

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

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

A Different Threat Landscape

APIs are the new big threat to application security



at 40% of companies are



say API security is now a "top priority"

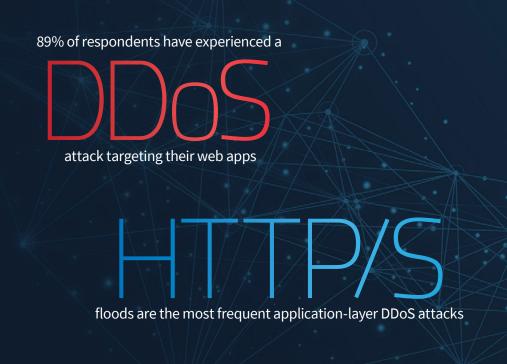


in it in 2021



New Use For An Age-Old Cyberattack

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



Mobility = Insecurity

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

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

have security "bolted-on"

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

and pending patent applications of Radware in the U.S. and other countries. For more details, please see: https://www.radware.com/

LegalNotice/. All other trademarks and names are property of their respective owners.