OPINION

5 ways to enable secure software development in 2023

Security teams have to help developers ensure security software development, but in today's rapidly scaling cloud environments, it's a challenging task.

Melinda Marks, Senior Analyst

Security is on the hook to enable cloud-native development at the same time organizations are under pressure to move their applications to the cloud to increase productivity while managing costs.

Read on to learn about cloud security initiatives designed to drive the efficiency needed to effectively manage security risk and protect applications in the cloud.

1. Developer-focused security tools to shift security left

We've been talking about shifting security left for so long, it has become a security buzz phrase that seems more aspirational than realistic.

Security teams can't force security tools or products onto development teams. Developers don't want to slow down or become security experts. At the same time, security teams can't scale to keep up with the speed and volume of releases. As development scales, there is a higher chance for mistakes, and those mistakes are causing security incidents.

My 2022 research, "Walking the Line: GitOps and Shift Left Security," found organizations have suffered from attacks that take advantage of misconfigurations, software vulnerabilities in proprietary and open source code, and access issues. Most of these are preventable mistakes if the right tools are in place to identify and remediate issues before applications are deployed to the cloud. But it's not just about testing or scanning before deployment; it's also about helping developers efficiently remediate issues found in running applications.

The research showed most organizations (68%) are prioritizing developer-focused security products to shift some responsibilities to developers, while 31% realize its importance. Only 1% didn't prioritize security approaches that shift security left.

To do this successfully, security tools need to work with development workflows so they don't require a security learning curve or switching context away from developer tools. Security must work closely with developers to understand their needs and roll out tools to support them. Security teams need an understanding of development and DevOps, which is a different skill set than traditional application security.

To scale, having developers use security tools isn't enough. The security team should roll out tools to ensure consistency across development teams. Then, they need visibility and control to manage security risk.

2. Addressing software supply chain security

Another key to modern software development security is supporting developer use of existing third-party components and resources when building applications. It saves time, enabling developers to spend their time on their proprietary code to efficiently build applications.

It's not just about securing what's in the application itself, however. It's about what it takes to run the application, including infrastructure, drivers, dependencies, compilers, repositories, OSes and cloud services, as well who has access to these components. With current economic pressures, open source software (OSS) plays a significant role because there are vast libraries of free code developers can use. Research from TechTarget's Enterprise

Strategy Group found most organizations (80%) currently use OSS, with an additional 19% planning to use it in the next year. Most organizations reported that more than half their code consists of OSS, with 49% saying their apps are comprised of 51%-75% OSS, and 6% saying over 75% of their code is OSS.

This raises security concerns, including worrying about the high percentage of OSS in the application code, being victims of hackers targeting OSS, trusting the source of the code, identifying vulnerabilities, understanding the code composition and creating a software bill of materials, and being able to quickly remediate any issues as they are found.

Industry initiatives can help in this area. The Open Source Security Foundation and the Cloud Native Computing Foundation provide resources, initiatives and OSS tools to help developers. But, as mentioned in the previous section, the key is enabling consistency across development teams with the visibility and control to scale. Security teams should work with developers to understand the resources and components they use and help them with the right tools, processes and training to efficiently identify and address security issues to mitigate risk.

3. Managing API security

Another rapidly scaling area that security needs to address is the growing attack surface due to APIs. Enterprise Strategy Group research showed the highest percentage of survey respondents (45%) rated APIs as the cloud-native application element most susceptible to attack. It was also the leading type of security incident experienced in the past 12 months, with 38% of organizations suffering data loss due to incidents from the insecure usage of APIs.

As attackers increasingly target poorly protected APIs, OWASP now has a separate API Security Project with updates on the API Security Top 10, the organization's periodically updated list of the 10 most critical API security risks. The Enterprise Strategy Group 2022 research report "Trends in Modern Application Protection" found that more than one-third of organizations (37%) face challenges with API inventory, while 32% cited issues discovering and remediating misconfigurations. Organizations often use multiple API products for management and security, but they need a comprehensive strategy for API security -- from inventory and visibility to reducing misconfigurations and monitoring for security issues -- as a key part of their cloud application security strategy.

4. Securing cloud infrastructure entitlements

Cloud platforms enable developers to build and deploy applications without having to procure or maintain physical infrastructure, such as servers or data centers. Developers are empowered to provision their own cloud infrastructure, configuring entitlements to set permission for entities to access various infrastructure resources -- including VMs, containers, serverless functions, databases and storage -- to run the applications. Entities include human users and developers, as well as devices, other resources and other applications.

The numbers of entities and entitlements are proliferating. Plus, access is typically overprovisioned, increasing the number of entry points for attackers. Cloud infrastructure entitlement management (CIEM) can manage risk by giving security a view of entitlements and application activities to implement least privilege access to reduce their attack surface area. Cloud service providers as well as security, identity and access management and privileged access management vendors may offer CIEM capabilities, but organizations should look for options that make it easy to accurately and efficiently remove overprovisioned access. This will help mitigate security risk and meet compliance regulations.

5. Consolidating products for context to increase efficiency

Organizations face cyber incidents despite having multiple security products in place because they cannot remediate security issues in time to stop attacks. Key themes in 2022 were alert fatigue and the need for more context to help security teams prioritize needed action. Although *platform* may seem like a buzzword, the idea of a platform approach makes sense to drive efficiency. A platform pulls data from multiple sources and analyzes that data to bring more context and drive efficient remediation.

In this challenging economic climate, expect more vendor consolidation via acquisitions, as well as partnerships and integrations. The key will be the integrations, as most point tools are built differently and may be difficult or require rebuilding to properly work together. Organizations should look for ease of use, ways to reduce manual work or analysis and faster feedback loops for remediation, as well as visibility and context that helps security teams gain a clearer picture of their security posture and the actions needed to mitigate risk and meet compliance regulations.

Next Steps

Shifting security left requires a GitOps approach

Cloud application developers need built-in security

5 ways to improve your cloud security posture

This was last published in January 2023

Dig Deeper on Application and platform security

operational support system (OSS)

By: Paul Kirvan

White House cybersecurity plan collides with SecOps reality

By: Beth Pariseau

Top takeaways from first CloudNativeSecurityCon

By: Melinda Marks

Qualys QSC 2022: Live show reports & insights

By: Adrian Bridgwater

Networking

Prosimo offers free multi-cloud connectivity

The new MCN Foundation can find and connect to public clouds and provide visibility. The company's full-stack product powers the ...

Cisco to add SamKnows broadband visibility to ThousandEyes

SamKnows data in ThousandEyes will let enterprises monitor the broadband connections of employees working from home. The ...