June 1, 2022

Research Reveals 75% of CISOs Are Worried Too Many Application Vulnerabilities Leak Into Production, Despite a Multi-Layered Security Approach

79% of CISOs say continuous runtime vulnerability management is an essential capability to keep up with the expanding complexity of modern multicloud environments

WALTHAM, Mass.--(BUSINESS WIRE)-- Software intelligence company Dynatrace (NYSE: DT) announced today the findings of an independent global survey of 1,300 chief information security officers (CISOs) in large-size organizations. The research reveals that the speed and complexity created by using multicloud environments, multiple coding languages, and open source software libraries are making vulnerability management more difficult. 75% of CISOs say that despite having a multi-layered security posture, persistent coverage gaps allow vulnerabilities into production. This highlights the growing need for observability and security to converge, paving the way toward AISecDevOps practices. This will empower organizations with a more effective way of managing vulnerabilities at runtime, and the ability to detect and block attacks in real time. The complimentary report, *Observability and security must converge to enable effective vulnerability management*, is available for download.

Findings from the research include:

- 69% of CISOs say vulnerability management has become more difficult as the need to accelerate digital transformation has increased.
- More than three-quarters (79%) of CISOs say that automatic, continuous runtime vulnerability management is key to filling the gap in the capabilities of existing security solutions. However, just 4% of organizations have real-time visibility into runtime vulnerabilities in containerized production environments.
- Only 25% of security teams can access a fully accurate, continuously updated report of every application and code library running in production in real time.

“These findings underscore that there are always opportunities for vulnerabilities to slip past security teams, regardless of how robust their defenses might be. Both new applications and stable legacy software are prone to vulnerabilities that are more reliably detected in production. Log4Shell was the poster child for this problem, and there will undoubtedly be other scenarios like it in the future,” said Bernd Greifeneder, Chief Technology Officer at Dynatrace. “It’s also clear that most organizations still lack real-time visibility into runtime vulnerabilities. The problem stems from the growing use of cloud-native delivery practices, which enable greater business agility, but also introduce new complexity for vulnerability management, attack detection, and blocking. The rapid pace of digital transformation means that already overstretched teams are bombarded by thousands of security alerts that make it impossible to see through the noise and focus on what matters. Teams find it impossible to

respond manually to every alert, and organizations are exposed to unnecessary risk by allowing vulnerabilities to escape into production."

Additional findings include:

- On average, organizations receive 2,027 alerts of potential application security vulnerabilities each month.
- Less than a third (32%) of the application security vulnerability alerts organizations receive each day require action, compared to 42% last year.
- On average, application security teams waste 28% of their time on vulnerability management tasks that could be automated.

"Organizations realize that to manage vulnerabilities in the cloud-native era effectively, security must become a shared responsibility. The convergence of observability and security is critical to providing development, operations, and security teams with the context needed to understand how their applications are connected, where the vulnerabilities lie, and which need to be prioritized. This accelerates risk management and incident response," continued Greifeneder. "To be truly effective, organizations should look for solutions that have AI and automation capabilities at their core, enabling AISecDevOps. These solutions empower their teams to quickly identify and prioritize vulnerabilities at runtime, block attacks in real time, and remediate software flaws before they can be exploited. This means teams can stop wasting time in war rooms or chasing false positives and potential vulnerabilities that will never make it into production. Instead, they confidently deliver better, more secure software faster."

The report is based on a global survey of 1,300 CISOs in large-size organizations with more than 1,000 employees, conducted by Coleman Parkes and commissioned by Dynatrace in April 2022. The sample included 200 respondents in the U.S., 100 each in the UK, France, Germany, Spain, Italy, the Nordics, the Middle East, Australia, and India, and 50 each in Singapore, Malaysia, Brazil, and Mexico.

About Dynatrace

Dynatrace (NYSE: DT) exists to make the world's software work perfectly. Our unified software intelligence platform combines broad and deep observability and continuous runtime application security with the most advanced AIOps to provide answers and intelligent automation from data at an enormous scale. This enables innovators to modernize and automate cloud operations, deliver software faster and more securely, and ensure flawless digital experiences. That is why the world's largest organizations trust the Dynatrace® platform to accelerate digital transformation.

Curious to see how you can simplify your cloud and maximize the impact of your digital teams? Let us show you. Sign up for a free 15-day Dynatrace trial.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20220601005391/en/

Meg Brenner
meg.brenner@dynatrace.com

Source: Dynatrace