Reblaze

How to Select

The Right Web Security Solution in 2022

Reblaze Technologies LTD

Introduction

Businesses adapt their digital infrastructure to the changing global environment. As they invest in infrastructure, they also need to consider their web security.

With business workloads, applications, services, and data exposed on open internet platforms, it is now more important than ever to invest in a web security solution that provides adequate protection against today's advanced and aggressive threats.

When evaluating web security solutions, these criteria should guide your decisions:

1. Security coverage and depth of the solution.
2. Effectiveness and sophistication.
3. Visibility into web traffic.
4. Flexible deployment options.
5. Privacy of data and isolation from other tenants.
6. Managed service and overall experience.
7. Total cost of ownership (TCO).

In this guide, we will discuss best practices for evaluating web security solutions and selecting the one that provides a holistic approach to securing your workloads, is scalable to meet future business needs, and will adapt to new threats as they emerge.

1. Security coverage and depth of the solution

Businesses will find a great variety of web security solutions available in the market. They can be classified into three categories:

- Native tools offered by the cloud service providers (CSPs).
- Single-focus products.
- Comprehensive platforms.

! **Each category offers certain benefits, but there are also weaknesses to be considered.**

Native tools:

The built-in CSP tools are simple to deploy and use. However, they won't work in multi-cloud architectures. Also, they do not provide full protection; they cover only a fraction of the wide variety of threats that are prevalent today. In addition, their automation capabilities are inadequate, and businesses run the risk of vendor lock-in.

Single-focus products:

Single-purpose products such as WAFs tend to offer more depth than CSP tools, but they have a limited scope. To mitigate the wide range of threats and vulnerabilities, organizations must purchase a collection of different solutions from different vendors. This introduces further challenges, including product interoperability, management and administrative overhead, and staff training for multiple solutions.

Comprehensive platforms:

Many of these offer adequate web security controls, but in almost all cases the platform is not offered as a unified suite. Typically, the advertised price is for a bundle of limited services; to achieve a robust security posture, customers must pay more for various add-ons (such as module upgrades, threat feed subscriptions, additional subdomains, and extra SSL certificates). Businesses end up paying more than they need to, compared to buying a more cost-effective solution.

For full protection in the current threat environment, you need a flexible, unified solution:

A comprehensive web security platform that includes a next-gen WAF, multi-layer DDoS protection, bot management, API security, ATO (Account Takeover) prevention, and more.

Look for a complete web security solution that includes:

Full-scope protection against the plethora of threats on today's Internet.

A single subscription that covers all functions, eliminating budgeting friction.

Reduced complexity, because all of your web security controls are managed under a single platform.

Highly granular policy options to meet your evolving business needs.

Flexibility, supporting vendor-independent architectures: single-cloud, multi-cloud, and hybrid.

2. Effectiveness and sophistication

Most web attacks include bots in one form or another, and threat actors are always inventing new ways to use them for various types of malicious activity.

Thus, it is important to filter bots out of incoming traffic.

Organizations need a reliable way to detect and block hostile bots from their sites, applications, and APIs.

Traditionally, hostile bots have been identified using approaches such as:

- Signature recognition.
- Rate limiting.
- Blacklisting.
- JavaScript injection and cookie handling.
- CAPTCHA and reCAPTCHA challenges.

These techniques are still useful against older bots. However, they do not work against the newest bots, which have been designed to avoid detection by these methods.

Threat actors are always improving their tools. Newer generations of bots can defeat traditional detection methods by:

- Spoofing user agent strings and other deceptive actions for the bot to appear like a legitimate human user.
- Rotating IPs and/or keeping the rate of requests to 'reasonable' levels.
- Deploying headless browsers (i.e., web clients that run programmatically without a GUI) that can pretend to be "real" browsers: they can handle cookies, execute JavaScript, and so on.
- Solving CAPTCHA and reCAPTCHA challenges automatically.

Look for a solution that includes technologies for detecting the latest-generation bots. These include:

Client certification mechanisms (available in some industries) to ensure that connections originate from legitimate clients.

Advanced browser verification to detect headless environments.

Client authentication (especially important for APIs, where browser verification does not apply).

UEBA (User and Entity Behavioral Analytics), contrasting current user data to a baseline of legitimate metrics

Machine Learning to create biometric and behavioral profiles of legitimate users, for detecting anomalous and abusive usage.

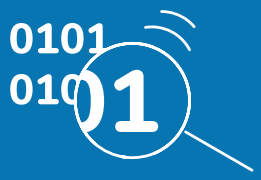
Mobile SDK to secure mobile/native applications and prevent abuse of their APIs.

'Invisible captcha': applying the above techniques and others that do not affect the user experience, while still accurately identifying even the latest generation of bots.

3. Visibility into web traffic

Many web security solutions only show the requests that were blocked. They also tend to provide incomplete information about why these requests were not allowed.

However, when security events occur, or even during normal traffic conditions, this partial visibility can hinder your ability to understand what is happening.



When comparing web security solutions, a vital aspect is often overlooked: traffic visibility.

For effective security in the modern threat environment, complete visibility is required.

Organizations need a full understanding of every incoming request (not just the ones that were blocked), along with its content and context. Further, it is also important to understand why these decisions were made. This is an especially important differentiator when evaluating security solutions, because it allows you to discover and correct anomalies, and eliminate sources of False Positive and False Negative alarms. Over time, this will increase the accuracy and precision of your web security.

Full visibility helps gain a clear understanding of all incoming and outgoing traffic to detect even subtle attacks. It's an important component of maintaining a robust security posture.

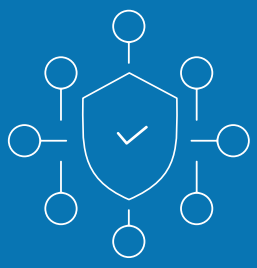
To provide full visibility, a web security solution must include:

- **Contents and metadata** for each HTTP request.
- **Information about what happened** to the request, and why.
- **User-friendly access** to current and historical data.
- **The ability to easily construct sophisticated queries** and gain insights from historical traffic data.
- **The ability to view data and control traffic in real time**, both for blocked requests and requests that were passed.

4. Flexible deployment options

Single-cloud environments are still popular, but multi-cloud and hybrid architectures are growing increasingly common.

In today's ever-evolving business environment, an inflexible security solution will hinder your organization's ability to adapt your products and services to market conditions and offer new ones. Many security solutions were designed for traditional infrastructure, and they create friction when trying to use them in modern architectures.



It's important to select a versatile, adaptive solution that can support your organization's growth and flexibility.

Look for a web security platform that:

- **Runs natively** on the top-tier cloud platforms.
- **Integrates fully with each CSP's stack** of security and reporting tools.
- **Integrates with a wide variety of other providers**: CDNs, SIEMs/SOCs, etc.
- **Avoids vendor lock-in**, and easily supports multi-cloud architectures.
- **Is deployable within** VMs, containers, hybrid architectures, and even service meshes.

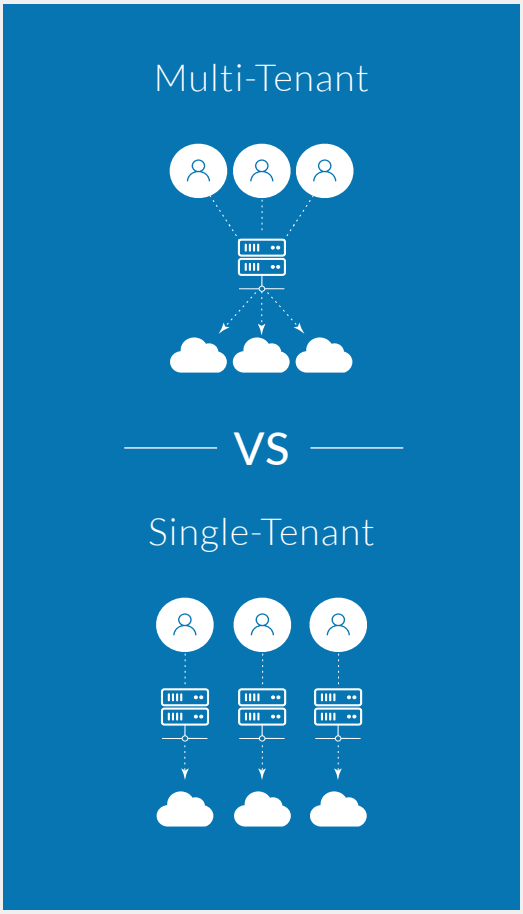
5. Privacy of data and isolation from other tenants

When evaluating web security solutions, the differences between single- and multi-tenant architectures are rarely considered.

Multi-tenancy includes compromises on performance, security, and privacy. Unfortunately, almost all security solutions available today are multi-tenant.

A good solution is single-tenant and runs within your environment.

Benefits include:



Maximum privacy:

Multi-tenant platforms decrypt and analyze your private data outside your perimeter. A single-tenant solution can process all traffic inside your environment.

Improved performance:

Multi-tenancy requires you to share infrastructure with many other customers running variable workloads. Single-tenancy provides dedicated resources for your use alone.

Maximum protection:

Multi-tenant solutions have exposed users to outages, private data exposure (e.g., the Cloudbleed incident), and other problems. Single-tenancy avoids these potential issues.

Avoiding third-party DDoS:

Multi-tenant solutions expose you to slowdowns or outages when a DDoS attack is waged against one of their other customers.

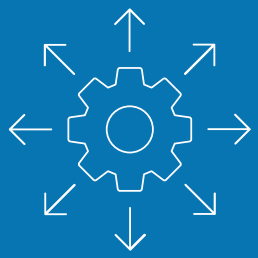
Avoiding routing latency:

In multi-tenant solutions, traffic is routed to external infrastructure for processing.

6. Managed service and overall experience

Deploying a web security solution is not a "fire and forget" practice. It is a continuous exercise that requires the full attention and commitment of security teams.

However, there are certain obstacles that hinder the effective configuration and management of web security solutions:



Security solutions run the gamut of management options: from none, to paid management & support, to all-inclusive fully managed solutions.

Time:

Managing a security solution takes time. Even beyond its initial setup, there are ongoing activities that are time consuming: making sure the solution is up to date, adding new rules, and continual monitoring to ensure everything is working as expected.

Complexity:

The threat environment is constantly evolving and growing more complex. Threat actors are often well-funded, with access to substantial resources. Meanwhile, the modern web provides high financial incentives for cybercrime.

Required expertise:

In an era of increasingly sophisticated attacks, managing a security solution requires a high level of expertise, and this standard is continually rising. It is expensive and challenging for many organizations to dedicate sufficient resources to this, and maintain the required in-house expertise.

In-house management of a security solution is neither simple nor inexpensive, and ultimately it might not even be effective. To solve these problems, many organizations are moving to Managed Security Solutions.

Rather than having an in-house team maintaining their security solutions, these organizations are letting the security vendor(s) manage them.

This solves all the issues noted above and has many other benefits as well.

Security vendors offering managed services have dedicated 24/7 support teams that can handle any request, big or small, immediately, and most issues can be solved instantly via a quick phone call or a brief email.

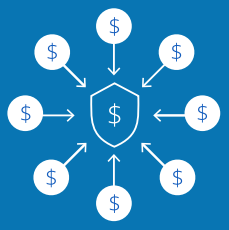
One security vendor can provide and manage multiple forms of security, if it offers an all-in-one platform (i.e. next-gen WAF, DDoS protection, bot management, etc., all in the same solution). This saves both time and money.

In addition to traffic filtering, a good managed security solution can also increase efficiency for other, related functions. For example, some solutions include administration capabilities for SSL certificates, DNS zones and records, and more. If the solution is fully managed, then the organization saves additional time and money, because these responsibilities are now fulfilled by the security provider.

7. Total Cost of Ownership (TCO)

Organizations must do their due diligence when considering and evaluating security solutions. Certain vendors are known for giving full demos of their product suites, but customers often don't discover that these products are priced *a la carte* until contractual negotiations have begun.

Even the solutions that are advertised as complete products are, almost always, incomplete, unless the customer pays for additional add-ons and subscriptions. This raises the TCO to a level that is significantly above the base cost.



There are two aspects of TCO: the cost of the solution itself (discussed here), and operational expenses that can be affected by the choice of security solution (discussed on the next page).

To avoid this problem, organizations should look for a cost-effective solution that includes comprehensive protection for a single price.

Another important—but often overlooked—source of potential savings is operational expenses. These are affected by the security solution's architecture.

Most solutions are multi-tenant, and run on external infrastructure owned/controlled by the vendor. This means that the vendor bills the customer for resource usage; this billing can be opaque, potentially involving **markups from the vendor's actual cost**. More importantly, depending on the configuration and the cloud platform being used, **the cost for resource usage can be higher due to ingress/egress fees**.

To optimize cost structure and achieve a low TCO, look for a solution with these characteristics:

A single-tenant solution that runs within your environment. Along with the advantages discussed earlier (for performance, privacy, etc.), this also eliminates many infrastructure expenses such as ingress/egress fees. Further, a solution that runs within the customer's environment and uses the cloud provider's CDN can eliminate operational costs such as CDN node fill fees.

Direct billing from the CSP for resource usage, with no markups.

Strong relationships with the top-tier CSPs. A good security vendor has partner arrangements with the major cloud service providers, and can extend special offers to customers. These include, among other things, substantial discounts on CDN usage. In some cases, **these savings can be more than 50%**.

Conclusion

In the modern threat environment, robust web security is essential. A variety of solutions are available, but they are not equal.

There are significant differences in effectiveness, flexibility, privacy, TCO, and more. Organizations which perform their due diligence when evaluating solutions can enjoy substantial savings, while simultaneously maintaining a stronger and more performant security posture.

Questions about this white paper? Feel free to contact us here.

About Reblaze

Reblaze is the cloud native, fully managed security platform for websites and web applications.

Reblaze's all-in-one solution supports flexible deployment options (cloud, multi-cloud, hybrid, DC), deployed in minutes and includes Bot Management, API Security, next-gen WAF, DDoS protection, advanced rate limiting, session profiling, and more.

Unprecedented real time traffic visibility enables full control of your web traffic. Machine learning provides accurate, adaptive threat detection, while dedicated single-tenant deployment ensures maximum privacy, performance, and protection.

Reblaze.com/get-a-demo