

A close-up photograph of a hand typing on a white computer keyboard. A magnifying glass is positioned over the keys, highlighting the letter 'A'. The image is overlaid with a purple semi-transparent banner on the left side containing the title text. The background is a blurred wooden desk.

HIMSS Survey Uncovers Critical Weaknesses In Hospital Web Security

HIMSS Analytics

 **Akamai**
FASTER FORWARD

HIMSS Analytics, in partnership with Akamai, recently conducted a survey of U.S. hospitals to understand the current state of web security in healthcare as well as what plans are in place to improve preparedness.

The results raise some concerns that despite greater consciousness of the increased risk to healthcare data security, many hospitals are still vulnerable to a wide range of cyberattacks. Hospitals clearly understand their security risks but do not agree on how best to address them — and in many cases are significantly under-protecting their organization.

For instance, only 61% of healthcare organizations have an on-premise Web Application Firewall installed to protect their data center. This means that a full 39% of organizations are not protected by the most traditional line of defense against web application attacks.

Additionally, only 42% have implemented DDoS protection solutions, with only another 13.2% planning to implement such a solution. This leaves 35% of healthcare organizations vulnerable to a type of cyberattack that is increasing in frequency and size across all industries, including healthcare, and is a significant threat to network availability.

But in the area where some of the cybersecurity threat could be mitigated – with cloud WAF solutions – only 21% of respondents say they have one, and only 16.5% intend to implement one. That 16.5% is mostly comprised of only very large hospitals, when in fact hospitals of all sizes have the same level of vulnerability to cyberattack.

While the number is relatively low, 23% of healthcare organizations responded that they have no web security programs in place at all. What makes this even more concerning is that nearly half of those respondents are from hospitals with 200 beds or more.

Healthcare organizations seem to understand part of the cause of their vulnerability, with 57% saying that they “Somewhat Agree”, “Agree”, or “Strongly Agree” with the statement “Requirements for interoperability with entities and systems outside of my organization’s network is a security issue my organization faces.” But perhaps the most discouraging result involves how well-protected respondents think they are: 61% of respondents said that they “Somewhat Agree”, “Agree”, or “Strongly Agree” with the statement “My organization is adequately protected against web application attacks.”

Overall, the survey indicates a troubling reality relating to cybersecurity in healthcare: Since web-based attack methods become more pervasive as the healthcare industry becomes more connected, healthcare organizations need to increase their sense of urgency and their investment in implementing fundamental web security solutions.

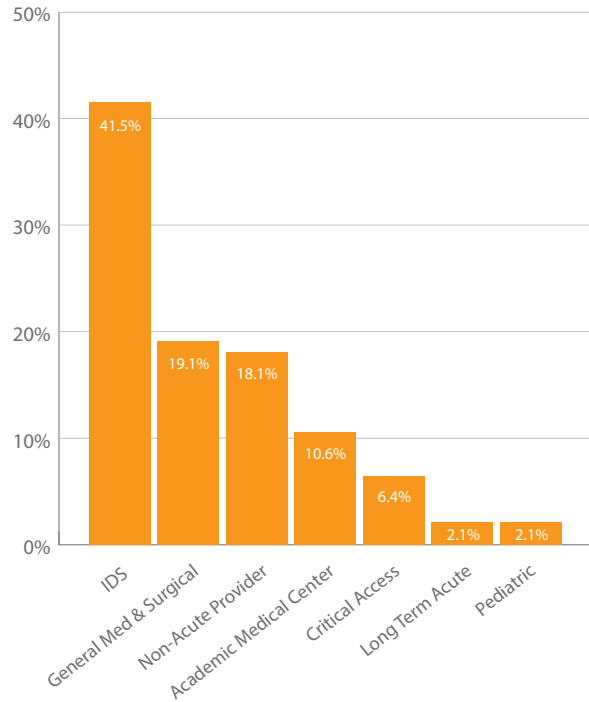
Total number of respondents: 94

Respondent Roles: CIO, CSO, Director of Technology, IT Director, IT Security Officer, Chief Compliance Officer

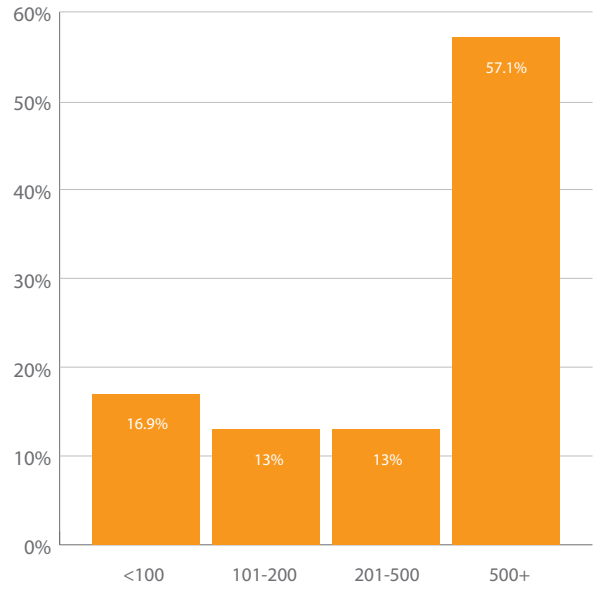
Organizations Surveyed: IDS organizations, General Medical & Surgical Hospitals, Academic Medical Centers, Critical Access Hospitals, Long-Term Acute Hospitals, Pediatric Hospitals.

Survey Results

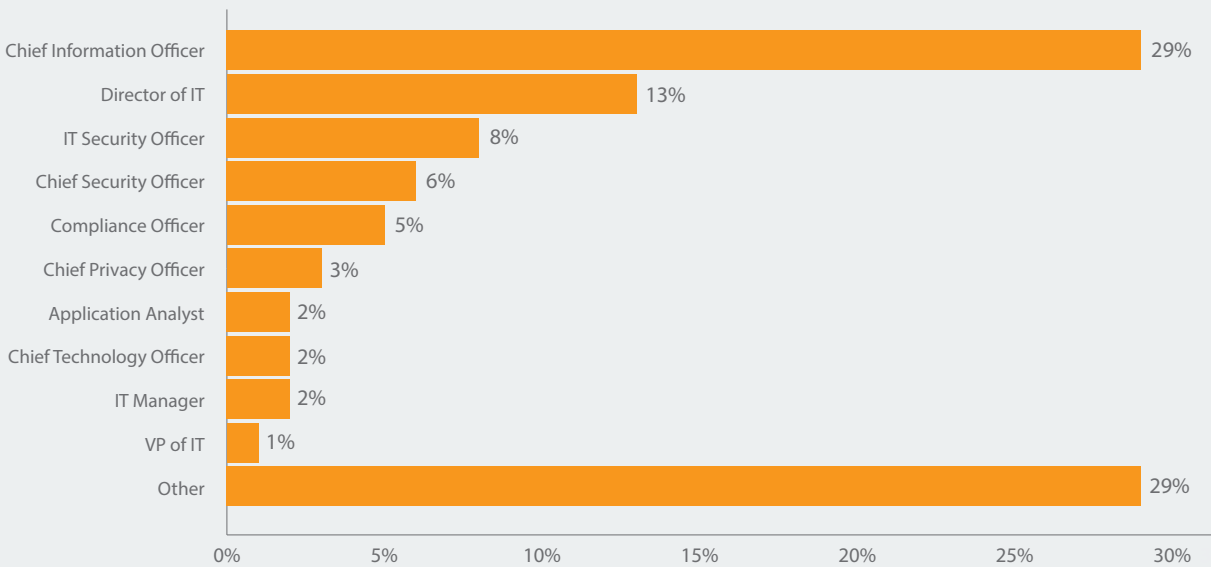
Organization Type



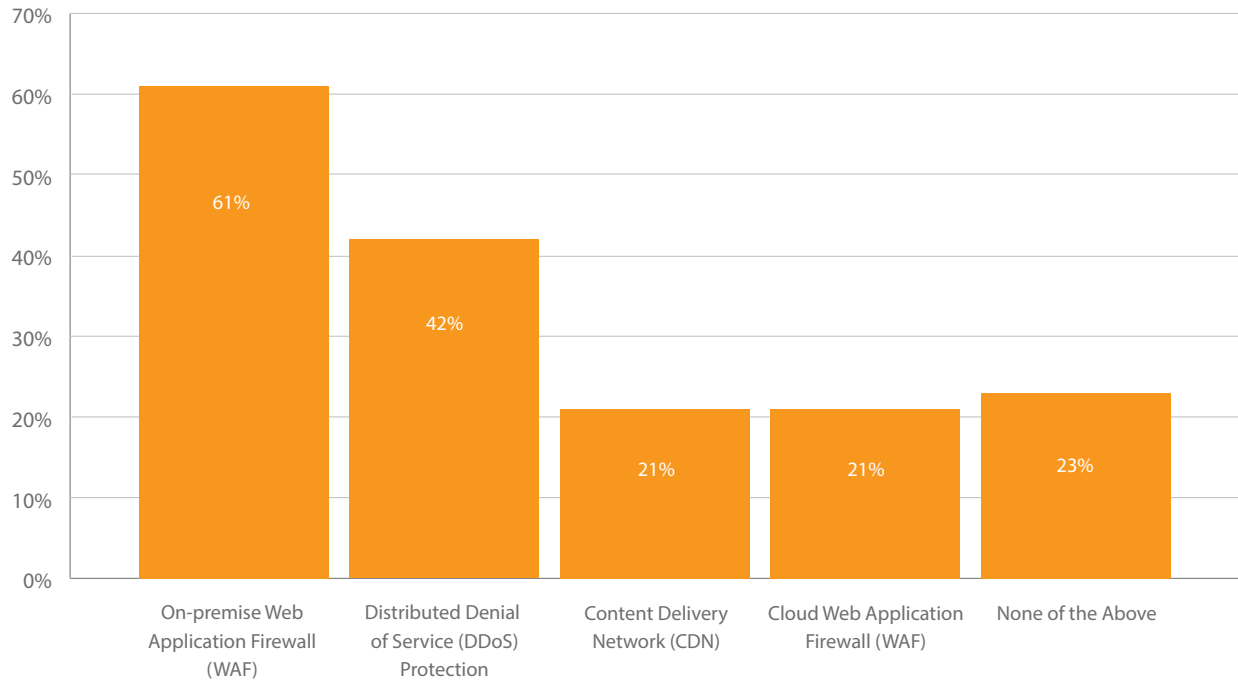
Organization Bed Size



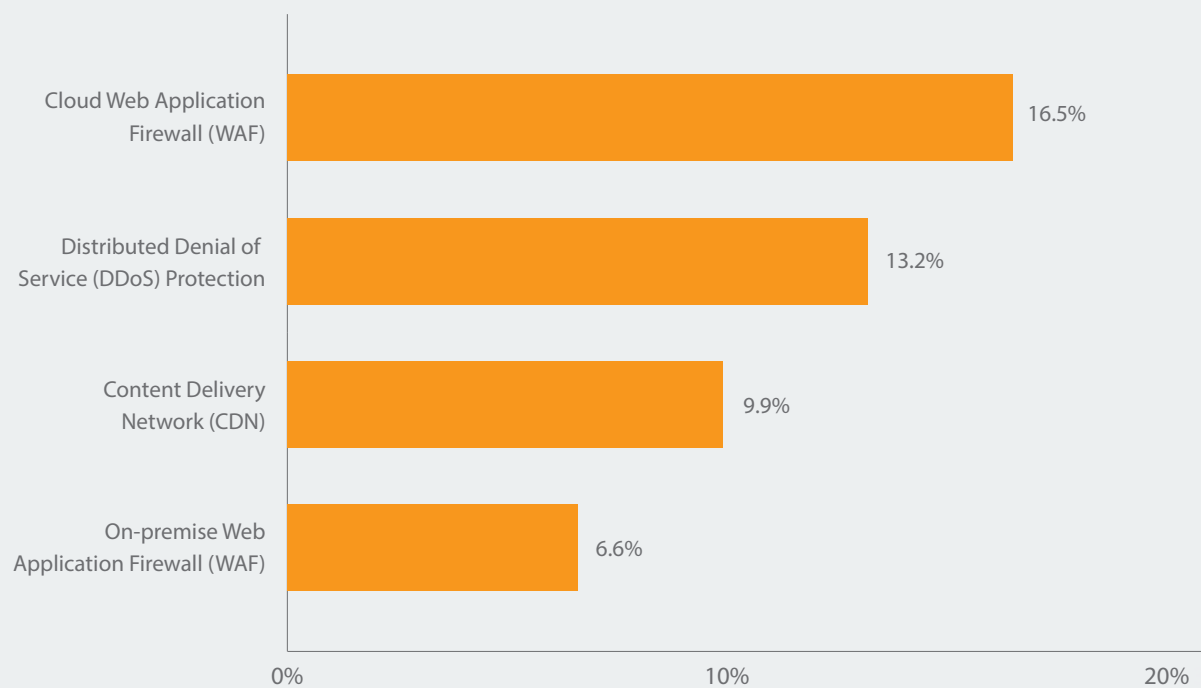
Respondent Role



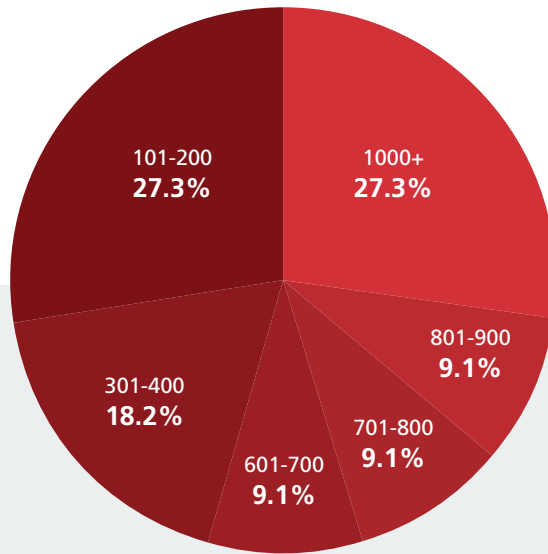
Which of the following does your organization currently use?



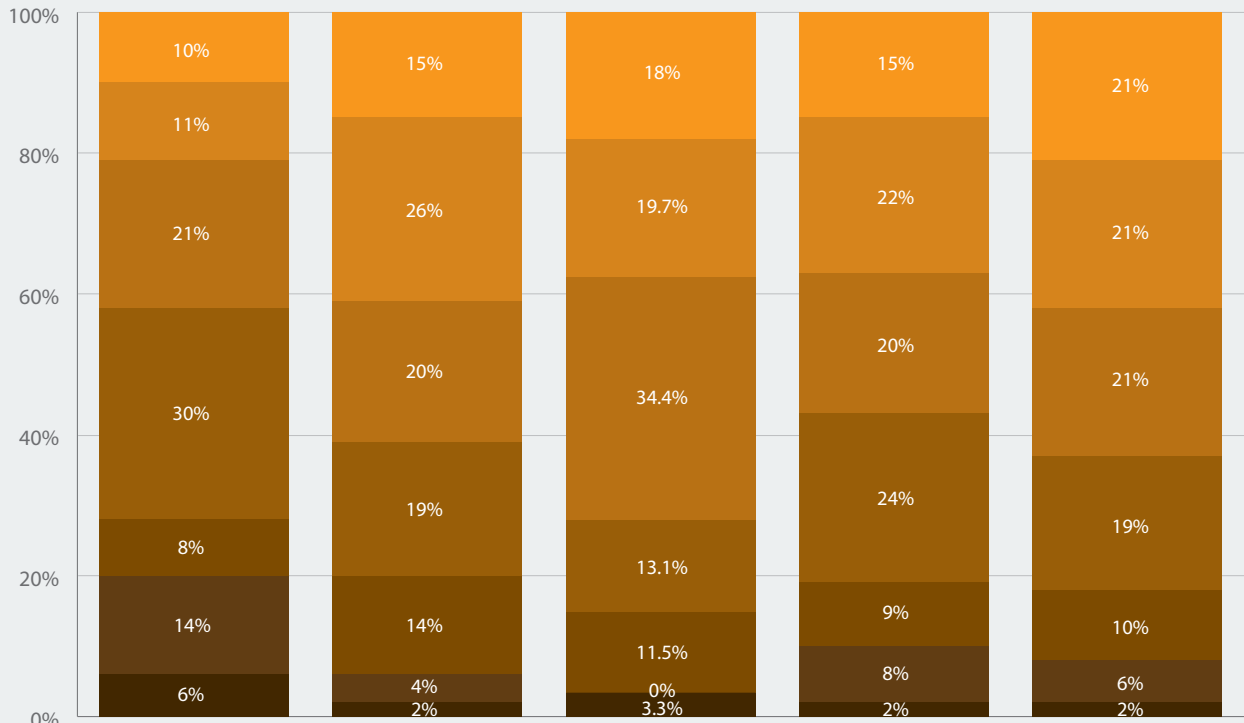
Of the solutions you do not currently have implemented, which does your organization have plans to implement?



Cloud WAF Plans by Bed Size



Please rate your level of agreement on the following statements



My organization's public web presence is a potential target for DDoS attacks

My organization is adequately protected against web application attacks

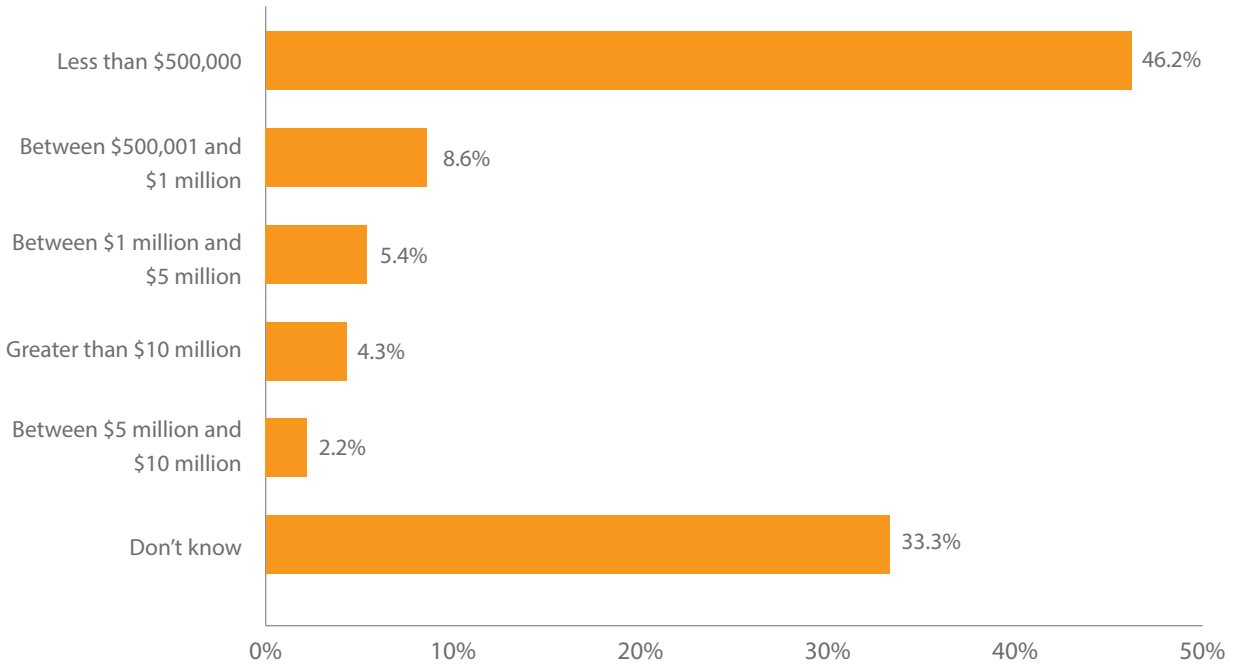
My organization's on-premise WAF is providing optimal web application security

Requirements for interoperability with entities and systems outside my organization's network is a security issue

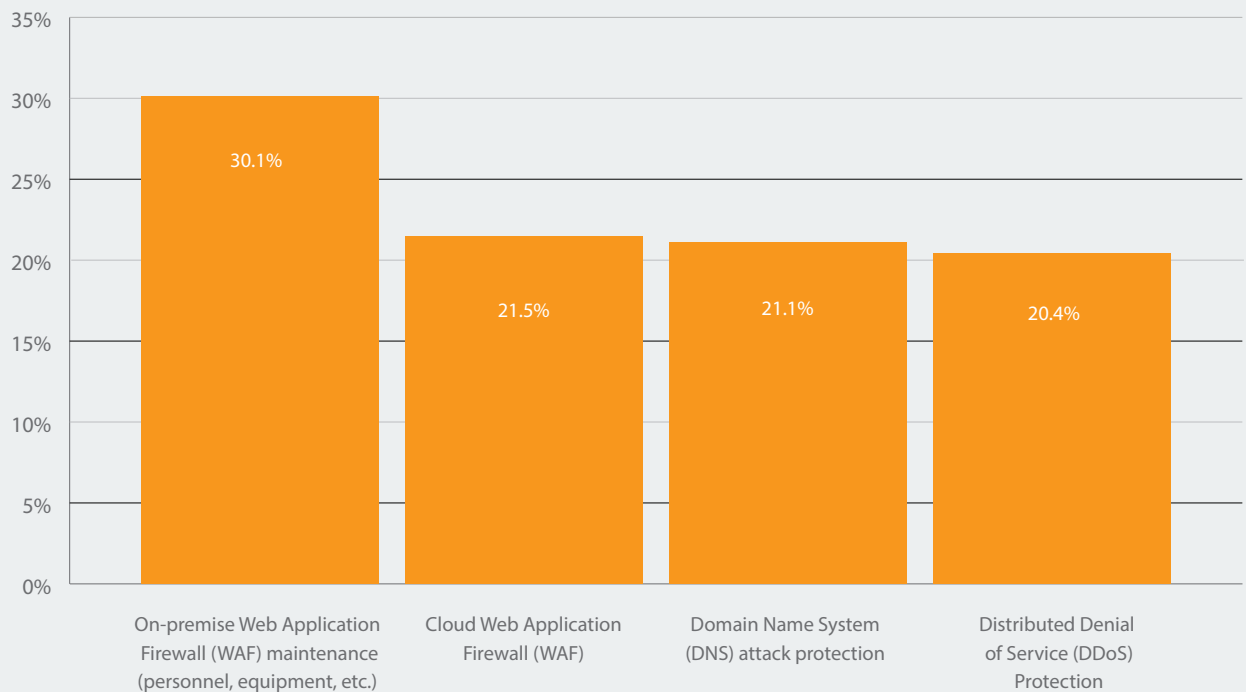
The performance and reliability of my public-facing website is a priority for my organization

- Strongly Agree
- Agree
- Somewhat Agree
- Neither Agree or Disagree
- Somewhat Disagree
- Disagree
- Strongly Disagree

What is your total cyber threat security budget for your organization's current fiscal year?



For each category below, please indicate the approximate percent of the total cyber threat security budget allocated to that category.





As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company's advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.

©2015 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice. Published 11/15.