

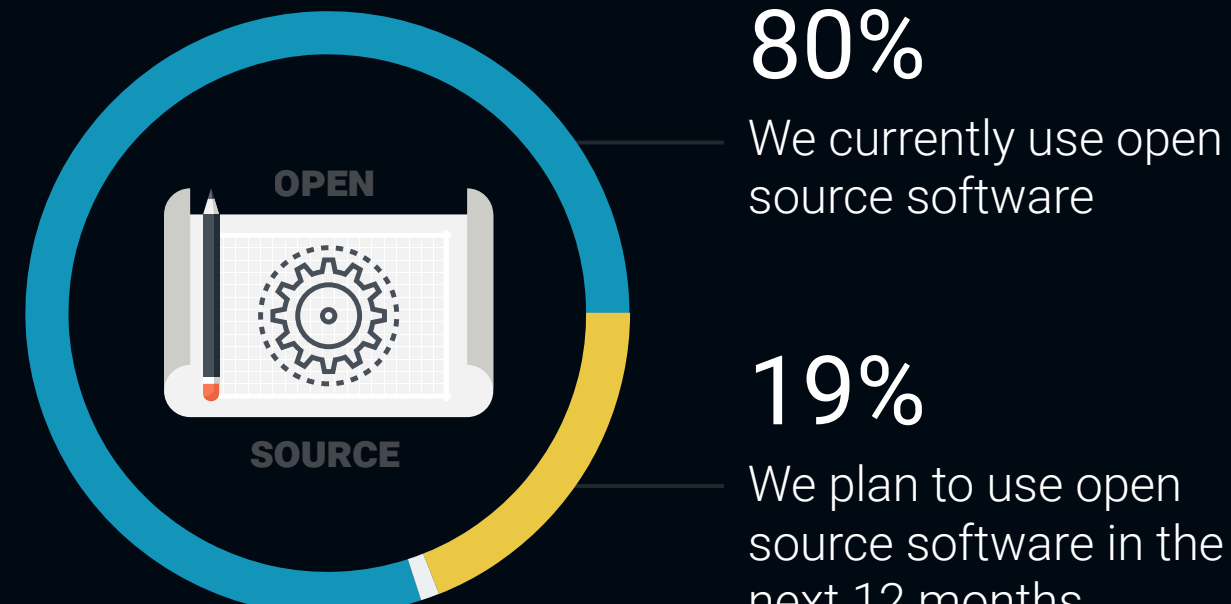
Using Runtime Visibility for Rapid Remediation of Java Vulnerabilities

Using open source software (OSS) helps development teams save time so they can focus on building custom code for their applications. However, the proliferation of third-party code in software supply chains introduces enterprise risk in the form of vulnerabilities, such as Log4j. When a vulnerability is discovered, security teams need the visibility to quickly find and remediate the security issues to protect their applications from attacks.

The Need to Secure Open Source Software

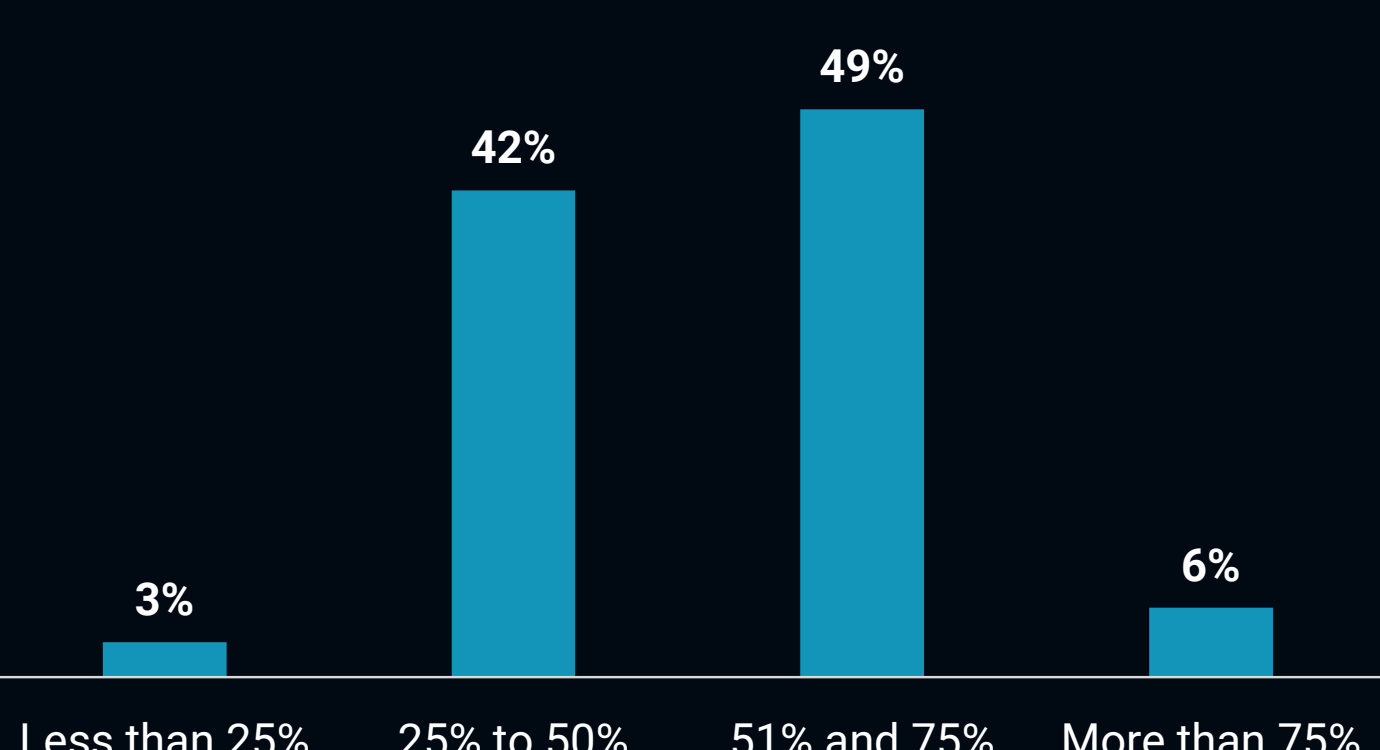
Organizations are increasingly using OSS components (libraries, frameworks, SDKs, etc.) in their software. Nearly all organizations are using or planning to use OSS, and OSS comprises a high percentage of their application code.

» OSS Usage

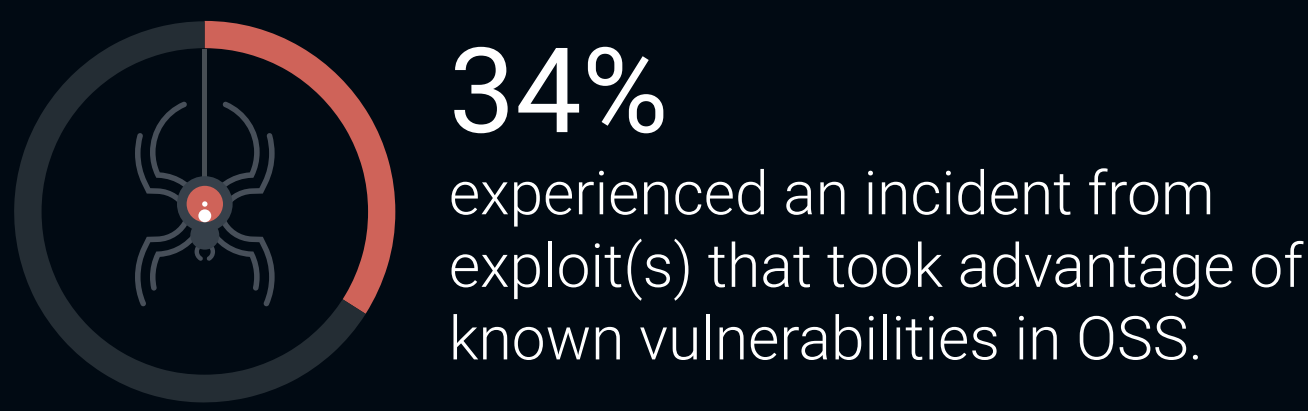


An additional 1% said they are interested in using open source software.

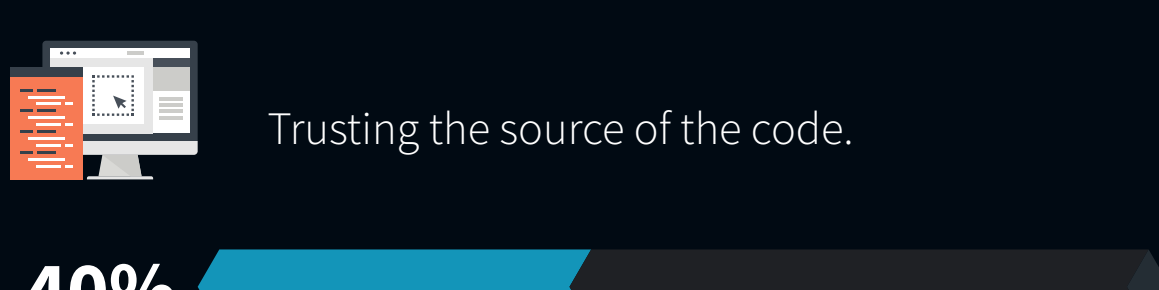
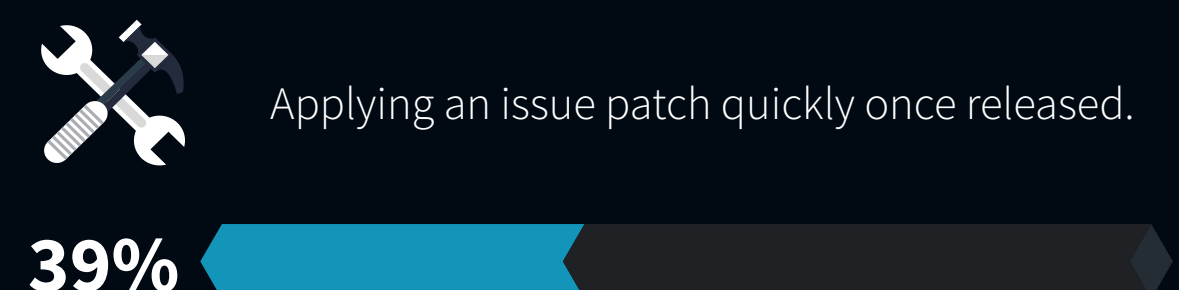
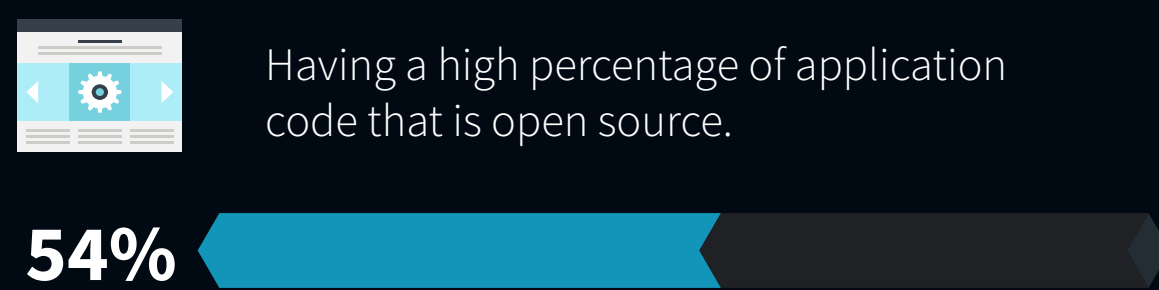
» Percentage of code composition that is OSS.



Over the past 12 months, organizations have faced security incidents related to their usage of OSS.

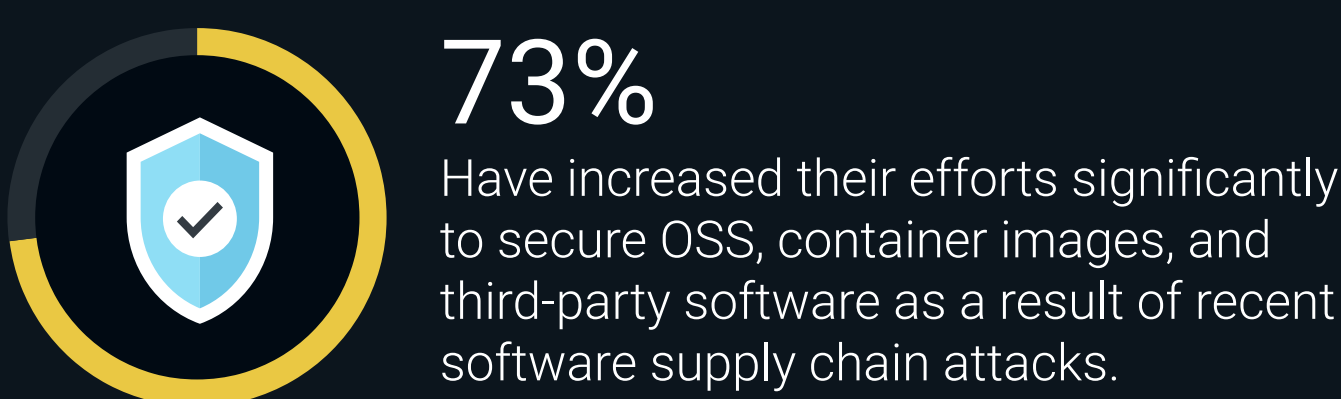


» Top security challenges and concerns about using open source software:

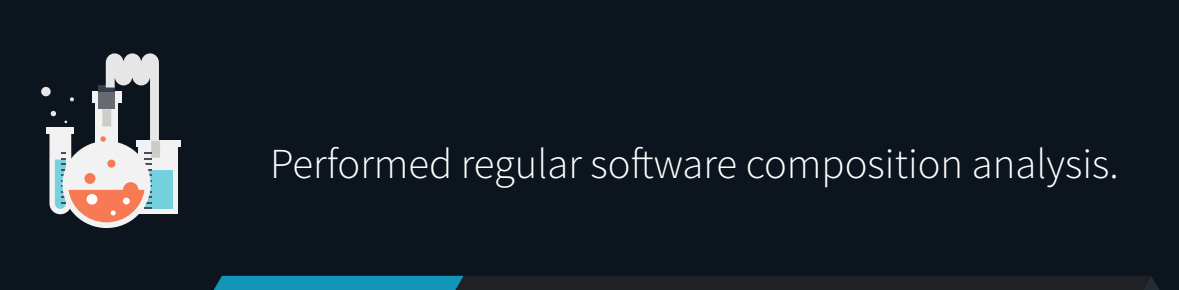
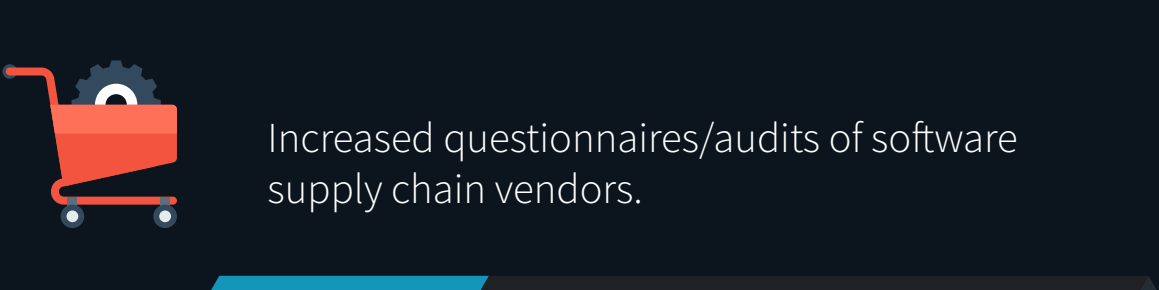
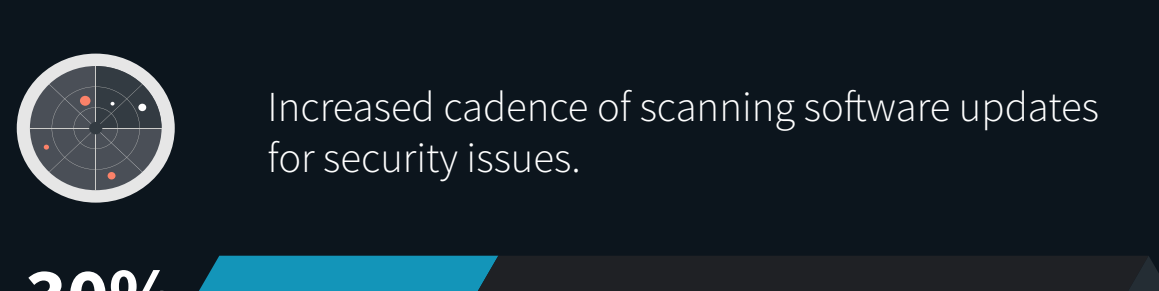
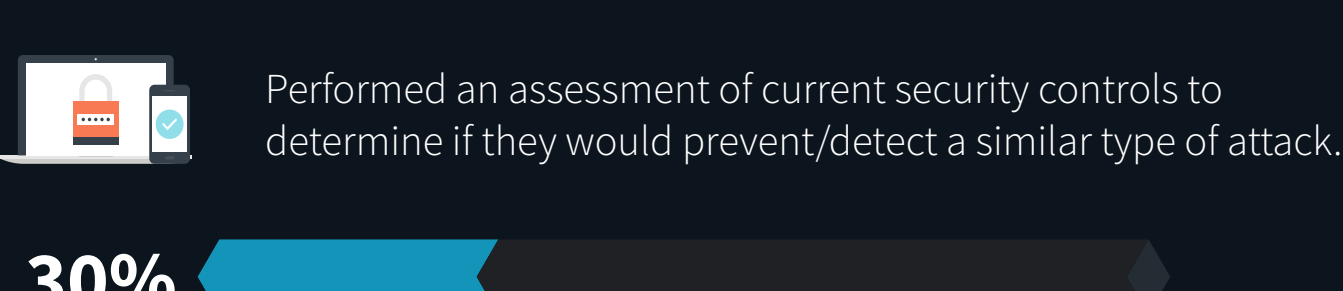


The Need for More Efficient Response to Java Vulnerabilities

In light of recent attacks, including Log4j, the Java attack where customers were challenged finding their affected Java instances and remediating the vulnerabilities, organizations have ramped up their investment in securing their software supply chain.



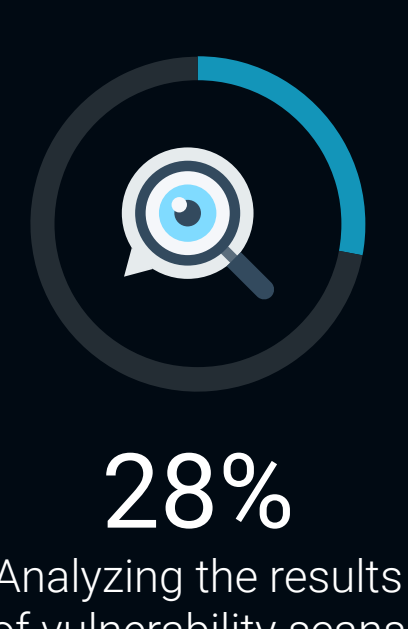
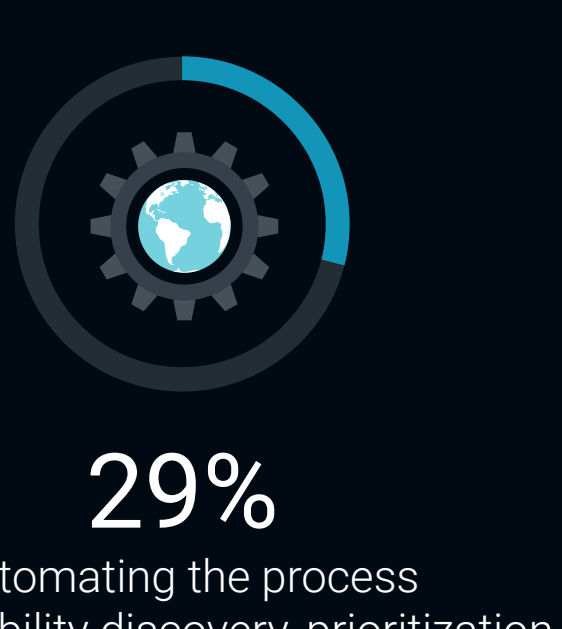
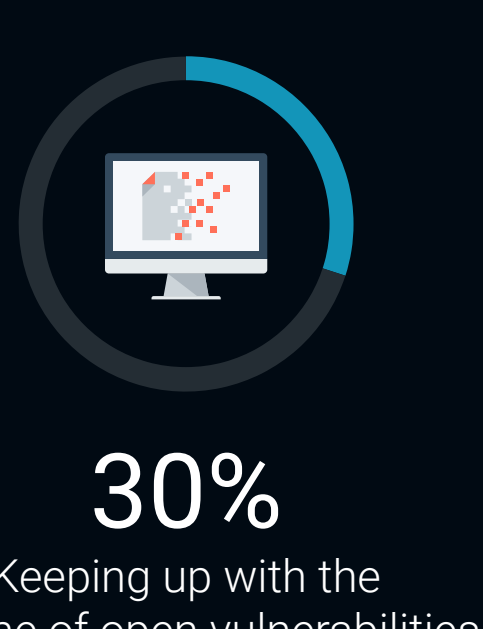
» Organizations are taking a wide range of actions to remediate risk, including:



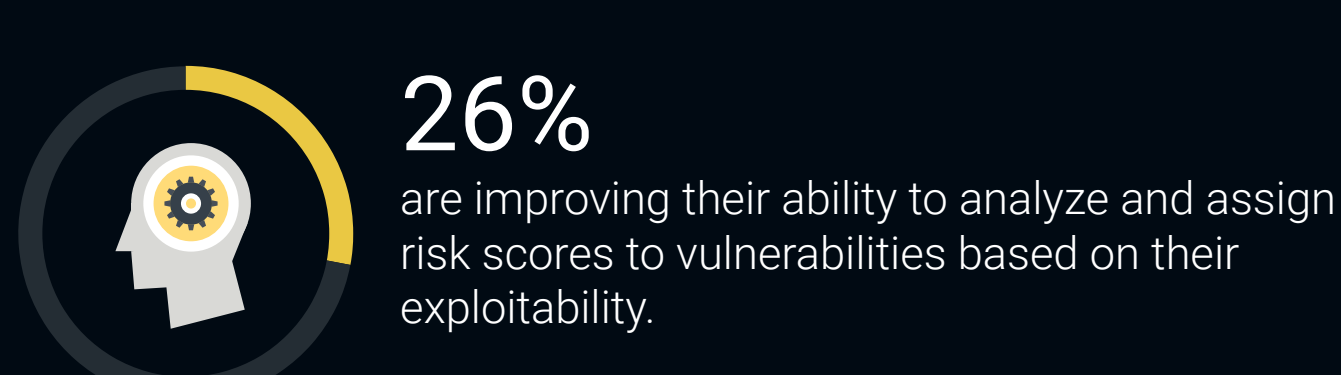
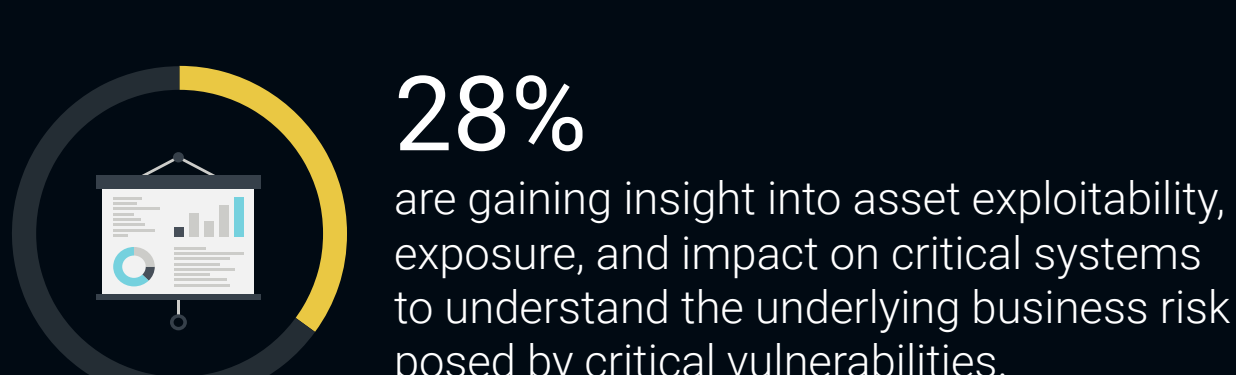
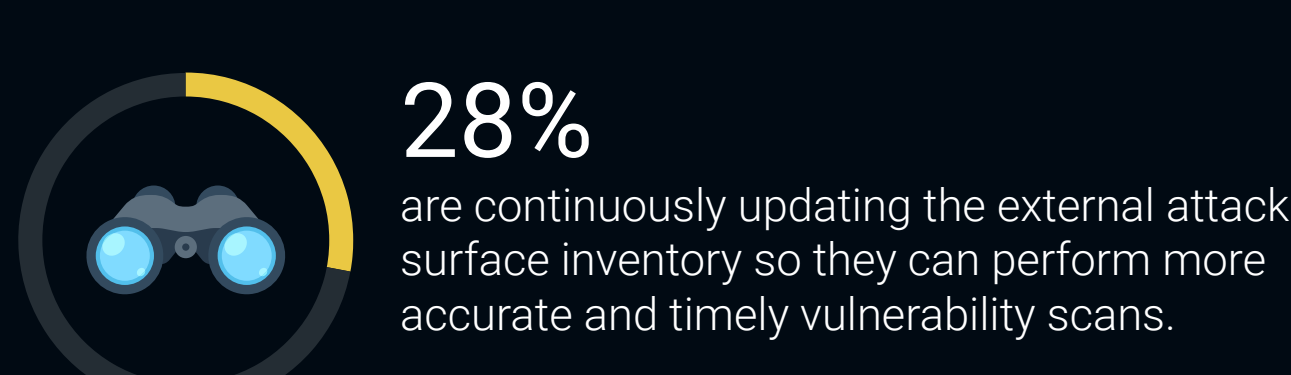
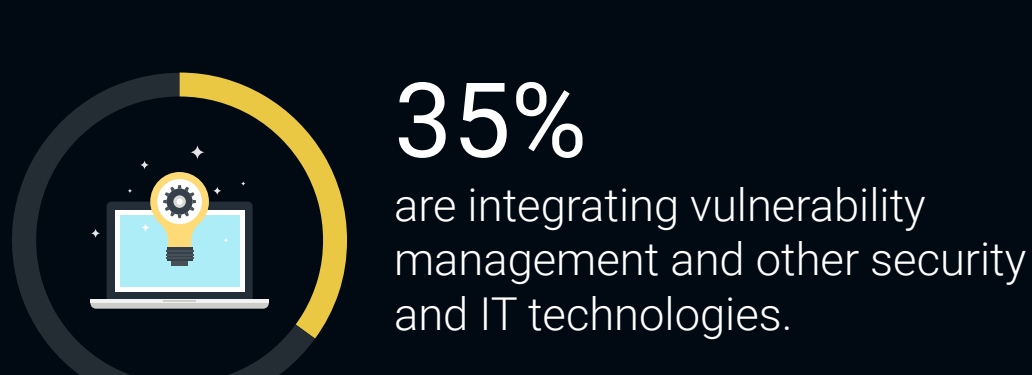
The Need for Efficient Remediation

While organizations have security testing and scanning in place to find vulnerabilities, they need a way to prioritize remediation when they have a high volume of vulnerabilities that have been found. For example, when there is a 0-day vulnerability, such as in the case of the Log4j CVE, organizations need to immediately find the instances of the vulnerability, with an understanding of their exposure to attack, to quickly remediate the vulnerability and protect their applications.

» Organizations' Vulnerability Management Challenges



» Improving Vulnerability Management Using Runtime Context



The Bigger Truth

It's important for organizations to be able to quickly respond to and remediate OSS vulnerabilities that expose them to attacks. Azul Vulnerability Detection helps customers identify and remediate Java vulnerabilities in runtime. The agentless service monitors applications for organizations with large Java footprints so they can efficiently respond to and remediate Java vulnerabilities and protect their applications from attacks.

[LEARN MORE](#)

