May 2, 2024

Mind the Gap: Global Report Reveals Alignment Issues Between Security Teams and the C-Suite are Exposing Organizations to Increased Cyber Risk

The rise of AI-driven attacks and accelerated software delivery cycles makes it more difficult to protect organizations, as 87% of CISOs say application security remains a blind spot

WALTHAM, Mass.--(BUSINESS WIRE)-- Dynatrace (NYSE: DT), the leader in unified observability and security, released its annual CISO survey today. This year's report, "The state of application security in 2024", reveals that organizations are struggling with internal communication barriers, which hinder their ability to address cybersecurity threats. The results indicate that CISOs find it difficult to drive alignment between security teams and the C-suite, leaving gaps in the organization's understanding of cyber risk. As a result, they find themselves more exposed to advanced cyber threats, at a time when AI-driven attacks are on the rise.

In this year's report, Dynatrace explored these communication gaps to better understand how a unified approach to observability and security can help teams collaborate more effectively and reduce exposure to risk.

Key findings include:

- **Lack of C-level and board alignment leads to cyber risks:** CISOs struggle to drive alignment between security teams and the C-suite, with 87% of CISOs saying application security is a blind spot at the CEO and board level.
- **Security teams are too technical:** Seven out of ten C-suite executives interviewed say security teams talk in technical terms without providing business context. However, 75% of CISOs highlight the issue is rooted in security tools that cannot generate insights that C-level executives and boards of directors can use to understand business risks and prevent threats.
- **AI is driving more advanced cyber threats:** Addressing this technology and communications gap is becoming more critical as the rise of AI-driven attacks and cyber threats significantly increase business risk.

Against this backdrop, nearly three-quarters (72%) of CISOs say their organization has experienced an application security incident in the past two years. These incidents carry significant risk, with CISOs highlighting the common consequences they've experienced, including impacted revenue (47%), regulatory fines (36%), and lost market share (28%).

"Cybersecurity incidents can have devastating consequences for organizations and their customers, so the issue has rightfully become a critical board-level concern," said Bernd Greifeneder, Chief Technology Officer at Dynatrace. "However, many CISOs are struggling

to drive alignment between security teams and senior executives because they're unable to elevate the conversation from bits and bytes to specific business risks. CISOs urgently need to find a way to overcome this barrier and create a culture of shared responsibility for cybersecurity. This will be critical to improving their ability to respond effectively to security incidents and minimize their risk exposure."

Additional research findings include:

- The need to drive closer engagement between security teams and the C-suite is becoming more important as the rise of AI exposes organizations to added risk. CISOs are concerned about AI's potential to enable cybercriminals to create new exploits faster and execute them on a broader scale (52%). They are also concerned about AI's potential to allow developers to accelerate software delivery with less oversight, leading to more vulnerabilities (45%).
- As they look for a solution, 83% of CISOs say DevSecOps automation is more important to manage the risk of vulnerabilities introduced by AI. Additionally, 71% of CISOs say DevSecOps automation is critical to ensuring reasonable measures have been taken to minimize application security risk.
- A further 77% of CISOs say current tools such as XDR and SIEM solutions cannot manage cloud complexity, as they lack the intelligence needed to drive automation at scale, and an additional 70% of CISOs say the need for multiple application security tools drives operational inefficiency due to the effort needed to make sense of disparate sources of data.

"The growing use of AI is a double-edged sword, creating efficiency gains for both digital innovators and those seeking to breach their defences," continued Greifeneder. "On the one hand, there's a greater risk of developers introducing vulnerabilities through AI-generated code that has not been adequately tested, and on the other, cybercriminals can develop more automated and sophisticated attacks to exploit them. Adding further pain, organizations also need to comply with new and emerging laws and regulation, such as SEC rules that require public companies to disclose material cybersecurity incidents within four business days of a determination. Organizations urgently need to modernize their security tools and practices to protect their applications and data from modern, advanced cyber threats. We believe the most effective approaches will be built on a unified platform that drives mature DevSecOps automation and harnesses AI to deal with distributed data at any scale. These platforms will have the ability to provide insights that the entire business can rally behind and can be used to help with legal and regulatory compliance."

The complimentary report, *The state of application security in 2024: The imperative of driving closer alignment among the CISO, CEO, and board*, is available for download.

This report is based on a global survey of 1,300 CISOs and ten interviews with CEOs and CFOs in enterprises with over 1,000 employees. It was commissioned by Dynatrace and conducted by Coleman Parkes between March and April 2024.

About Dynatrace

Dynatrace (NYSE: DT) exists to make the world's software work perfectly. Our unified platform combines broad and deep observability and continuous runtime application security with Davis® hypermodal AI 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's 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 15-day Dynatrace trial.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20240502425390/en/

Investor Contact:
Noelle Faris
VP, Investor Relations
Noelle.Faris@dynatrace.com

Media Relations:
Jerome Stewart
VP, Communications
Jerome.Stewart@dynatrace.com

Source: Dynatrace