With a bimodal approach, you need the ability to apply the same security policies in both the new and legacy architectures so that there is uniformity across modern and traditional applications.
- **Single management interface:** Introducing new application ecosystems should not create new security silos. That’s why your security solutions should be manageable across both traditional and modern applications with one common interface.

5 Security Strategies for the Modern Application World

1 Learn How to Deploy Your Application Measures to New Environments

Mainstay security solutions such as your WAF become even more critical for modern application environments. They become part of the layered security model and complement emerging solutions such as API gateways.

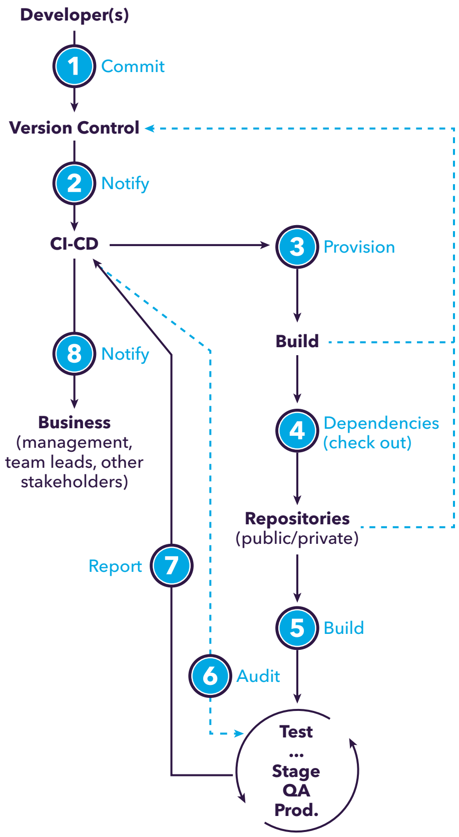
For instance, the right WAF can provide anti-bot and DDoS protection, Layer 7/application-layer protection, and filtering while the API gateway manages the APIs. The sample application shown here is completely serverless and uses AWS services for scaling, automatic provisioning, authorization, logging and so on. The WAF is inspecting the incoming and outgoing HTTP/HTTPS as with any other web application, providing all the usual protections including: profiling, blocking attacks, bot and DDoS protection, preventing account takeover and more.



Your WAF should also help secure applications and data in the new application environment, with automatic deployment any time that new services or containers are provisioned.

2 Implement Continuous Security

CI-CD Process Example



While fundamental security practices and objectives remain the same for new application ecosystems, there are two important differences: the need to 1) shift left, and 2) become continuous. Both of these requirements depend on the integration of security into the DevOps workflow. The result is DevSecOps, an approach where your application security processes are integrated early into the workflow and are components of CI/CD.

The challenge for security teams is to enable your development pipeline to reliably produce secure software without creating roadblocks or speedbumps that would result in bottlenecks on software development and potentially impact time to market. This requires security solutions designed to integrate easily and seamlessly into your DevSecOps workflow.

Continuous, Automated Security

One example of integrating security into your DevOps workflow is to automate the deployment, provisioning and configuration of security solution instances. Regardless of whether you spin up a new server, deploy a new application, or move an existing service from one server to another, the security policies and provisioning layer linked to this service are automatically deployed.

Programmability of your security solution helps it scale automatically and support rapid deployment of security resources as new applications and microservices are deployed. Leveraging cloud-specific templates such as AWS Cloud Formation or Microsoft Azure Resource Manager (ARM) when integrating your security solution can be one way to achieve this type of autoscaling in your cloud environment.

3 Insist on Security Solutions that Continue to Evolve

> *By 2020, more than 90 percent of enterprise DevOps initiatives will have incorporated security controls, up from less than 10 percent in 2015.*
>
> GARTNER, GARTNER SECURITY & RISK MANAGEMENT SUMMIT 2017

It will be difficult to implement the previous strategies and continue to evolve your security stance unless the security solutions you use are also evolving to keep pace with new application environments and tools.

For instance, modern application approaches and infrastructure–including DevOps, APIs, microservices, public cloud, containers and more–require security solutions that are designed to deliver:

- **High availability:** All of your solutions should ensure stable business continuity by allowing your organization to protect sensitive web applications without introducing excessive IT overhead or blocking legitimate web traffic.
- **Integration:** Choose security solutions that support appropriate, automated toolchains and other orchestration techniques used in DevOps, so that as new applications, instances and containers are deployed, security functions are implemented automatically, whenever and wherever they are needed. This typically requires exposure of capabilities via API that support DevOps workflows, cloud deployment, and orchestration.
- **Feature/function parity:** Your solution should be agnostic to whether applications are deployed across public and private cloud, containers or on-premises. This allows you to transition traditional development to agile DevOps without compromising security.
- **Centralized management:** Manage on-premises and cloud gateways from a single management console to consolidate and simplify security for hybrid cloud deployments.

4 Secure Your Data

While most of the focus in DevSecOps is on the application and infrastructure, don't lose sight of the data. Data security becomes even more critical as the applications and infrastructure become more distributed, with complex interdependencies that potentially span services, APIs, containers and clouds.

One way to protect your data in this increasingly complex application ecosystem is with a data-centric audit and protection (DCAP) solution. A DCAP solution helps you protect data in databases, file stores, and big data repositories with real-time monitoring, auditing, and security and rights management.

With a DCAP solution, you can:

- Analyze all database activity in real time. You can monitor all users who access the database, whether through a browser, a mobile app or a desktop application.
- Take action to avoid compromise and data loss, such as blocking access to sensitive data based on security policies.

In 2016, the U.S. experienced a 40 percent increase in data breaches.

"ITRC DATA BREACH REPORT 2016," IDENTITY THEFT RESOURCE CENTER AND CYBERSCOUT, 2017

5 Keep Doing What You’re Doing

Application & Data Security Deployments
The most commonly used technologies for protecting applications and data:

1 Database Firewall

2 Web Application Firewall

3 Data Encryption/Tokenization

While the application development approach and architecture look much different today, the gold-standard security best practices you’ve come to rely on are even more relevant now than before. After all, your attack surface may be larger if you’re exposing APIs to the outside world. Code is likely deployed far more frequently—including the third-party software and services you may have in your stack—which increases your risk and pace of vulnerabilities being introduced.

For all of these reasons, your organization should continue to focus on:

- Reducing your attack surface by hardening your infrastructure and services
- Ensuring confidentiality by encrypting communications and data at rest
- Enforcing granular access control
- Filtering malware and blocking known bad traffic
- Monitoring and detecting anomalous behavior to prevent all types of attacks, including: distributed denial of service (DDoS), abuse of functionality, access violation, exploit and more
- Auditing access and events with logging and analysis

Learn More

Today's modern applications, services and APIs are attractive targets for cybercriminals looking to gain access into your environment. Securing new application ecosystems requires applying the same security best practices as in the past, but using security solutions built to handle today's complex application environment.

Find out how Imperva solutions can integrate into your DevSecOps workflow to protect your applications and data from cyber threats. Learn more:

- **Blog:** "*Moving Securely to the Cloud: WAF Requirements and Deployment Options*"
- **White paper:** "*Securing ECS with SecureSphere*"

About Imperva

Imperva® (NASDAQ:IMPV) is a leading provider of cyber security solutions that protect business-critical data and applications. The company's SecureSphere, CounterBreach, Incapsula and Camouflage product lines enable organizations to discover assets and risks, protect information wherever it lives –in the cloud and on-premises–and comply with regulations. The Imperva Defense Center, a research team comprised of some of the world's leading experts in data and application security, continually enhances Imperva products with up-to-the minute threat intelligence, and publishes reports that provide insight and guidance on the latest threats and how to mitigate them. Imperva is headquartered in Redwood Shores, California. Learn more: www.imperva.com, our blog, on Twitter.

EBook-Application_Evolution_1217-f

imperva.com

IMPERVA®