Cloud Native Security Microsurvey:

More than 80% of organizations want to build modern security systems with open source software

With the help of the CNCF Security Technical Advisory Group (TAG), CNCF recently conducted a microsurvey of the community to see how organizations are managing cloud native security.

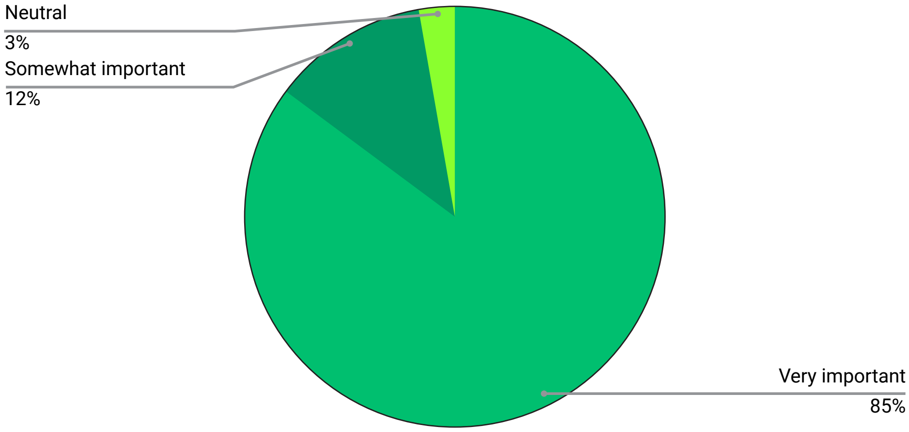
The survey received 128 responses, with the majority of questions receiving about 75 responses.

MODERN SECURITY IS IMPORTANT

An overwhelming 85% of respondents indicated that modernizing security is very important to their organization's cloud native deployment. Another 12% believe it is somewhat important, and 3% feel neutral. No one indicated that it is not important.

Organizations recognize the differences between traditional and modern security in cloud native architectures. Modern Security doesn't just mean traditional security with cloud native solutions tacked on. It requires an entirely different approach that emphasizes dynamic, granular, and nuanced control rather than legacy checklists.

How important is modernizing security to your cloud native environments?



A string of recent high-profile breaches underscores that the stakes are higher than ever. More and more data is living online. Organizations have to figure how to manage all of this data with a secure configuration without breaking functionality. Bad actors don't need to go to extremes, they only need to be savvy enough to find a window of opportunity and take it. Which they will.

While many organizations have large security teams working to neutralize these threats, smaller organizations are putting trust in developers and operators to ensure the applications and infrastructure they are building have security built-in.

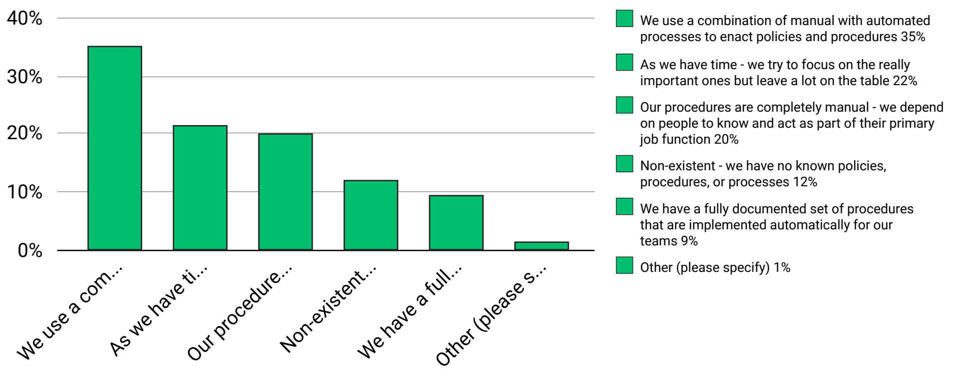
In theory, cloud native is designed to provide a complete — yet flexible — trusted toolkit for modern architectures. This becomes more difficult given the rate at which new projects are emerging. Teams have to figure out how these tools best operate together, if at all. Each tool adds value, yet to be capable of working well together, there needs to be some standardization and security integration across the architecture and stack. This is where the Security TAG is focusing its efforts.

THE STATE OF CLOUD NATIVE SECURITY

Survey respondents were asked to describe their processes and policies for securing third-party software. Only 9% had a fully documented set of procedures that are implemented automatically for their teams. So, while organizations recognize the importance of having these policies in place, there is still a very long way to go as a community to increase adoption and develop tooling to ease the burden of implementation.

Just over one-third (35%) of respondents indicated their organizations use a combination of manual with automated processes to enact policies and procedures. Another 22% said they do it as they have time and focus on the really important ones but were leaving a lot on the table. This indicates too much noise in tooling to drive these processes and not enough signal to make automation possible. As a result, organizations have to work by trial and error to find the tools that provide value and context to drive policy decisions.

Some 20% said their processes are completely manual, and they depend on people to know and act as part of their primary job function. Alarmingly, 12% said non-existent – they had no known policies, procedures, or processes. Organizations in these categories leave themselves vulnerable. Employees are liable to be overworked, burned out, dealing with fires, and playing catch-up before another incident happens, and therefore be less likely to proactively improve security or innovate in that space.



How would you describe your processes and policies for securing third-party software:

Even though very few organizations reported having processes and policies firmly in place, 82% of respondents said it's important that the security systems they implement are built using open source software. No one indicated that they felt open source was too risky to trust, a sign that Linus' Law is well understood. This may be because organizations see open source tools as being more interoperable and focused on standards. This enables organizations to pick and choose the security they want, knowing they are gaining collective benefit, with the added value of contributing critical changes that benefit the wider community. Security is not a proprietary concept. The ecosystem as a whole collectively benefits from the lessons and learnings of others. However, there is a long-standing stigma around sharing, especially in security, that we will continue to dissolve.

NO SHORTAGE OF CHALLENGES

While most respondents felt optimistic about cloud native and open source, many have also experienced challenges.

The top challenges organizations experience in running cloud native environments include:

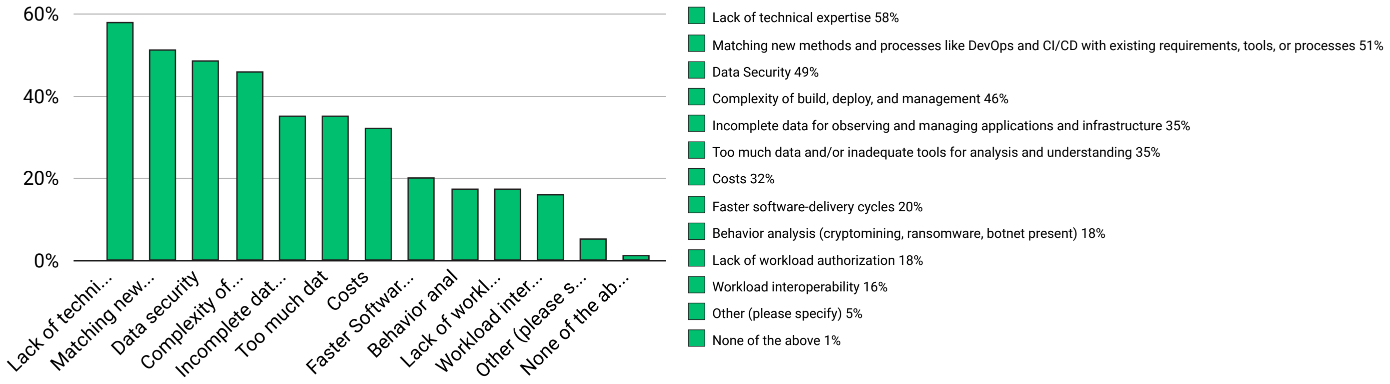
1. **A lack of technical expertise (58%).** This is not surprising as talent shortages have been reported in many other areas of software development. Also, cloud native security is a broad field, so the demand for security professional talent is high.

2. **Trouble matching new methods and processes like DevOps and CI/CD with existing requirements, tools, or processes (51%).** This is a well-known gap in the community – existing compliance frameworks have yet to catch up. While necessary, it is not particularly an exciting area, as we've seen with the general limits of automated compliance tooling (OSCAL being an exception).

3. **Data Security (49%).** Seeing this high-up on the list is actually a good thing. Organizations are considering shifting to a data-centric security model and might be positioning themselves to begin looking into Zero Trust. It may become a more prolific area of focus in the coming years, so be sure to keep an eye out.

4. **The complexity of building, deploying, and management (46%).** This likely ties back to the lack of technical expertise. Like all technology revolutions, modern security requires a cultural shift, and many organizations are still figuring out how to do this. There is no "easy out" on cloud native journeys, and there certainly isn't one for cloud native security. Each organization will need to learn and transform its approaches and processes while considering the existing documentation and papers available in this space, another where TAG Security contributes.

Which of the following challenges have you experienced in running cloud native environments? Please select all that apply.



Many cloud native tools claim to be secure by default. Still, respondents indicated that there were many things they have had to augment in cloud native projects to deliver greater security. These included:

1. **Authentication, identity, and access management (66%).** There is a known lack of tooling in this space and an inconsistency in support for identity and access management (IAM) tooling. Establishing new standards or specifications around IAM could help alleviate this.

While some tooling does exist, lack of adoption, different use cases, and organizations' bespoke IAM solutions increase the challenges in this area.

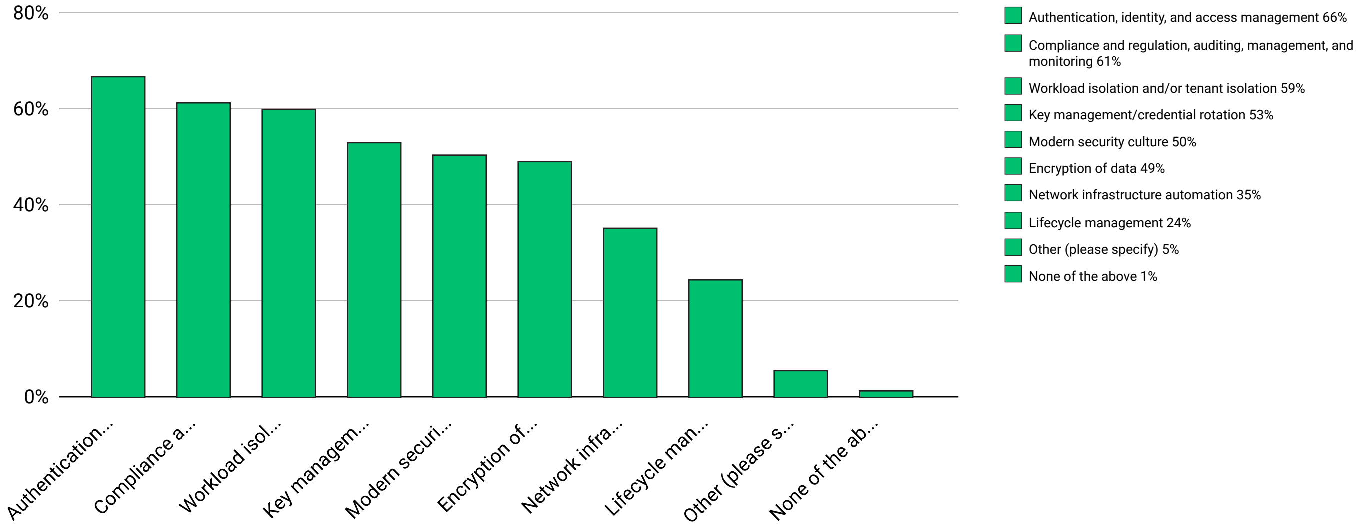
2. **Compliance and regulation, auditing, management, and monitoring (61%).** There is a gap in existing frameworks where industry, regulatory bodies, and the community needs to catch up.

3. **Workload isolation and/or tenant isolation (59%).** One issue is that orchestration systems do not have this baked in from the start. A lot of tools have adopted the tenancy model that the orchestration system has provided because the orchestration system sets the foundation of the threat model. Isolation is also difficult and not well discussed, and the tooling in this space has resource implications. We would love to see more engagement from the community and organizations about elevating and implementing the existing isolation methods and tooling to increase maturity in this space.

4. **Key management/credential rotation (53%).** The secrets and credential management spaces are also very limited, though new solutions are emerging.

5. **Modern security culture (50%).** This is very likely tied to the lack of technical expertise. Security is still very traditional in culture. There has not been much discussion within the security community about how DevOps, CI/CD, and distributed, immutable, ephemeral (DIE) contribute to more secure architectures.

Which of the following have you had to augment in cloud native projects to deliver greater security? Please select all that apply.



While being in favor of cloud native and open source, respondents expressed concern for making greater use of cloud native. When asked, respondents indicated their biggest concerns were:

1. **No secure-by-default guarantees or options (53%).** This could be due to a lack of certifications or conformance with existing practices. Projects adhering to CII and adding a badge to their repositories could help to alleviate this concern around how projects were

developed securely. However, it does not express a project as secure-by-default. There have been several nominations and ideas around the growing attestation of secure-defaults, but this is still nascent.

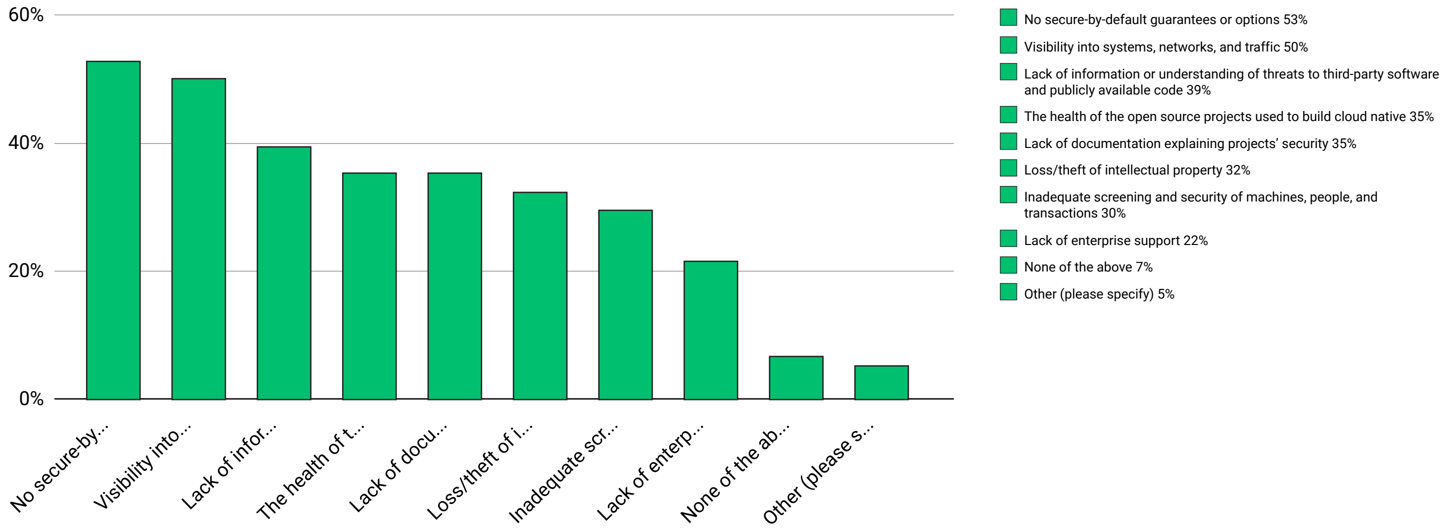
2. **Visibility into systems, networks, and traffic (50%).** While cloud native monitoring tools like Prometheus exist, they are primarily used for tracking performance. Tools like Falco will help, but it is still in the early stages of adoption.

3. **Lack of information or understanding of threats to third-party software and publicly available code (39%).** This is a problem with open source software in that no one is charged with providing this information. Foundations and groups need to work together to fill this need.

4. **The health of the open source projects used to build cloud native (35%).** This is another area where adding a CII badge or other security label could help to ensure conformance with secure development.

5. **Lack of documentation explaining projects' security (35%).** This is often missed by projects that are not designed for security. The Security TAG encourages projects to complete a self-assessment and submit a pull request to their repo (for independent storage) to help identify gaps in documentation.

Which, if any, of the following concerns do you have about making greater use of cloud native products or projects? This includes processing, transmitting, or storing data with hybrid, multi, and/or on-prem cloud environments. Please select all that apply.



WHAT ABOUT EDGE?

Edge computing has emerged as a viable option for building and deploying applications, and more developers want to use Kubernetes and other cloud native technologies outside of typical data center deployments. These developers want to use all of the tools and best practices they are accustomed to, even in non-tradi tional environments. However, this brings new security implications.

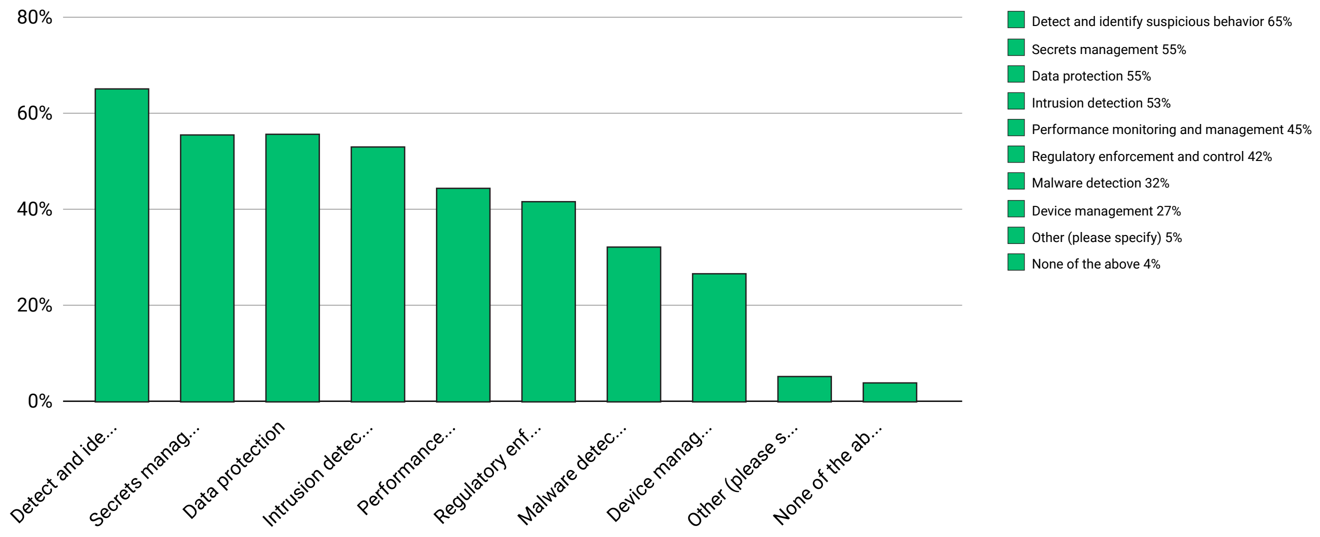
Respondents had concerns about security at the edge, the largest being:

1. **Misconfiguration (31%).** This is due to a lack of documentation and testing for secure configurations.
2. **Unpatched vulnerabilities (18%).** Organizations should increase their release and update cadence to help address this.
3. **Backdoors into the corporate network (15%).** This underscored the importance of having identity and access management tools available and ensuring they are being utilized correctly.

At the same time, expectations are high. Respondents expect cloud native projects in edge computing to have the following capabilities:

1. Detect and identify suspicious behavior (65%)
2. Secrets management (55%)
3. Data protection (55%)
4. Intrusion detection (53%)

Which of the following security capabilities do you expect from cloud native projects in edge computing? Please select all that a...

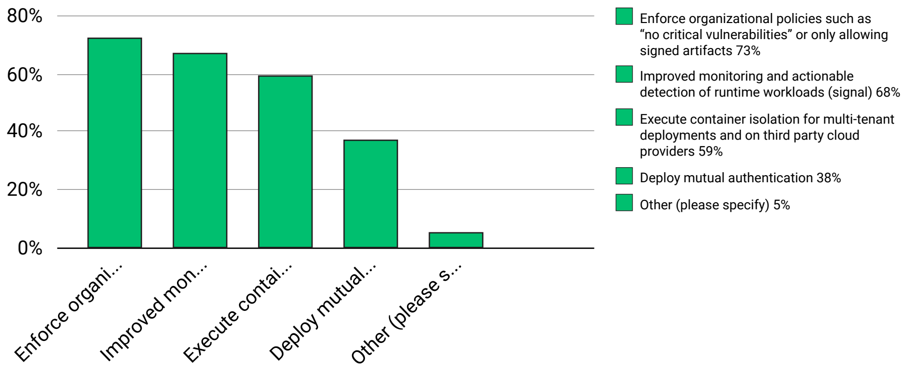


LOOKING FORWARD

Further demonstrating the desire for open source software, organizations would like to have multiple open source alternatives for security for the following proprietary technologies:

1. Key Vault, Vault (59%)
2. Splunk, ELK (53%)
3. AWS Key Management Service (30%)
4. HSM replacement (23%)

Looking at the next two to five years, organizations have big plans for security. Nearly three-quarters (73%) of respondents said their organizations intend to focus efforts on enforcing organizational policies such as “no critical vulnerabilities” or only allowing signed artifacts. More than two-thirds (68%) said they would focus on improving monitoring and actionable detection of runtime workloads in the same timeframe. Three-fifths (60%) said their organization intends to execute container isolation for multi-tenant deployments and third-party cloud providers. Respondents were allowed to select more than one area of focus.



Where do you intend to focus your efforts for greater security in cloud nativeover the next 2-5 years?

METHODOLOGY

The microsurvey was designed by the CNCF Security TAG. It was conducted between July and September 2021 and was shared with the CNCF and Kubernetes communities.

Of 128 respondents:

- 41% were from Europe
- 35% came from North America
- 16% from Asia
- The remaining 8% were from Africa, Australia/Oceania, or Central/South America.

Nearly half (49%) represented organizations with more than 1,000 employees.

- 31% came from organizations with between 50-999 employees.
- 20% represented organizations with fewer than 50 employees.

The most common job functions were SRE/DevOps Engineer (23%), Software Architect (17%), and Security Engineer (15%)

- Other job functions included Engineering Manager (9%), DevOps Management (7%), and Full-Stack Developer (5%).
- 10% selected Other, with responses including CTO, CIO, and single-person company.

43% represented organizations in the software/technology industry. Other industries include:

- Consulting (13%)
- Financial Services (13%)
- Consumer (7%)

The majority of respondents (58%) indicated their organizations use a hybrid cloud approach.

- Another 29% use only the public cloud, while 13% use only private or on-premises data centers.