Reblaze

2022 State of Web Security Survey

March 2022

Reblaze

Table of Content

Introduction and Key Findings

Introduction

In the first half of 2021 alone, **bot-driven cyberattacks grew 41%**, while human-initiated attacks actually dropped 29% year on year. It's well documented that cybercrime has leapt since the advent of COVID-19, but how are today's security teams arming themselves against the realities of this threat?

To understand how organizations are approaching web security as we start 2022, we went straight to the source, the CISOs, CIOs and Information Security and DevOps leaders themselves. We asked them, what were your greatest threats in 2021 and where are you channeling your budget and attention for 2022?

The results shine a light on the true state of web security in today's organizations. Companies are increasingly reliant on the cloud, and are using a mix of different technologies to compete with larger players in the market. Half of respondents have no idea how much of their traffic comes from hostile bots – while almost all of the other 50% radically underestimate the problem.

As security leaders recognize that their visibility and control are dangerously low, they are increasingly turning to new technologies, with two thirds of companies increasing their security budget for 2022, and Adaptive Protection considered the most important technology overall.

Methodology

To collect this essential industry insight, we commissioned this survey of 300 respondents from the US, EU, and APAC. These respondents ranged from CISOs and CIOs, to those working in Information Security, DevOps and DevSecOps teams, from small companies (1-50 employees) to large (over 5,000). The survey was completed by Global Surveyz, an independent survey company, and took place during Q4 2021.

The respondents were invited via email to complete the survey, with the average amount of time spent on the survey 6 minutes and 41 seconds. The answers to the majority of the non-numerical questions were randomized, in order to prevent order bias in the answers.

Key Findings

01

The Most Common Attack of 2021 was DDoS

DDoS was the most common attack in 2021, with half of respondents reporting DDoS attempts. For most regions, SQL injection was next at 38%, and ransomware was third at 29%. However, in the US there is a more severe ransomware problem, and 40% of the US respondents were targeted by ransomware attacks in 2021.

02

Cloud-Based Security is Growing

Companies have embraced cloud-based security technologies. 64% of respondents now use a native WAF from their cloud provider, while third-party WAFs and Unified Solutions are also popular, at 41% and 24% respectively. This reliance is growing, as 59% of respondents plan to adopt more cloud security solutions in 2022.

03

Non-Traditional Security Technologies Are Becoming Important

72% of companies consider it very important to secure the OWASP Top 10 vulnerabilities — most of which are long-standing issues within web security. However, companies are also seeking other new types of defenses. 99% of respondents consider Adaptive Protection to be important, followed by API security at 98%.

04

Most Companies Have Inadequate Defenses Against Hostile Bots

Modern attack bots have become quite sophisticated, and for most security solutions, are difficult to detect. While 50% of respondents have no idea about the percentage of hostile bots in their traffic, the other half think they know, but tend to radically underestimate the number, at an average of 6.2%. In reality, the percentage is closer to 26%.

05

The Fastest-Growing Security Technologies Are Bot Solutions and Unified Solutions

With so many companies unable to accurately ascertain the composition of incoming traffic, it's no surprise that the security technology with the highest expected growth rate is Dedicated Bot Solutions. Various sizes of company report increased usage of between 133% and 214% in 2022 over their current rates. The second-highest growth item is Unified Solutions, where companies expect usage rates of up to 150% over 2021 levels.

Threat Environment

Types of Cyberattacks Experienced in 2021

DDoS was the most common attack in 2021, with half of respondents reporting DDoS attempts.

The next-most common threats are SQL injection at 38% and ransomware at 29%, except for companies within the US, where ransomware (at 40%) is the more severe threat. This probably reflects the high perceived value among hackers for successful ransomware infections within the US. (According to the Treasury Department, ransomware payouts from US firms in the first half of 2021 alone were $590 million.)

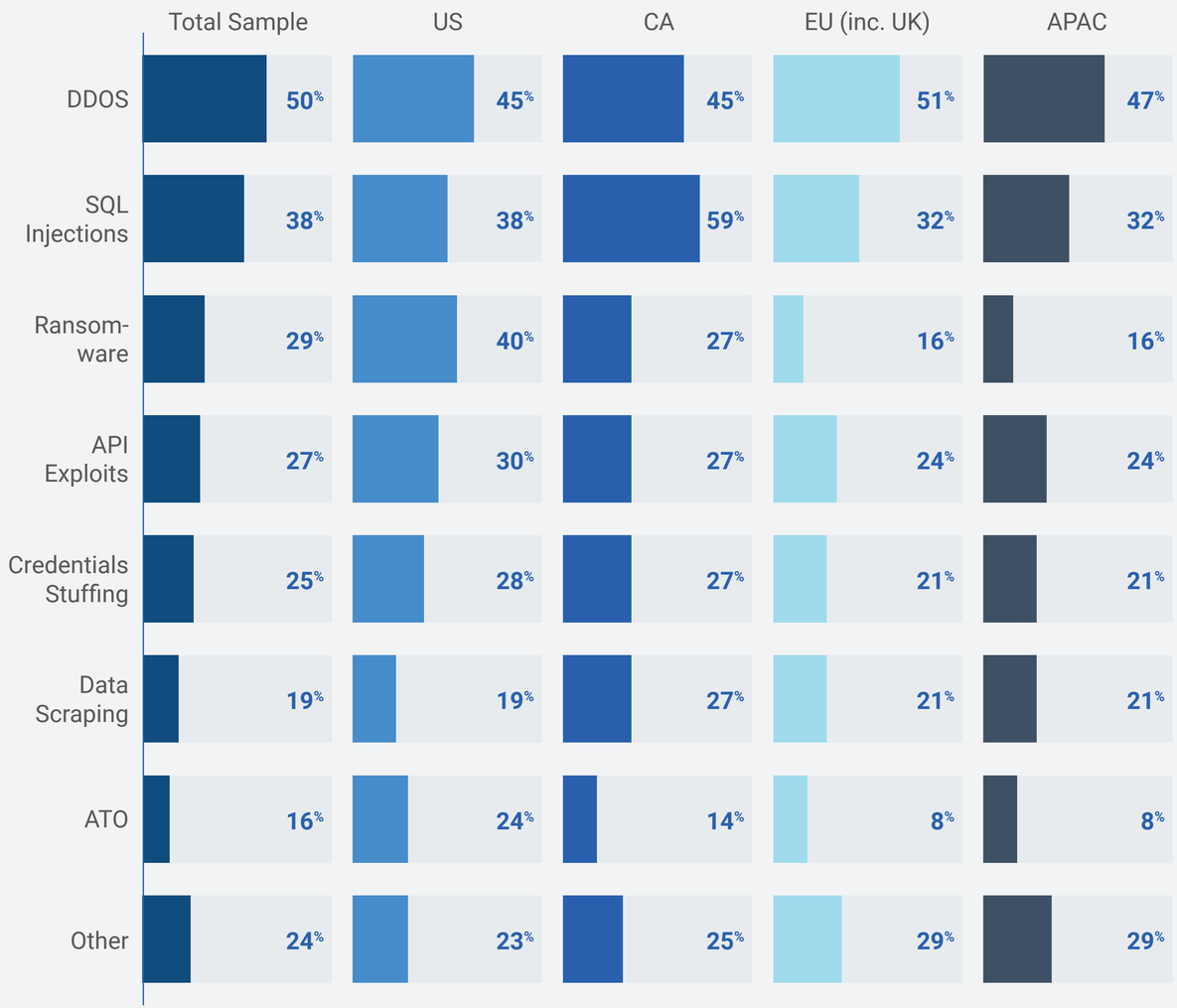

Figure 1 Types of Cyberattack Experienced

Bots Proliferation in Traffic

Half of respondents don’t know the number of bots in their traffic. The others estimate their bot traffic at various levels, with an overall average of 6.2%.

This mirrors the current state of web security solutions. While some solutions don’t offer bot mitigation at all, others only offer it with limited scope (only for web applications and not for APIs or services). Very few solutions can reliably detect the latest generations of hostile bots, which leads to most respondents underestimating their bot traffic. **External data** puts malicious bots at around 26% of all traffic, much greater than this estimation, and correctly estimated by just 7% of respondents.

Weighted Average: 6.2%

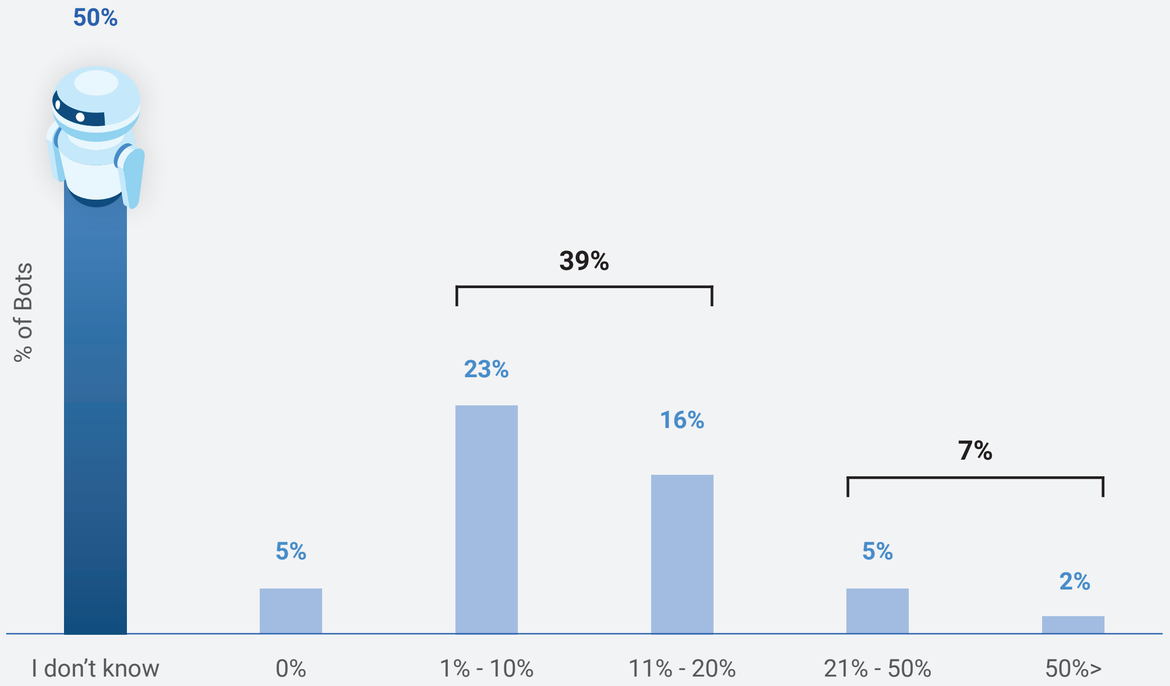

Figure 2 Bots Proliferation in Traffic

**Percentages on figure 2 do not add up to 100% due to rounding up of numbers*

Reblaze

Cloud Security Posture

Public Cloud Usage

90% of survey respondents are using a public cloud, with the top cloud vendors AWS (67%), AZURE (51%), and GCP (28%).

Multi-cloud usage is becoming more common, with 51% using more than one cloud

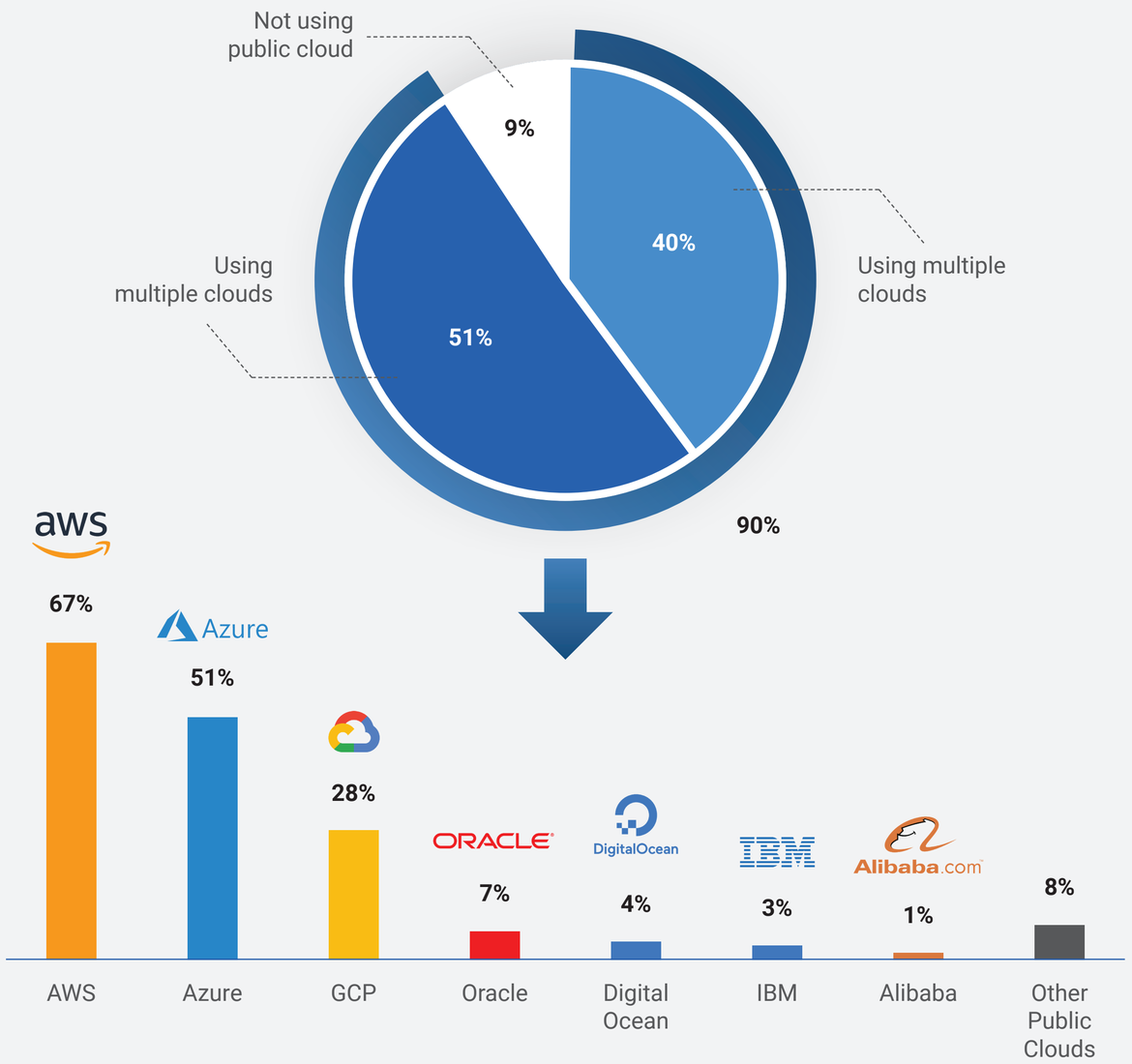

Figure 3 Public Cloud Usage

** This question allowed more than one answer and as result, percentages will add up to more than 100%*

Security Technologies in Use

All three top-tier CSPs (Cloud Service Providers) now offer their own Web Application Firewalls (WAFs), and these have become the most popular security technology, at 64% usage. CSP WAFs are easy to deploy and control, which perhaps explains their popularity among DevSecOps and SREs.

However, the CSP WAFs do not protect against all forms of web attack. Many organizations recognize this and continue to use other solutions, whether single technologies (such as 3rd Party WAFs) or all-in-one platforms (Unified Solutions that include WAF, DDoS protection, bot management, API security, etc.)

The combined usage of CSP WAFs, 3rd party WAFs, and Unified Solutions is above 100 percent, which indicates that many organizations use more than one WAF. This is probably due, at least in part, to the rising popularity of multi-cloud and hybrid architectures.

** This question allowed more than one answer and as result, percentages will add up to more than 100%*

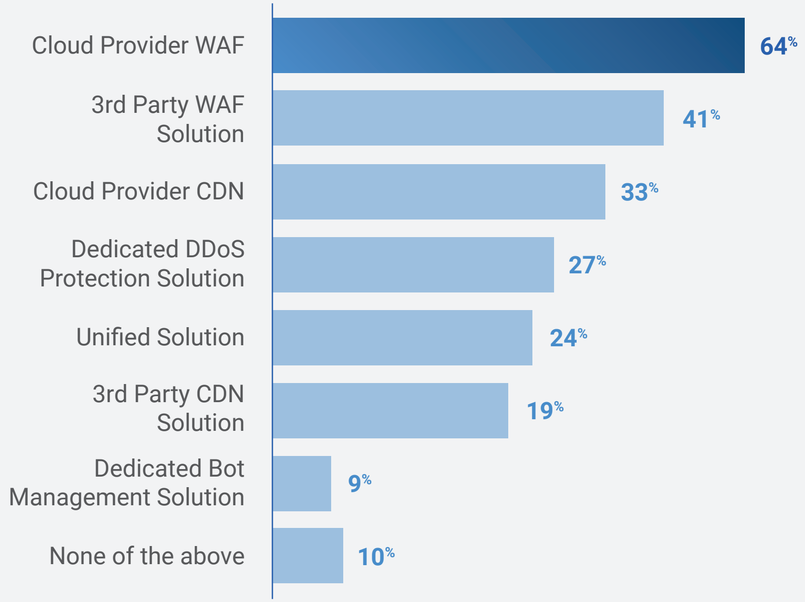

Figure 4 Security Technologies in Use, 2021

Figure 5 Use of “Cloud Provider WAF” by Role

Top Cloud WAF Technologies

The top cloud WAF* technologies named as very important are API Security, Securing the OWASP top 10, and Adaptive Protection — all with at least 70%.

For overall weight, Adaptive Protection is at the top of the list (99% indicate this technology is at least somewhat important). It's also interesting to see that respondents recognize that all these technologies are at least somewhat important; every item has a combined weight of at least 93%.

* This survey item includes all forms of cloud WAF: CSP, 3rd Party, and Unified Solutions.

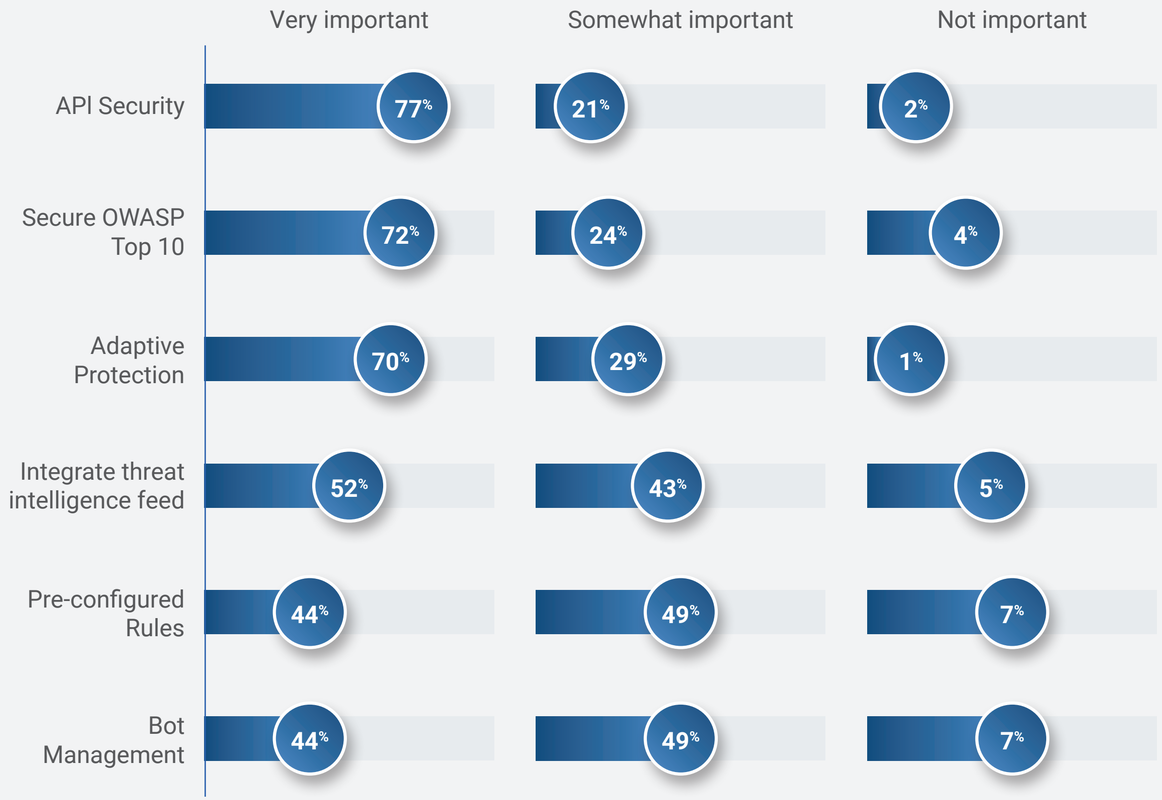

Figure 6 Top Cloud WAF Technologies

Security Plans and Investments in 2022

Security Implementation, Next 12 Months

59% of respondents expect to rely more on cloud solutions in 2022.

In figure 8, we see that the more technical the role, the more interested the respondents are in implementing mesh technology and IaC (Infrastructure as Code). This is understandable given the rising popularity of cloud-native architectures (including microservices and service meshes), and the number of organizations evolving from traditional DevOps to DevSecOps.

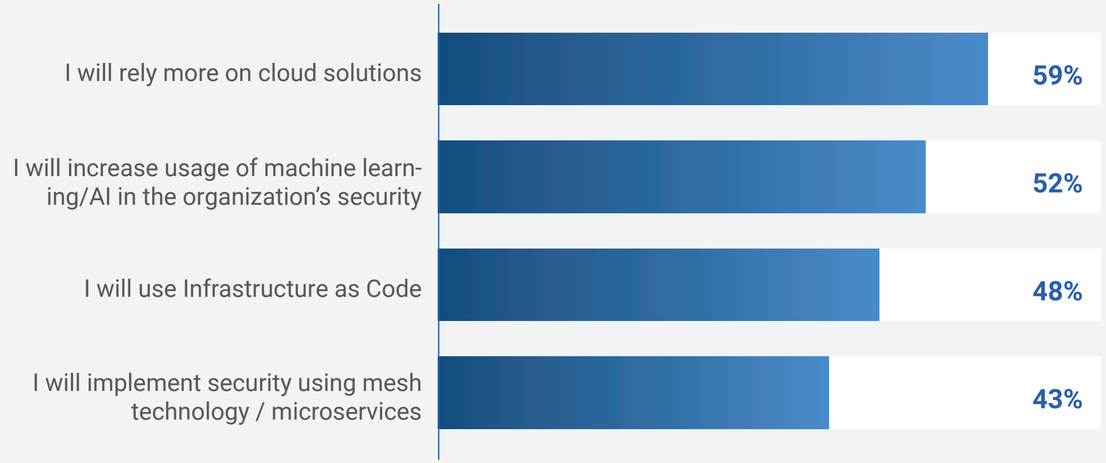

Figure 7 Security Implementation, Next 12 Months

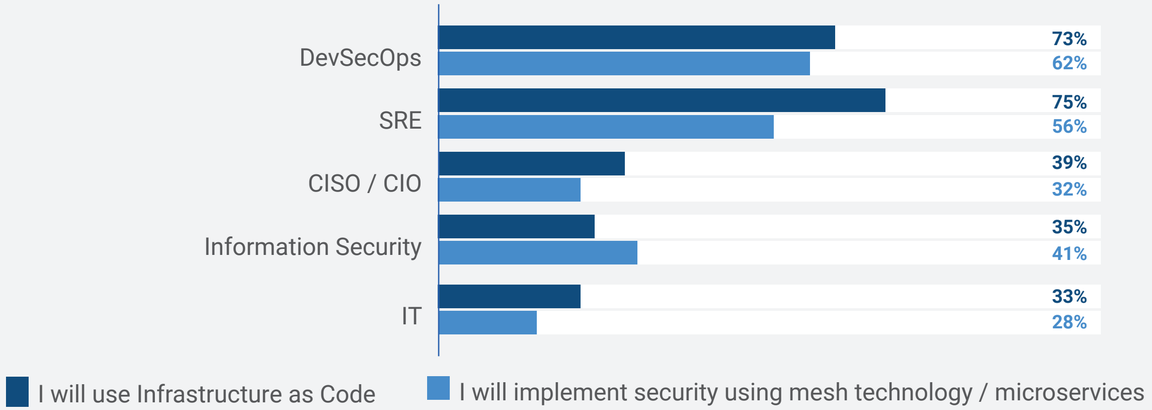

Figure 8 Selected Security Implementation by Role

Top Expected Security Technologies in 2022

The 3 top security technologies the respondents expect to use in 2022 are cloud provider WAF (60%), unified solution (31%) and cloud provider CDN (30%).

In large security teams of six or more team members, 40% of respondents expect to use a unified security solution, while this number drops to 24%-34% when looking at smaller teams of 1-6.

Larger teams are likely to use more security services as they have more security needs to cover. These teams find unified solutions a better fit for optimizing their workload and covering their requirements rather than managing multiple point solutions that can add complexity. In a one man show or a lean team, not all security services are absolutely essential.

* This question allowed more than one answer and as result, percentages will add up to more than 100%

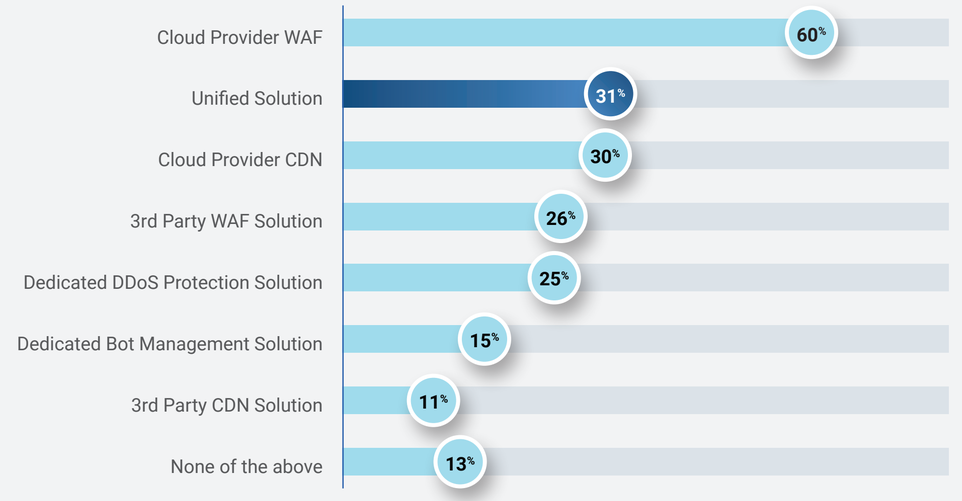

Figure 9 Top Security Technologies Expected for Use, 2022

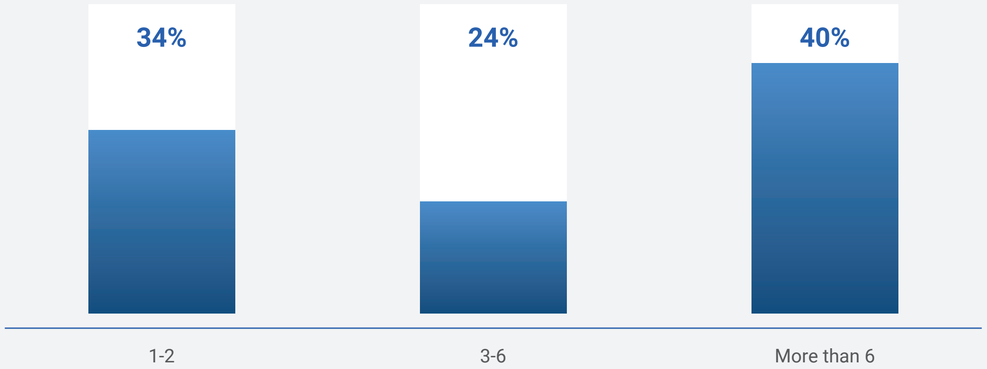

Figure 10 Expecting to Use Unified Solution by Security Team Size

Security Technologies' Expected Growth, 2021-2022

Respondents recognize that they need better detection of hostile bots in their traffic. **Dedicated Bot Management** is the technology with the highest expected growth (from 133% to 214% of current usage) across companies of all sizes.

The second-highest growth category is **Unified Solutions**, with companies expecting to increase their usage by up to 150%. Other categories were mostly flat, except for:

Cloud Provider WAF: There is an expected growth of 18% among small companies (1-50), while large (501+) and very large (5001+) companies are not displaying this. It seems that small firms are attracted by the low prices and ease of use of the CSP security tools, while larger organizations are discovering that these tools, although useful, have significant limitations.

Dedicated DDoS Protection Solutions are gaining ground among large and very large companies (with 14% and 6% anticipated growth, respectively).

CDN solutions: There is a shift in interest away from 3rd Party solutions and towards Cloud Provider CDNs. This is especially true for very large (5001+) companies, with an expected growth of 14% for Cloud Provider CDN usage.

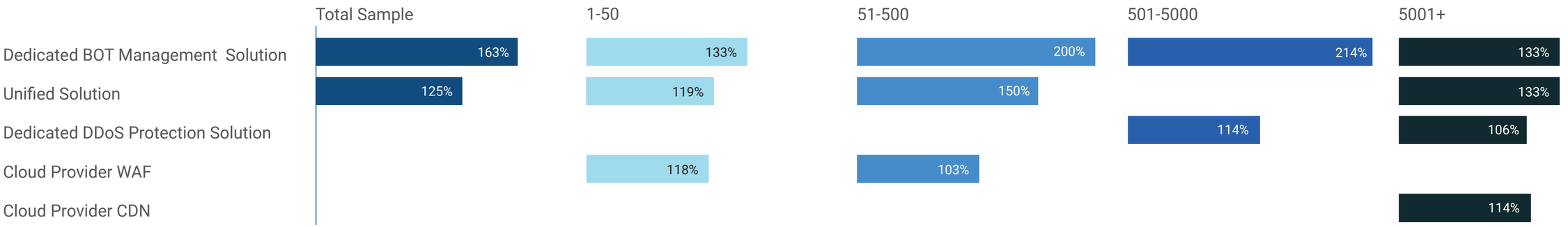

Figure 11 Strongest Responses from Security Technologies' Expected Growth, 2021-2022

Fastest Growing Technologies Over the Next 12 Months

In the next 12 months, containers will receive the most investment and resources for 53% of respondents.

Since respondents were asked to select one answer for this part of the survey, and containers are not mutually exclusive with NGNIX and Envoy, it's quite possible that the latter two will also receive more investment than is implied here.

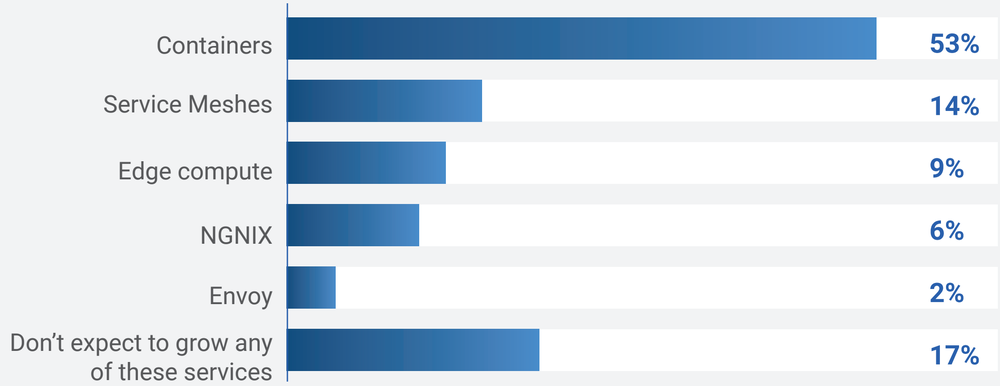

Figure 12 Fastest Growing Technologies, Next 12 Months

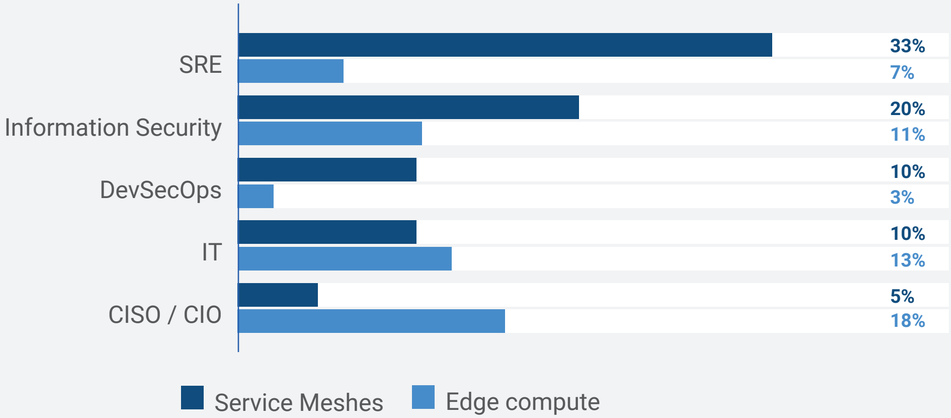

Figure 13 Selected Fastest Growing Tech by Role

* Percentages in figure 12 do not add up to 100% due to rounding up of numbers

Web Security Budget Growth, 2022

Over two-thirds (69%) of companies are expecting to grow their web security budgets and only 3% will decrease them in 2022.

On average, web security budgets are expected to grow in 2022 by 11.4% (compared to 2021).

Weighted Average: 11.4

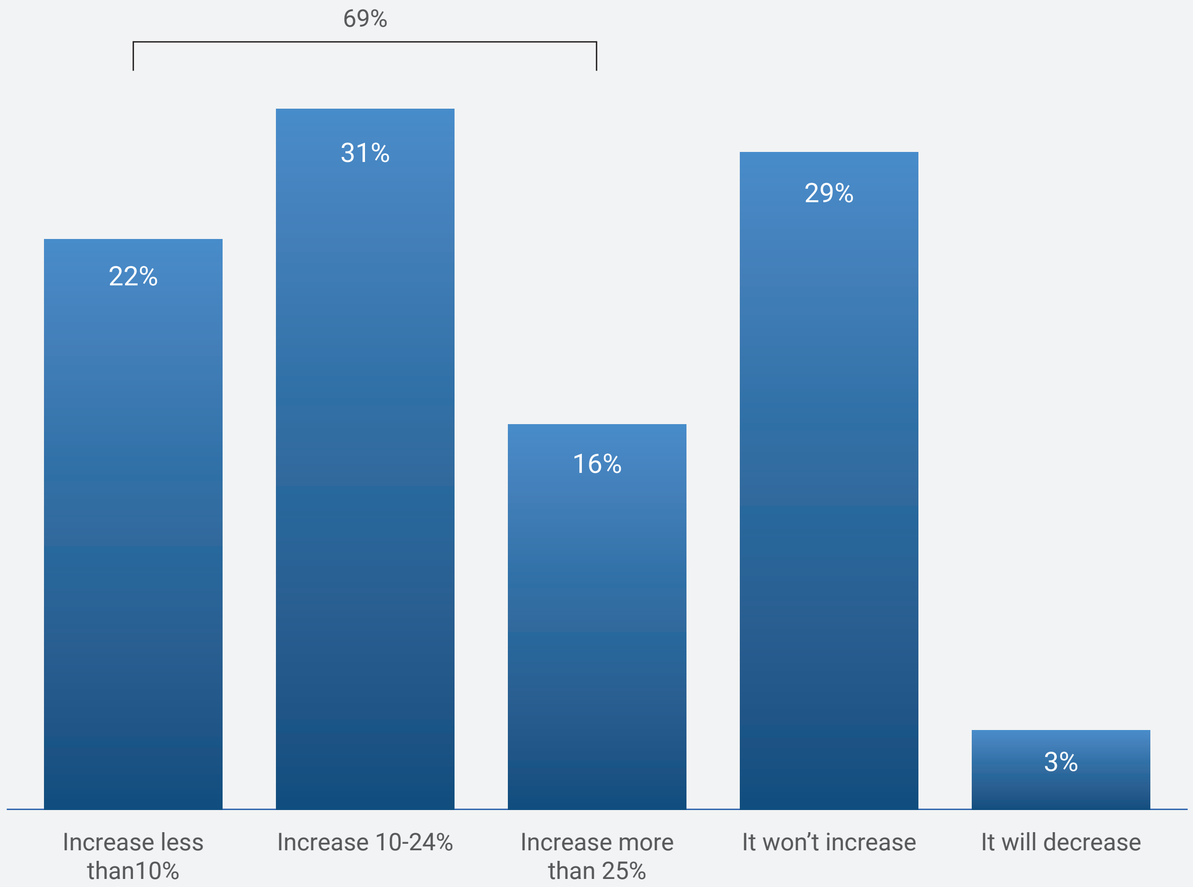

Figure 14 Web Security Budgets Growth, 2022

* Percentages in figure 14 do not add up to 100% due to rounding up of numbers

Demographics and More

Number of Websites, Domains, and Applications Owned

On average, respondents own 110 websites, domains, and applications.

Weighted Average (# of sites, domains, etc.):110.3

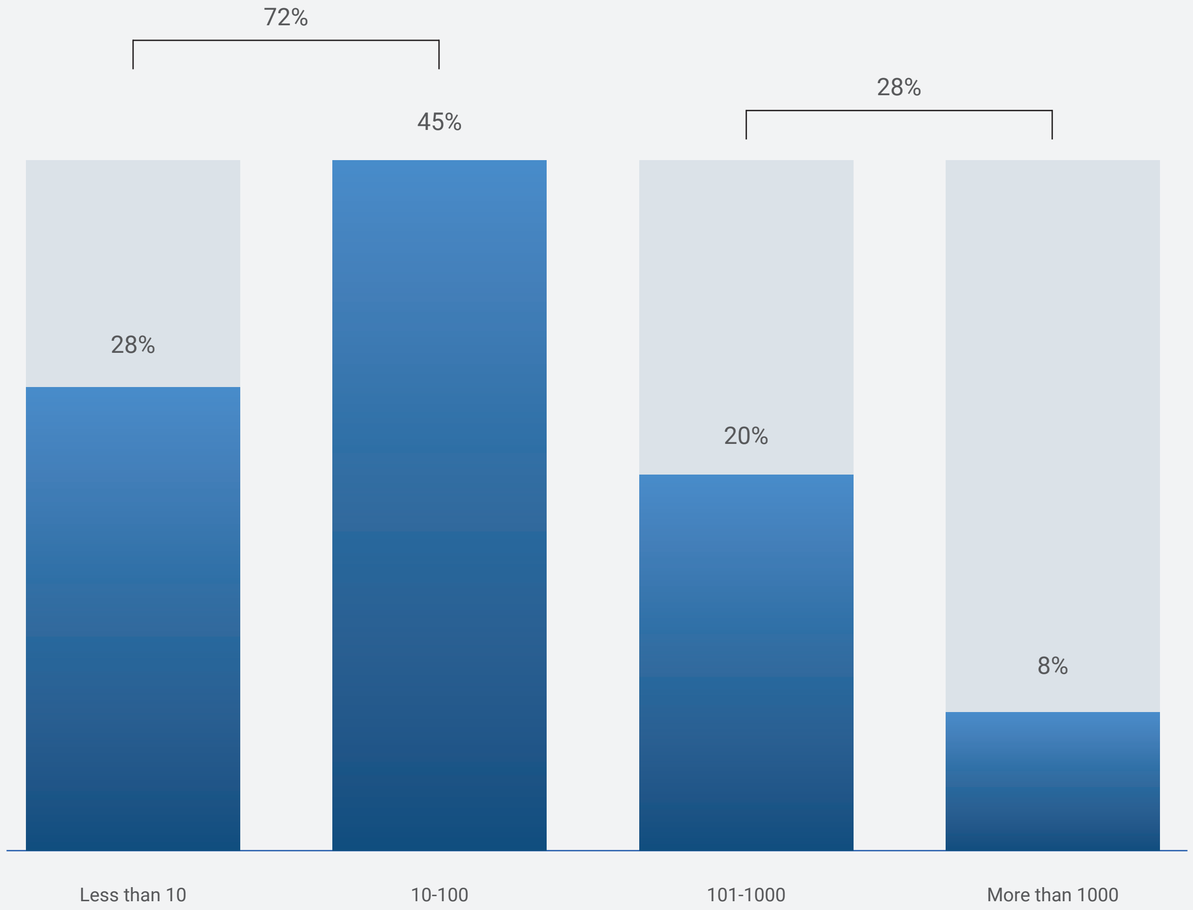

Figure 15 Number of Websites, Domains, and Applications Owned

* Percentages on figure 15 do not add up to 100% due to rounding up of numbers

Country, Role and Company Size

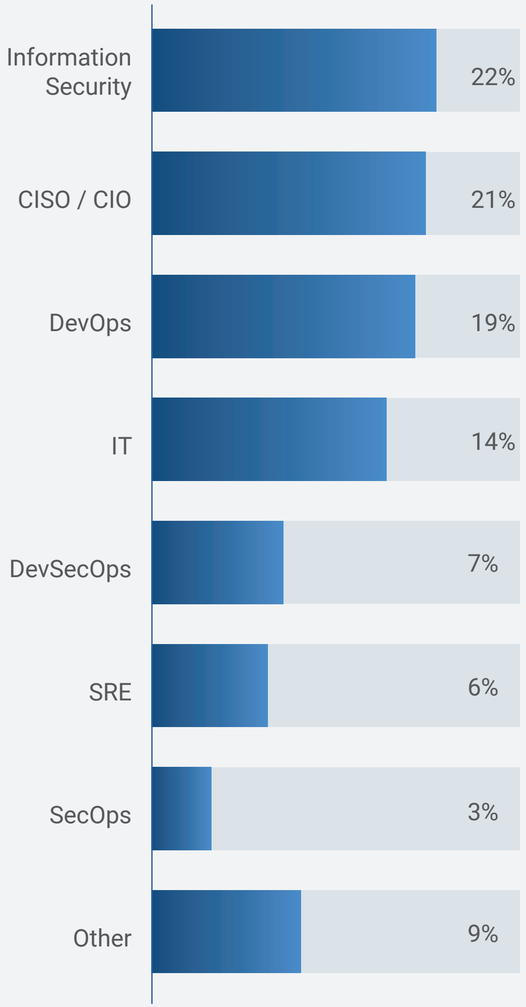

Figure 16 Role

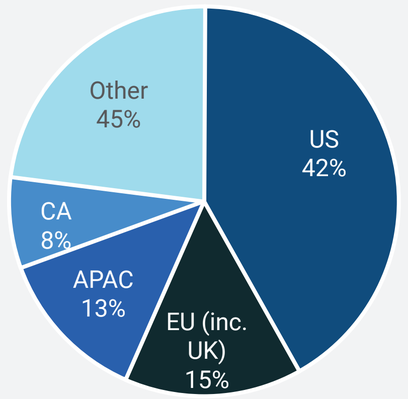

Figure 17 Country/Region

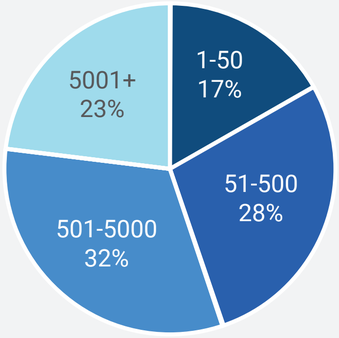

Figure 18 Company Size

Size of Security Team

On average, the size of a security team is 3.8 employees.
It is more common in the US to have a security team with more than 6 employees (43%) in comparison to other regions.
The average size of a security team in the EU is the smallest at 3.7.
The larger size in the US might reflect the greater prevalence of ransomware attacks, as discussed earlier.

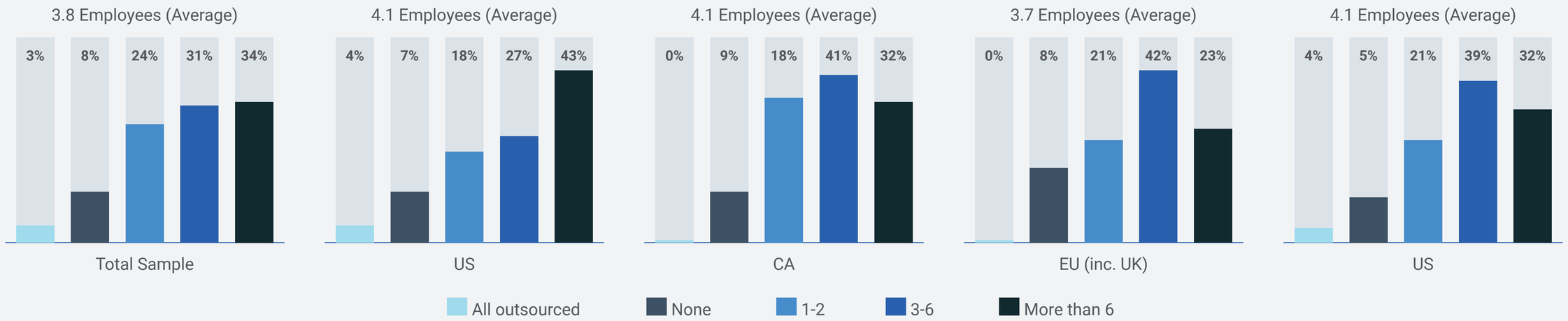

Figure 19 Size of Security Team

Solving the Issues
revealed by the survey

Reblaze: Cloud Native WAAP (Web Application and API Protection)

Reblaze

Unified All-Inclusive Security Solution

Reblaze provides complete web security; it includes next-gen WAF (Web Application Firewall), DDoS protection, bot management, API security, ATO (Account Takeover) prevention, advanced rate limiting, and more. It protects sites, services, applications, and APIs.

Runs Natively on Your Clouds of Choice

Reblaze is fully integrated with, and runs natively on, the top-tier cloud service providers (AWS, GCP, and Azure). It deploys in minutes, and supports single-cloud, multi-cloud, and hybrid architectures.

Turn-Key Web Security

Reblaze converts the native CSP security tools (AWS WAF, Google WAAP, Azure WAF, etc.) into autonomous systems which react immediately to every type of attack. Reblaze identifies hostile traffic, and the native tools immediately block it at the edges.

Maximum Performance, Complete Privacy

Other cloud security solutions route your traffic to self-owned external infrastructure, and decrypt private data outside of your environment. Reblaze runs and performs all its processing *inside* your clouds.

Defeats Hostile Bots

Other solutions use legacy techniques such as IP blacklists and CAPTCHAs; these hurt UX by interrupting user sessions, while still being unable to detect the latest generation of evasive bots. Reblaze blocks hostile bots using behavioral analysis, biometric human verification, and other advanced technologies that are invisible to legitimate users.

Adaptive Protection

Reblaze uses Machine Learning to learn from, and adapt to, the ever-changing Internet threat environment. Even as new web threats arise, Reblaze remains effective.

Unmatched Customer Experience

Reblaze is a fully managed platform, maintained for you by Reblaze's team of experts. Your web security is always up-to-date, and always effective.

About Reblaze

Reblaze is the leading provider of cloud-native web application and API protection in a fully managed security platform. Reblaze's all-in-one solution supports flexible deployment options (cloud, multi-cloud, hybrid, data center, and service mesh), deployed in minutes and includes state-of-the-art Bot Management, API Security, next-gen WAF, DDoS protection, advanced rate limiting, session profiling, and more. Unprecedented real time traffic visibility and highly granular policies enables full control of your web traffic. Machine learning provides accurate, adaptive threat detection, and dedicated VPC deployment ensures maximum privacy, performance and protection while minimizing overhead costs. Reblaze's customers include Fortune 500 companies and innovative organizations across the globe.

For more information, please visit us:

Request a Demo

Email: contactus@reblaze.com