Reblaze

Single-Tenant Architecture for Web Security

why it's essential

Reblaze Technologies LTD

Introduction

Web application security continues to be challenging for many organizations today.

According to Edgescan’s 2020 Vulnerability Statistics Report, 27% of internet-facing assets have a CVE with a CVSS score of 7.0 or more.

Meanwhile, the direct and indirect costs of successful exploits are high. In 2020, for example, the average cost to an enterprise of a data breach was $3.92 million. And the annual global cost of cybercrime is expected to reach $6 trillion in 2021.

Therefore, organizations must pay close attention to the security of their web applications and services.

In this white paper, we discuss the problems inherent in a multi-tenant web security architecture for security, privacy, performance, and cost.

We then show how these issues are avoided by a single-tenant architecture.

A robust web security solution has to address many layers, from threat detection and access control to DDoS protection, API security, and bot detection. The architecture of the solution has a direct impact on its effectiveness and performance.

Web Security Architecture

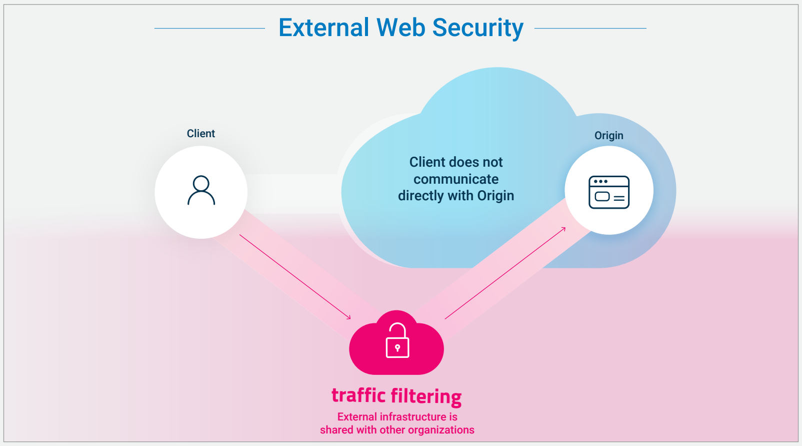

External Web Security
Client
Origin
Client does not communicate directly with Origin
traffic filtering
External infrastructure is shared with other organizations

Figure 1: Traffic flow for a multi-tenant web security solution

As shown in Figure 1, a typical web security architecture diverts user traffic to a multi-tenant scrubbing center, where data packets are decrypted in order to be checked for possible security threats. The scrubbed traffic is then re-encrypted and routed to the origin server hosting the application.

By contrast, in a single-tenant web security architecture, the security solution runs on dedicated infrastructure within the customer's environment. All processing takes place within the customer's perimeter.

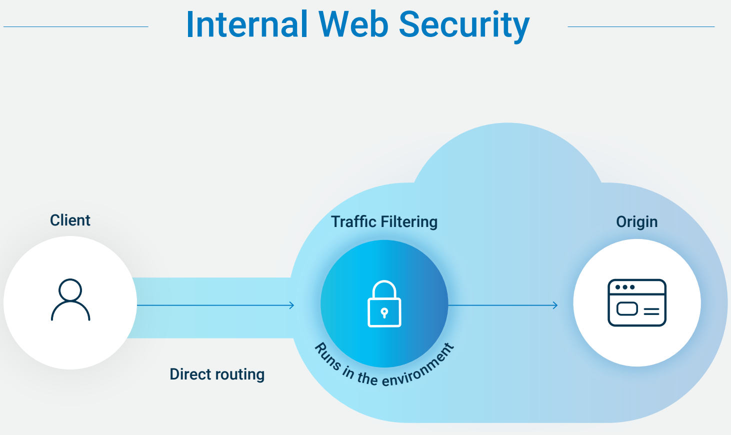


Figure 2: Traffic flow for a single-tenant web security solution

Multi-Tenancy's Security Problems

1. Data Exposure

In the multi-tenant web security model, data is decrypted and processed by the security solution vendor outside of the environment of the customer, i.e., the owner of the web application.

Vendor software bugs or admin errors could open the door to unauthorized access to a fellow tenant's data, or accidentally return data to the wrong tenant.

The multi-tenant web security architecture shown in Figure 1 exposes the web application to several security challenges, including data security, DDoS, and potential compliance issues.

The months-long Cloudbleed incident in 2017 is a classic example of this problem.

Cloudflare provides CDN and hosting services for internet sites. An error in Cloudflare's code allowed user data from one website to be randomly inserted into pages served by other sites. This included highly sensitive information such as encryption keys, cookies, and passwords, much of which was publicly cached by search engines. The vulnerability was already five months old when discovered, and later estimates were that the bug was triggered 1.2 million times and affected thousands of websites. This highlights the risks incurred when data is processed by a third-party multi-tenant solution outside of the customer's environment.

2. DDoS Attacks

Another risk of the multi-tenant security model is that a DDoS attack on one tenant can affect the other tenants sharing that infrastructure.

A certain high-profile ecommerce site was using a popular multi-tenant security solution. A massive DDoS attack on a fellow tenant brought down their site as well, creating a terrible dilemma: to absorb significant financial losses from the downtime, or to disconnect temporarily from the security service and come back online without protection.

DDoS (Distributed Denial of Service) attacks worsen each year, in their frequency, bandwidth, and severity. New records keep getting set; several events have reached 2 Tbps, and an attack in 2021 hit over 17 million requests per second.

After this incident, the ecommerce company sought a different security provider. They are now satisfied customers of Reblaze.

3. Compliance

Data protection regulations such as the European Union's GDPR apply not only to the direct data controller, but also to all third-party service providers (known as data processors) that are given access to the data.

In other words, not only does the organization collecting the data have to be GDPR-compliant, but all of the suppliers and partners that store, process, or otherwise “touch” the data.

As shown in Figure 1, a multi-tenant web security solution routes user data through its external infrastructure before re-routing it back to the customer’s environment.

Most regulators allow a multi-tenant web security solution if the vendor can show compliance. However, for sectors where data privacy is paramount, such as banking, insurance, and healthcare to name just a few, the multi-tenant security solution could be considered a weak link in their data governance chain.

Multi-Tenancy Hurts Performance

Web application owners must optimize performance because a poor UX (user experience) has been shown to have a direct impact on business metrics.

The last thing an executive wants is for a web security solution to slow down performance. But that's exactly what can happen in a multi-tenant security model.

Web performance includes DNS lookup time, page load time, time to start render, time to interactive, and so on.

The impact of poor performance:

- **Average bounce rate jumps** from nine percent to 38 percent when page load time rises from two seconds to five seconds.
- **Abandonment rate leaps** to 53 percent when a mobile site takes more than three seconds to load, according to Google.
- **Conversion rates drop** by 4.42% on average for every second of load time within the first five seconds.
- **Revenue decreases** by 20 percent when latency rises by one-half of a second, according to Google. AWS ran similar tests, introducing delays in increments of 100 ms, and discovered that "even very small delays would result in substantial and costly drops in revenue."

Why multi-tenant web security can negatively affect performance:

Extra Routing

As shown in Figure 1, data packets travel in two legs from the user to the origin server: from the client to the external security infrastructure, and then from the infrastructure to the server. Except for the (very rare) situation where the infrastructure is geolocated exactly in-between the user and the origin, this extra routing will add latency and degrade performance.

Extra Encryption/Decryption

Data packets are decrypted for processing by the security solution, and then encrypted again for transmission to the web server. As discussed earlier, this additional decryption/re-encryption can have an impact on data privacy. Here, we note that it also adds more processing time, which again will degrade performance.

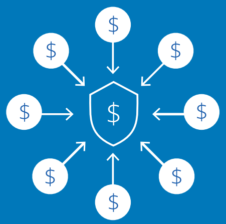
Resource Sharing and Load Balancing

In a multi-tenant web security solution, the customer (i.e., the web application owner) has no control over resource sharing and load balancing among the various tenants. We already noted how a DDoS attack targeting a fellow tenant could bring down other tenants' applications as well. But even if that more dramatic scenario does not occur, a customer's workloads may experience delays while the security platform deals with fluctuating demand across multiple tenants.

Multi-Tenancy's Higher Costs

Multi-tenant web security solutions run outside of the customer's cloud infrastructure. Almost always, this results in higher costs for the customer.

Most public clouds do not charge for data ingress (when data enters the cloud), or intra-cloud data transfer, but they do charge for egress (when data leaves the cloud).



Cloud providers charge for resource usage, including bandwidth. This affects the operational cost of a security solution.

Higher costs from multi-tenant web security include:

Usage charge mark-ups. A multi-tenant solution runs on resources controlled by the vendor, who bills the customer for usage. Often, the vendor will mark up the underlying usage cost—an incremental charge that's not necessarily visible to the customer.

Overhead. A multi-tenant architecture requires additional infrastructure for running and administering the system. Customers must pay their share of these costs.

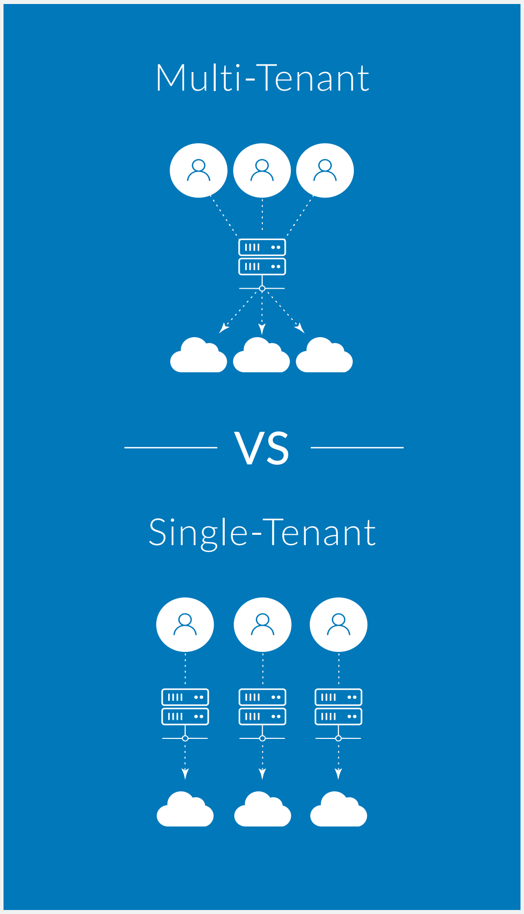
Data transfer. Traffic enters and leaves the security solution's environment before entering the origin server's environment. This additional ingress and egress incurs extra usage charges.

CDN. With a multi-tenant solution, Content Delivery Network charges can be higher, especially cache-fill fees.

The Advantages of a Single-Tenant Web Security Solution

Single-tenancy avoids all of the problems discussed earlier: all of the issues with security, privacy, performance, and cost.

A single-tenant web security solution runs within the customer's environment, such as a virtual private cloud (VPC). Traffic flows directly to the destination environment, where filtering occurs; data packets from users are decrypted once at the gateway, and the scrubbed traffic proceeds directly to the origin server.



Maximum privacy

Private customer data is never decrypted, processed, or stored outside your perimeter.

Improved performance

Resources are not shared with others. Extra decryption/encryption is avoided.

Minimal expense

Resource usage is not increased by external infrastructure; charges are billed directly with no markups.

No third-party DDoS

Your web applications and APIs are not affected by attacks aimed at others.

No routing latency

All traffic moves directly to your environment, without being sent to external infrastructure first.

Additional savings

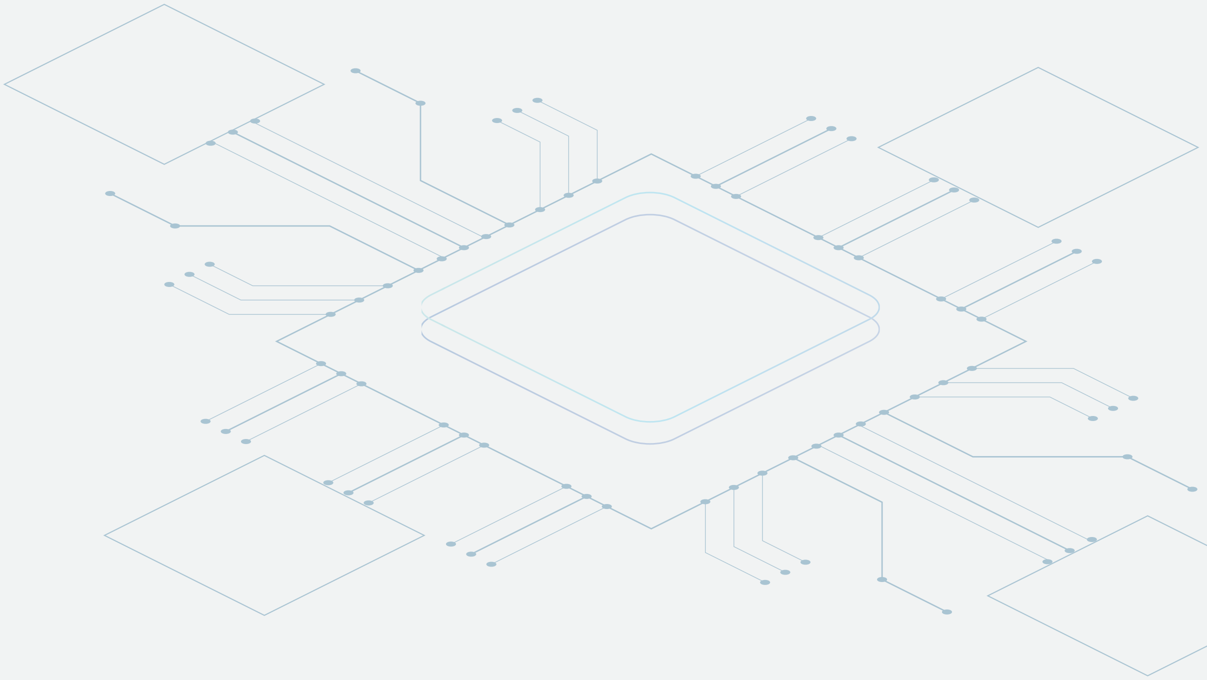
Some vendors have agreements with cloud providers to get large discounts on usage fees.

Conclusion

A multi-tenant web security solution running outside of the customer’s environment can make web applications and APIs vulnerable in several ways. These vulnerabilities are eliminated when the solution is single-tenant, running within the customer’s perimeter.

When evaluating web security solutions, their architectures are often overlooked. Perhaps this is because almost all solutions are multi-tenant; thus, few decision-makers will question this approach. Nevertheless, as shown above in this white paper, multi-tenancy brings a number of inherent problems, all of which can be avoided by selecting a single-tenant solution.

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