2023:

Cisco Panoptica's Top 5 Cloud-Native Security Predictions for 2023

What we think lies ahead for DevOps and Security teams this year & beyond

Contents

Embrace the New in Cloud-Native Security

Welcome to 2023!

Looking ahead, we undoubtedly see the cloud-native landscape reinforcing its core business value into becoming even more mission critical to the digital economy.

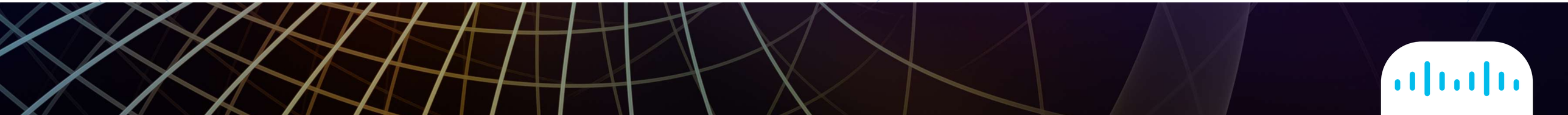
As the times ahead mark an unprecedented shift towards hybrid cloud, multi-cloud, and cross-cloud solutions, the cloud-native ecosystem will extend and expand across industry verticals. The adoption of Kubernetes will become a mainstay while barriers to the adoption of serverless computing will lift, making it even more accessible to DevOps.

A carryover from previous years, the question of security will persist on everyone's minds. CISO and DevOps across the board will be left with no choice but to take a bird's eye view into securing their microservices, APIs, and software supply chains with utmost resolve.

New and emerging security tools, best practices, regulations, frameworks, and solutions will simplify DevOps to advance their methodology to the next level of DevSecOps, where taking a "security-first" approach becomes paramount.

Now that 2022 is behind us, and we look to 2023, let's dive into five major cloud-native security predictions from Cisco's Emerging Technology and Incubation (ET&I) team. As you set sail towards the new year, keep our predictions in mind and prioritize cloud-native security over and above all else.

Are you ready to hear what the future of cloud-native security holds this year? Let's begin!



Prediction #1

“40% of organizations will take a ‘cloud-native first’ strategy in 2023 as they look to increase agility and efficiency while reducing costs, but security will continue to be a major concern.”

Source: Forrester

Prediction #1

In 2023, technology leaders are expected to continue to take a keen interest in cloud-native technologies comprising containerization, microservices, declarative code, serverless computing, and “composable” SaaS architectures that are driven by automation and orchestration. Forrester expects more enterprises to adopt cloud-native technologies as they increasingly opt to run workloads in containers rather than legacy virtual machines. Containers run more efficiently when leveraging new and emerging technologies like artificial intelligence and machine learning (AI/ML) and automation. The growing adoption of containers will also drive organizations to modernize their application development processes. Forrester’s survey found that containerized applications account for half of the total number of applications running in enterprises today, with Kubernetes orchestrating them at scale.

Securing cloud-native infrastructures is constantly evolving as a discipline, and new technologies and best practices are constantly emerging. However, some potential trends may shape the direction of cloud-native security in 2023:

DevOps will respond more thoughtfully to security: In 2023, threat actors will continue to develop and unleash new iterations of malware designed to gain access to data in cloud-native environments, and thus, this year, developers will feel a greater need to incorporate failsafe security practices earlier in their application development cycles, thereby further solidifying the DevSecOps methodology in their workflows this year.

There will be a much greater need to proactively anticipate where the dangers lie in order to take preventive measures to forestall them. Up until now engineering teams have been simply trying to get up to speed with Kubernetes, causing security to typically take a back seat. Moving forward, this will change as more DevOps engineers will take to adopting cloud-native security best practices that incorporate security into their processes.

Development of new security standards and best practices: As the cloud-native ecosystem matures, it is likely that new security standards will continue to emerge and solidify into best practices. These may include guidelines for securing cloud-native infrastructure, as well as recommendations for securing applications that are built using cloud-native technologies.

Greater adoption of cloud-native security tools: As organizations increasingly adopt cloud native technologies, they will likely also adopt security tools that are specifically designed for these environments. This may include tools for automating security checks and enforcing security policies, as well as tools for incident response and forensic analysis.

Increased focus on zero-trust security: Zero trust security is a security model that assumes that all network traffic is potentially malicious and requires authentication and authorization. This model is well-suited to cloud-native environments, where resources are often ephemeral and may be accessed from anywhere. The value of zero trust has been seen even at the federal government level, as the Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency (CISA) are working to move the U.S. government toward a zero-trust architecture. In fact, the Department of Defense (DOD) released its Zero Trust Strategy and Roadmap in November 2022, which goes into detail on how the department will implement zero trust to achieve a stronger cybersecurity posture over the next five years.

The global DevSecOps market is expected to grow at a CAGR of 33.7% by 2023. Growing at a CAGR of 30.76% from 2022 to 2030, it is projected to reach USD 41.66 billion by 2030.

Source: Infosec Institute

Prediction #2

“Securing containerized applications and Kubernetes will become a priority in 2023 due to adoption going mainstream. Policy-as-Code for Kubernetes will mature while troubleshooting Kubernetes will be driven by observability data.”

Prediction #2

This year dozens of leading organizations will embrace Open Policy Agent (OPA) in their Kubernetes deployments. The Open Policy Agent is an open source, general purpose policy engine that aims to provide a common framework for applying policy-as-code to any domain.

As more organizations adopt containers and Kubernetes, there will likely be a corresponding increase in the development of tools and practices for securing containerized applications. This may include new approaches to image signing and verification, as well as improved visibility and monitoring for containerized applications. Some other trends that will shape Kubernetes and container security in 2023 include:

Integration of Kubernetes security with broader cloud security frameworks: As organizations increasingly adopt both Kubernetes and cloud-native technologies, there will be a greater focus on integrating Kubernetes security with broader cloud security frameworks including integrations with cloud-based identity and access management systems and cloud-based security event and incident management systems.

Greater emphasis on securing the Kubernetes control plane: The Kubernetes control plane is the central management component of a Kubernetes cluster, and it is responsible for coordinating the actions of the worker nodes. Securing the control plane is critical to the overall security of the cluster, and it may become an increasingly important focus for Kubernetes security practitioners.

Greater traction in the use of Policy-as-Code: Policy-as-code enables DevOps teams to implement and enforce controls in different Kubernetes resources like pods, nodes, and clusters at virtually unlimited scale. It simplifies collaboration by providing a uniform and systematic way of managing policies. This includes collaboration not just within the same team, but also between different types of teams-especially between developers who are accustomed to working in code and specialists from other adjacencies like security or IT operations.

Observable approaches to troubleshooting Kubernetes: Applications running on a Kubernetes cluster at scale can be troublesome not just because Kubernetes itself is complex, but also due to the connections between so many moving parts.

Troubleshooting requires identifying issues in Kubernetes clusters, nodes, pods or containers. Identification makes the way for diagnostics and remediation. In 2023, DevSecOps will benefit from observability solutions that bring the following four elements together to provide a single comprehensive aggregated view from which to quickly determine troubleshooting issues in Kubernetes:

- **Events**—Event monitoring zeros-in on every change that occurs, where it occurred, and what caused it.
- **Logs**—Log analytics are used to spot warnings and ongoing issues to then determine what went wrong.
- **Telemetry data**—With standards like OpenTelemetry growing in adoption, data from telemetry is becoming essential in troubleshooting Kubernetes.
- **Trace data**—Trace data is powerful in giving insights on golden signals like error rate, throughput, and traffic.

Prediction #3

“Serverless computing will continue to be a popular choice for event-based workloads in 2023, and evolve in areas of standardization, interoperability, emerging code concepts, and most importantly—security.”

Prediction #3

Serverless computing provides “Function-as-a-Service” or (FaaS) to application developers on an as-needed basis from cloud service providers or CSPs such as AWS Lambda. Under FaaS, developers still write custom server-side logic, but it’s run within containers that are fully managed by the cloud service provider. This is useful as it provides flexibility for server-side applications. But being a new technology means despite its ability for adaptation and integration, the DevOps community is still dealing with a lack of standardization and interoperability with serverless. The resulting risk of vendor lock-in has left many enterprises stalled in their adoption journey even as serverless computing continues to pique the interest of developers for event-based workloads.

To bridge the gap and broaden adoption across vendor-agnostic functions, we will witness disruption with the Google-sponsored Knative project, which it describes as an open-source framework that provides serverless building blocks for Kubernetes. Kubernetes is the container platform of choice and vendors working together on the Knative project will ensure that standards would be shared across different FaaS implementations, thereby increasing interoperability. Another disruption to serverless in 2023 is a new emerging concept called “infrastructure-from-code” or (IfC) as a way of creating applications that allow your cloud provider to inspect the application code during deployment, and then automatically provision the underlying infrastructure the application code needs.

On the question of securing serverless, several potential trends will come into play in 2023:

Increased focus on securing serverless functions: As the use of serverless technologies continues to grow, there will likely be a corresponding increase in the development of tools and practices for securing serverless functions. This may include new approaches to authenticating and authorizing function invocations, as well as improved visibility and monitoring for serverless applications.

Development of new tools and practices for securing serverless infrastructure: In addition to securing the functions themselves, there will likely be a focus on securing the underlying infrastructure that powers serverless platforms. This may include new approaches to securing the runtime environments in which functions execute, as well as tools and practices for securing the underlying infrastructure that supports serverless platforms.

Integration of serverless security with broader cloud security frameworks: As organizations increasingly adopt both serverless and cloud native technologies, there will likely be a greater focus on integrating serverless security with broader cloud security frameworks. This may include integrating serverless security with cloud-based identity and access management systems, as well as integrating serverless security with cloud-based security event and incident management systems.

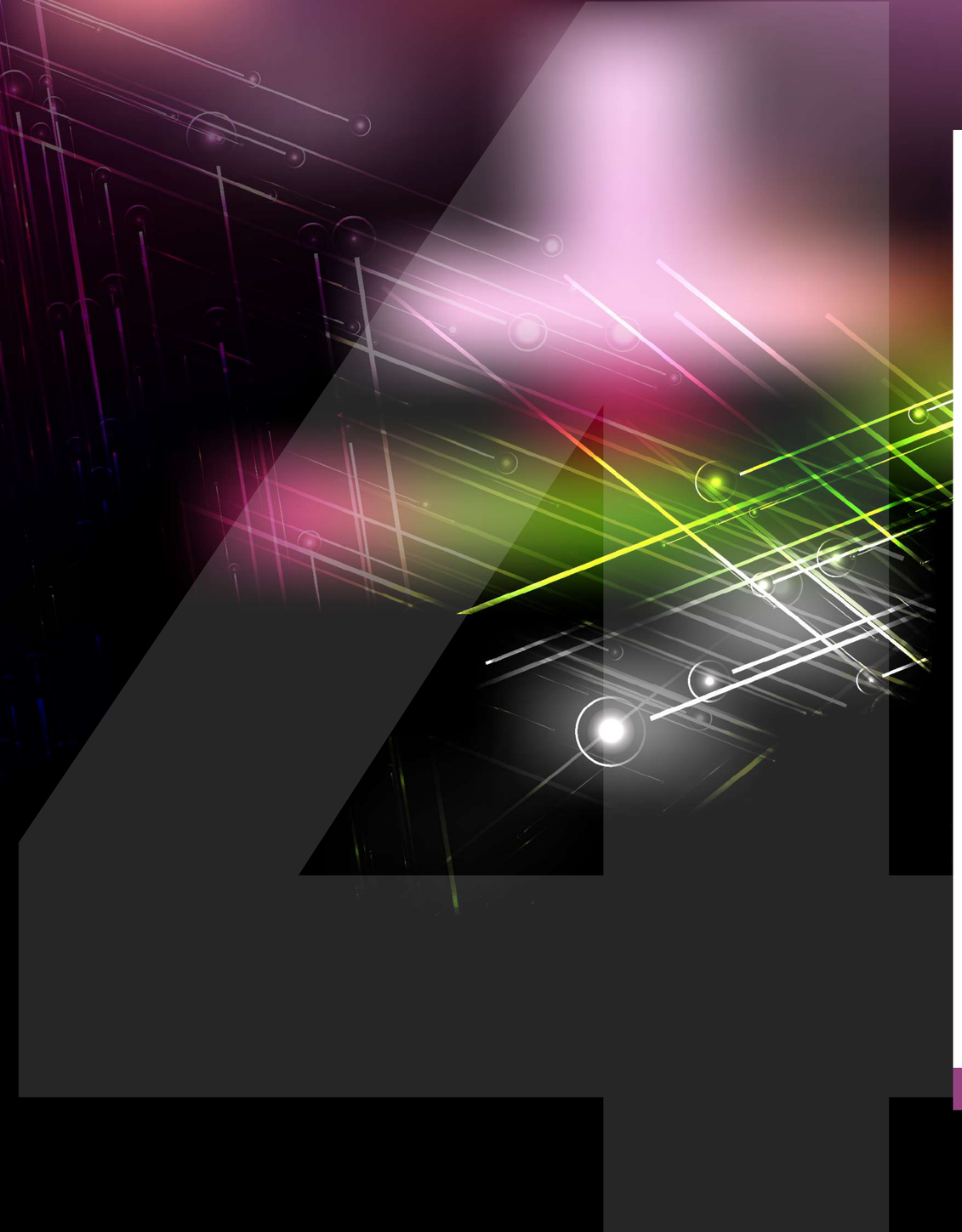
Emphasis on security automation: As the complexity of serverless environments increases, there will likely be a greater emphasis on automating security tasks and processes. This may include the use of automation tools to enforce security policies, as well as the use of machine learning and artificial intelligence to improve the accuracy and efficiency of security operations.

Greater adoption of zero-trust security: As mentioned earlier, zero trust security is a security model that assumes that all network traffic is potentially malicious and requires authentication and authorization. This model is well-suited to serverless environments, where resources are ephemeral and may be accessed from anywhere.

Increased emphasis on securing the function code and runtime environment: In serverless architectures, the function code and runtime environment are critical components that need to be secured. This may include measures such as code signing and verification, as well as hardening the runtime environment to prevent malicious code injection.

A key driver of serverless architecture adoption in 2023 will continue to be the ability to eliminate server management. By 2027, the serverless architecture market is estimated to reach US$ 25.65 Billion at a CAGR of 19.03%.

Source: Digital Journal



Prediction #4

“API security will be top-of-mind in 2023 due to unmanaged API sprawl becoming the prime target for bad actors. The financial services industry will be most vulnerable to API attacks.”

Prediction #4

According to Gartner, by 2023, over 50% of B2B transactions will be performed through real-time APIs, and by 2025, less than 50% of enterprise APIs will be managed, as the growth in APIs surpasses the capabilities of API management tools.

Source: Infosec Institute

APIs are powerful in that they enable DevOps teams to seamlessly integrate various functionalities and programmatic interactions into applications. From facilitating financial transactions and marketing automation to creating connected customer experiences, APIs are the de facto backbone of cloud-native application development.

While REST and HTTP-based services continue to remain the most popular API architecture styles, their usage will continue to level off in 2023 as newer event-driven API architectures such as GraphQL and gRPC will grow in popularity. GraphQL connects disparate data sources faster while gRPC facilitates faster two-way data exchange between internal microservices.

That said, the ubiquity of APIs will exacerbate sprawl issues this year. The sprawl of APIs within and between cloud-native infrastructures has made API security one of the biggest challenges for DevOps today. This also means that unmanaged APIs will become a popular target for cyber criminals who can use them as gateways to get unfettered access to sensitive data. In pursuit of this data, cybercriminals will put more focus on vulnerable API endpoints that connect directly to an organization's underlying databases. Expect to hear about more damaging attacks on individual APIs that lead to data leakage.

In the financial services industry, APIs will predictably remain at the center of open banking. That means, newly minted APIs will continue to overrun modern banking apps causing a continuous widening of the attack surface and therefore, requiring robust protection from cyberattacks. We would be remiss if we don't overemphasize that API security should be the single most important cybersecurity priority for the Banking and Financial Services (BFSI) vertical this year.

As far as securing APIs goes, we can expect to see API security gain more traction as a subdiscipline of cloud-native security, more so this year than in previous years, with these potential developments:

Increased adoption of zero-trust security: As mentioned earlier, zero-trust security is a security model that assumes that all network traffic is potentially malicious and requires authentication and authorization. This model is well-suited to API-based architectures, where resources are often accessed remotely and may be accessed from anywhere.

Greater emphasis on securing the API gateway: The API gateway is a critical component of an API-based architecture, and it serves as the entry point for all API requests. As such, securing the API gateway is critical to the overall security of the API ecosystem. This may include measures such as access control, rate limiting, and request/response validation.

Development of new tools and practices for securing APIs: As more organizations adopt APIs, there will likely be a corresponding increase in the development of tools and practices for securing APIs. This may include new approaches to API testing and vulnerability assessment, as well as improved visibility and monitoring for APIs.

Integration of API security with broader security frameworks: As organizations increasingly adopt both APIs and cloud native technologies, there will likely be a greater focus on integrating API security with broader security frameworks. This may include integrating API security with cloud-based identity and access management systems, as well as integrating API security with cloud-based security event and incident management systems.

Prediction #5

“Software supply chain attacks are expected to rise in 2023. Industry solutions that support accurate SBOM generation and software signatures will dominate the enterprise.”

Prediction #5

If what the industry has witnessed in the past three years with software supply chain (SSC) security is any indication, then cyberattacks on software supply chains will only increase in both frequency and severity this year, as they have in the last three years.

Software supply chain security is a key priority this year, as organizations expect to face an onslaught of attacks on everything from open-source and third-party software packages and libraries to developer's user accounts and log-in credentials, and all other components needed to build, package, and sign software.

That said, new federal mandates and industry guidance intended to address supply chain risks will put new pressure on enterprises this year to adopt established and evolving best practices that address SSC security. Most notably, these new regulations and frameworks will make the most difference in shaping how things fare in 2023:

- The Securing Open-Source Software Act (SOSSA) of 2022 mandated by U.S. Congress to directly address open-source security in terms of vulnerability detection and disclosure, software bill of materials (SBOMs) and the office of open-source programs (OSPOs).
- Guidelines for securing the software supply chain under Enduring Security Framework (ESF) that establish new requirements to secure the federal government's software supply chain
- The new Supply-chain Levels for Software Artifacts (SLSA) framework from Google that ensures end-to-end software supply chain integrity.

Considering the points made earlier, some developments that will shape the direction of SBOM-related security in the world of cloud-native applications are:

Software component management tools will become important: Tools used to track and manage open-source software (OSS) components that developers use to build and deploy cloud-native applications will become important to developers. These tools will ensure that developers are using secure and up-to-date OSS software components and help them identify and address any vulnerabilities that may be present in their SBOMs.

New assessment tools and testing practices will come into focus: for securing software components. These include new approaches to testing of software components and assessing them for vulnerabilities assessment, as well as improved visibility and monitoring for software components.

Integrating SBOM-related security with broader security frameworks: These will include cloud-based identity and access management systems and cloud-based security event and incident management systems. Integrations with these frameworks will enable organizations to manage the security of their software components in a more holistic and integrated way, and to more effectively detect and respond to security threats.

Gartner predicts that by 2025, 45% of organizations will experience attacks on their software supply chains, which will be three times as many as in 2021.

Source: Gartner

Conclusion

Today, it is imperative for enterprises of all sizes and geographies to adopt a cloud-native application development model—one that supports the development of modern apps built to meet the needs of the modern user. But, for a modern app to yield unprecedented efficiency, scale, and value, its single biggest enabler is security.

Cisco's Emerging Technologies and Incubation team is paving the way with "DevOps-friendly" cloud-native security solutions that fundamentally simplify conventional offerings. Built from the ground up to meet the needs of your mission-critical modern applications, our Panoptica solution simplifies cloud-native application security making it easy to embed into your software development lifecycle.

Panoptica protects the full application stack from code to runtime by scanning for security vulnerabilities in the cloud infrastructure, microservices (Containers or Serverless), the software bill of materials, and the interconnecting APIs.

And best of all, it integrates with the tools that your application development and SecOps teams are already using like GitHub, Helm, and Terraform.

Learn more and get started

Visit Panoptica.app

Sign Up for a Free Trial

Access Additional Resources

Read Our Blogs

Get More Content