radware

Protecting APIs and Securing Applications So Business Can Thrive

Application development and production has never been more amorphic, and businesses have never been at greater risk. The cloud, adoption of APIs and the increasing loss of visibility into security has left apps increasingly vulnerable. Radware's latest application research underscores the gravity of the situation.

A Disconnect Between Application Development and Application Security

92% of organizations, security staff have no say regarding the continuous integration/ continuous deployment architectures

In 89% of companies, information security teams do not own budget for security solutions **89%**

A Different Threat Landscape

APIs are the new big threat to application security

<50%

Over half of applications at 40% of companies are exposed to the internet or third-party services via APIs

55%

say API security is now a "top priority"

59%

want to "invest heavily" in it in 2021

New Use For An Age-Old Cyberattack

Long used as a network-level cyberattack, DDoS is now the most common attack vector against apps

89% of respondents have experienced a

DDoS

attack targeting their web apps

HTTP/S

floods are the most frequent application-layer DDoS attacks

Mobility = Insecurity

A global pandemic increased the reliance on mobile applications but mobile application development is far less secure

36%

Only 36% of apps have fully integrated security built into them

42%

have security "bolted-on"

22%

have none

As data and apps migrate to the cloud and developers increasingly rely on APIs to integrate, ensuring security and data integrity becomes more challenging.

Read the 2020-2021 State of Web Application & API Protection Report to learn how to overcome these challenges