IDC

Operationalizing Defense in Depth

With the growing use of open source technologies, gaining visibility into and vetting upstream open source software using a software supply chain security process is imperative to consume open source technologies securely

When you think about open source software supply chain security, who should be primarily responsible?

n = 203; Source: IDC *OSS Use and Support Survey,* Feb 2022

The future of digital-first economies is enabled by cloud-centric architectures, cross-cloud autonomous operations, consumption-driven subscriptions, robust edge connectivity and continuous lifecycle support and security for traditional and cloud-native applications and IT infrastructures.

The decision to adopt cloud computing involves organizations assuming several risks including relational, performance, compliance, and regulatory technological risks. To reduce these risks, organizations should seek vendors that offer a wide range of robust services for compliance, governance, resource allocation, availability, and security. What's key is enabling a defense-in-depth approach including visibility and transparency into open-source usage by implementing a layered security approach across the entire stack and software development life cycle (SDLC).

According to the IDC *Open Source Software Use and Support Survey,* February 2022, nearly half of respondents believe open source software (OSS) supply chain security is the responsibility of the entire community – developers, users and commercializers. However, unprecedented challenges such as increasingly sophisticated cybersecurity attacks, escalating and complex regulatory requirements and fragmented IT and security infrastructures lead many organizations to focus on engaging with commercial OSS vendors that provide solutions that allow for a defense-in-depth approach.

The attributes of such a defense-in-depth approach should include the following:

- **Security.** Hacking and identity theft incidents leading to data breaches have become increasingly commonplace and a daily cost of doing business on the internet. IDC's *Kubernetes and Security: Friend or Foe of Implementing Secure Code?* survey findings indicate that organizations initially deploy containers and/or Kubernetes to improve security even as security continues to remain the #1 challenge in cloud deployments, including containers and Kubernetes deployments. It is therefore crucial to test for vulnerabilities in applications and container images early in the application development life cycle. Software supply chain security with security integrated early in the application life cycle during the build, run, and deploy phases; talented cybersecurity staff; and tools for hybrid multicloud security, visibility, configuration, automation, and management are a must to ensure a robust security posture.
- **Compliance.** IDC's *Future of Trust 2021* survey indicates that increasingly complex regulatory compliance requirements are one of the key drivers of trust. Adhering to industry and regional regulations can be a complex undertaking and requires constant reevaluations as new regulations take shape. Compliance is also being closely monitored by internal boards and customers as seen by the sharp increase in audit requests by these stakeholders.
- **Transparency.** Trust and transparency go hand-in-hand. The 2021 U.S. Executive Order 14028, Improving the Nation's Cybersecurity in Sec. 4 *Enhancing Software Supply Chain Security* states the importance of "ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product." This guidance is a precursor for a software bill of materials (SBOM). While organizations need to ensure they have processes in place that can document what information is being stored, where it's being stored, and when to make it available, if necessary, the transparency and vetting of upstream open source code has now become an integral part of the software supply chain security conversation.

Essential Guidance for Finding a Trusted Software Vendor

When evaluating vendors, it's important to understand the needs of the workforce. For example, IDC research indicates:

- 35% of the global workforce are millennials who value trust perceptions of the vendor. For these end users, transparency, ethics and data security and privacy in hybrid multicloud environments are critical.
- Choosing vendors that provide automated assessment tools to predict risk, recommend actions, and track costs to better manage hybrid multicloud environments increases staff productivity and acts as a talent gap bridge.

Additionally, vendors should be able to operationalize defense in depth:

- Seek vendors that provide trusted hardened technologies and who take a layered, defense-in-depth approach to help organizations implement security across the infrastructure and application stack and life cycle.
- Insist upon software that is developed and hardened using a software supply chain security process. This includes scanning and vetting of all software source code, code signing, extensive quality engineering testing, software distributed from a trusted and secured distribution platform, and enterprise level support and service as modern-day prerequisites to securing the enterprise.