Enterprise Strategy Group™ by TechTarget

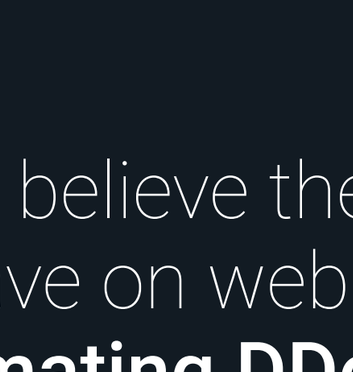
Balancing Requirements for Application Protection

Application environments are more complex than ever, with web applications increasingly cloud-resident, containerized, connected via APIs, and delivered via CDNs. On top of this increasingly heterogeneous environment, security responsibility is distributed across a variety of roles and personas. This has resulted in complexity and tool sprawl as security teams struggle to keep pace, with attackers understanding this and using it to their advantage. TechTarget's Enterprise Strategy Group recently surveyed IT and cybersecurity professionals to gain insights into these trends.

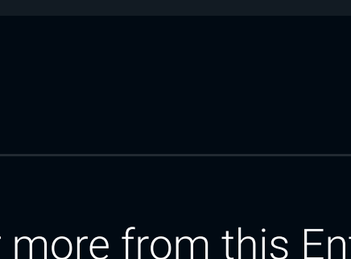
Notable findings from this study include:

46%
of organizations say protecting their public-facing web applications and APIs is **more difficult than it was 24 months ago.**

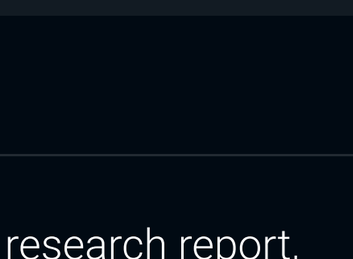
38%
of organizations that suffered attacks on their web applications and APIs experienced downtime.



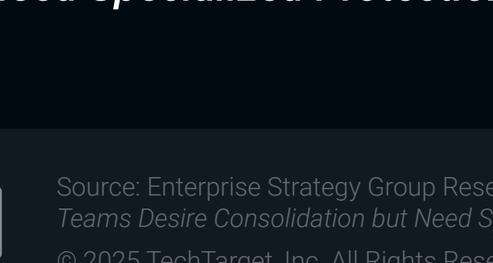
75%
of organizations say they use bot management and mitigation tools from specialized vendors.



70%
of organizations that experienced a diversionary denial-of-service attack indicated it was successful.



91%
of organizations say consolidating web application firewall vendors is an important or critical priority.



50%
of organizations believe the biggest impact AI will have on web application security is **automating DDoS mitigation**.

For more from this Enterprise Strategy Group study, read the full research report, ***Balancing Requirements for Application Protection: Teams Desire Consolidation but Need Specialized Protection.***

Learn More

Source: Enterprise Strategy Group Research Report, *Balancing Requirements for Application Protection: Teams Desire Consolidation but Need Specialized Protection*, April 2025.