Reblaze

Web Security:

Reducing Costs While Improving Effectiveness

Reblaze Technologies LTD

As threat actors continue to improve their capabilities, web security is more important than ever.

According to Gartner, annual information security spend recently rose to over

$123 Billion

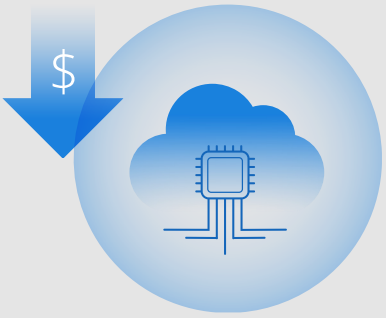
Many organizations consider the line-item price of their security technologies to be their whole cost; however, there are more aspects to consider.

There are also opportunities for savings that are usually neglected.

In this white paper, we'll discuss ways to reduce security-related costs, while at the same time achieving a more robust security posture.

We'll discuss how to:

- Optimize cloud security architecture for cost and performance
- Reduce CDN costs
- Avoid revenue loss and "collateral damage" when attacks are aimed at others
- Eliminate hidden expenses created by threat actors
- Eliminate hidden costs within the security infrastructure



Some of the tactics discussed in this white paper apply to any architecture, whether cloud, hybrid, or traditional datacenter. Others apply specifically to cloud architectures.

In particular, organizations using the public cloud to host their sites, apps, and services can expect significant financial benefits when using a web security solution running in the same VPC and using the same CDN.

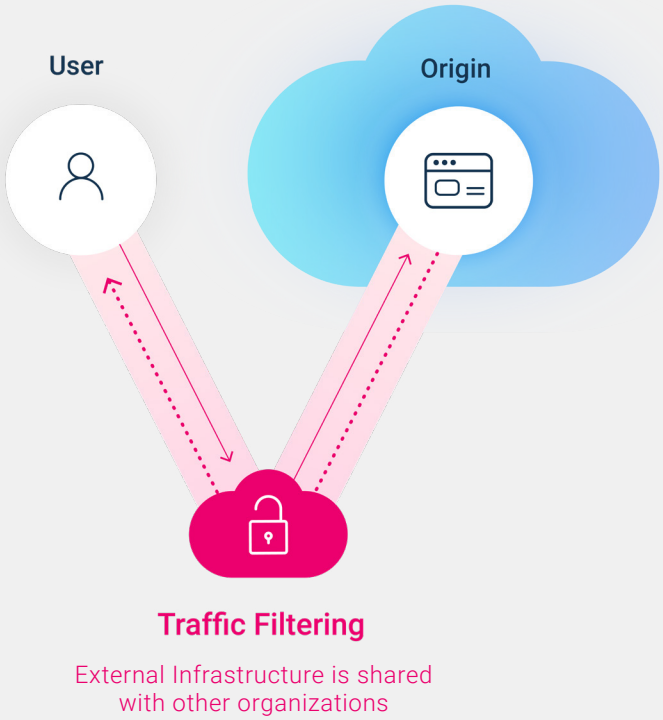
Optimize Cloud Security Architecture for Cost and Performance

Many organizations have moved a substantial portion of their workloads to the cloud. In this environment, the need for web security is more important than ever, but traditional on-prem appliances are no longer useful. Thus, alternative approaches are necessary.

01. External web security

Many web security vendors offer traffic filtering in a SaaS (software as a service) delivery model. Usually this is provided in the form of a 'scrubbing center', to which all incoming traffic is routed. There it is scrubbed and verified before being forwarded to its original destination.

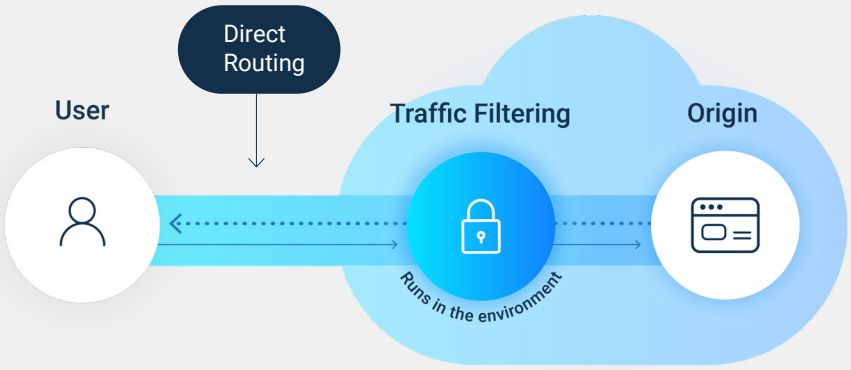
Client does not communicate directly with Origin



02. Internal web security

A different approach is to run security on a virtual machine within the customer's VPC (Virtual Private Cloud) environment. Here the traffic flow is different; incoming traffic flows directly to the VPC without being diverted elsewhere first.

Clients communicate directly with Origin



These two architectures (external versus internal) have substantially different cost structures. All else being equal, the external security solution is more expensive than the internal solution.

$

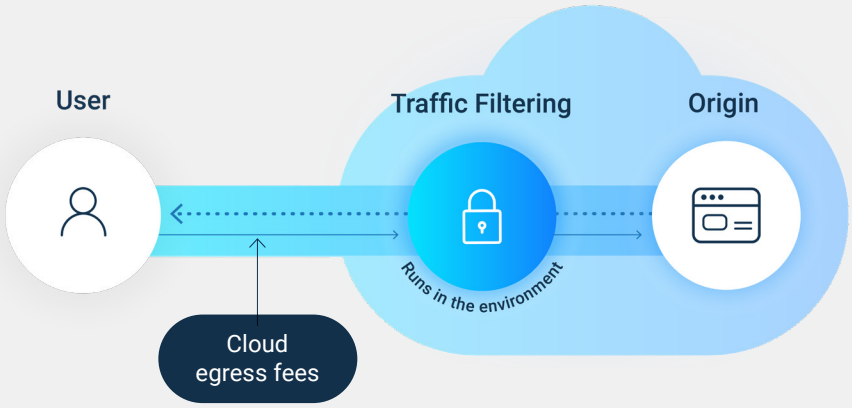
Costs common to both external and internal security architectures

In both architectures, compute resources are necessary for analyzing incoming traffic. For the sake of this comparison, we'll assume that these are the same for both. The same is true for potential ingress fees ("potential" because most providers do not currently charge for data ingress). We'll also assume that all security SaaS vendors charge similar rates for their services, so these costs will also be the same.[1]

[1] However, as we'll see later, there are significant differences in cost structure among vendors.

The final common cost is data egress. When the origin server receives the filtered traffic, it will respond to the requests. As the responses leave the customer's cloud environment, egress fees are charged; again, these will occur under both security architectures.

Both internal and external architectures incur egress fees.



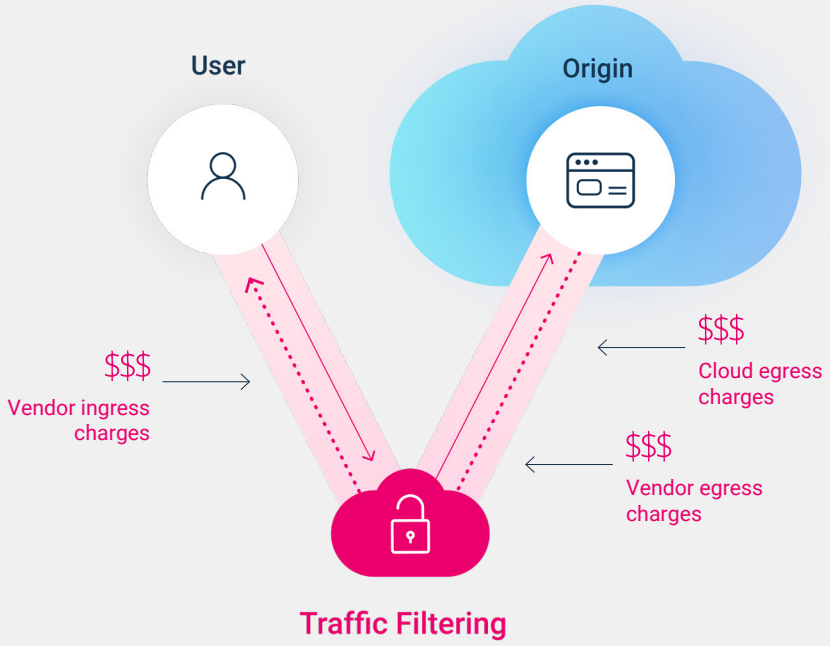
This is where the similarities end. For the internal solution, we have just described the costs involved, but for the external solution, there are additional costs beyond these.

Additional costs for the external solution

Along with costs listed above, the external 'scrubbing center' architecture also includes:

- Bandwidth expenses as the traffic enters the scrubbing center; although these might be zero (as mentioned above, an on-cloud solution will usually not incur ingress fees), they might also be significant (e.g., transit costs, if the solution runs in a physical datacenter).
- Additional egress/transit costs as the traffic leaves the scrubbing center
- Overhead costs for managing a multi-tenant infrastructure, serving hundreds or thousands of clients simultaneously, plus additional egress/transit costs as the traffic leaves the scrubbing center

Multi-tenant infrastructure incurs additional charges



Usually, many (or even all) of these costs are not directly visible to the customers. Nevertheless, the customers pay them anyway, in the form of higher rates charged by the vendor.

The most significant items here are the egress charges. These can be substantial; depending on the cloud provider and volume, as high as $100 per TB.

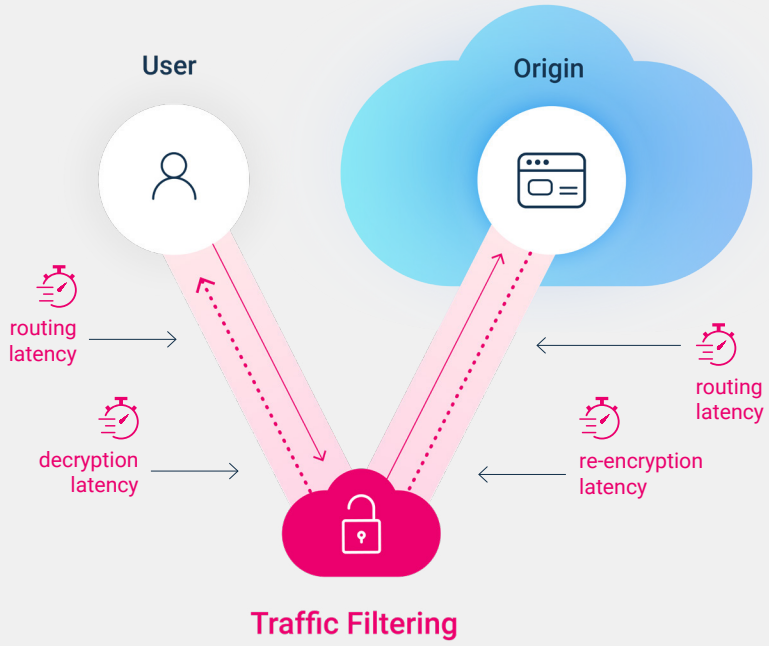
! Note that using an external security solution will double the amount of traffic egress. The associated costs are likely to be indirect, manifested as higher vendor rates.

!

Other problems associated with external solutions

An external solution creates several additional issues that do not exist for an internal solution, because incoming traffic does not travel directly to the customer's VPC.

Multi-tenant infrastructure adds latency and degrades performance



- The traffic is diverted to the external solution, which adds routing latency.
- There, it is decrypted, which takes time and adds processing latency.
- After analysis, it must be re-encrypted, which takes additional time.
- Then it is forwarded to the customer's cloud, adding more routing latency.

All of this can add non-negligible amounts of latency and perceived sluggishness to the customer's web applications. This can cause user dissatisfaction and reduce response rates. It also introduces privacy risks, since sensitive data is being decrypted outside of the customers' environments.

The importance of immediate responsiveness

Back in 2006, Google found that added latency of one-half of a second reduced traffic and revenue by 20 percent. 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." Since then, Internet users have become even more impatient, and small amounts of added latency can increase bounce rates significantly.

Summary

Traffic filtering is a vital part of modern cloud workloads. This can be done within the customer's VPC, or it can be done externally on the vendor's infrastructure.

Most security vendors offer the external architecture, but this is significantly more expensive than an internal solution.

Switching to an internal in-cloud solution will:

Optimize your security workload

Reduce your costs

Avoid unnecessary degrading of performance and privacy

Reduce CDN Costs

In the previous discussion about architectures, we ignored the use of a CDN (content delivery network). However, most organizations use a CDN, and this introduces additional opportunities for cost reduction.

A CDN can accelerate the perceived responsiveness of a web application to its users. It can also save money for the organization, because it removes workloads for serving static content from compute and storage resources, and moves them to the CDN, which is designed to perform this role quickly and cost-effectively.

However, the savings can vary, depending on the architecture. Some configurations can save much more than others.

We'll illustrate this by once again contrasting two common architectures:

01. An external security solution and separate CDN

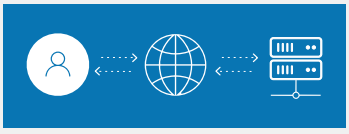
Organizations often have their origin, security solution, and CDN running as separate entities from different providers. With this approach, here is what happens when a client sends a request to the origin.

First, the request arrives at the CDN. The CDN node examines it to see if it is a request for static content that the CDN can serve.

If the request is for static, CDN-serviceable content:

For requests that can be served by the CDN, there are two possible situations:

- If the CDN node already has the content cached, the node responds and sends the content to the client. The organization is charged a CDN egress fee.



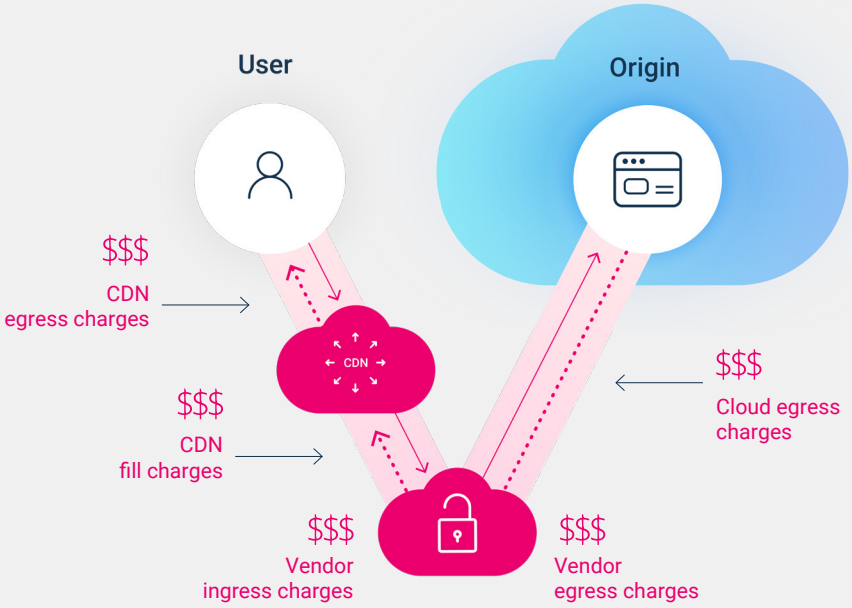
- If the CDN does not have the content cached, the CDN node requests the content from the origin. Upon receipt, the content is cached (to make it available to subsequent clients) and a response is sent to the client with the content. The organization is usually charged at least two fees: the regular CDN egress fee, plus another fee for filling the cache.

In some situations, depending on the provider and the configuration, an organization may also incur additional fees, e.g. an ingress fee for the request to be sent from the CDN node into the origin's cloud, and/or an egress fee for the content to be sent out from the origin to the CDN node.

If the request is not for CDN-serviceable content:

If the request cannot be fulfilled by the CDN, then it is forwarded to the origin. Along the way, it passes through the security solution, which filters out hostile requests before they can reach the origin. Depending on the configuration and the cloud platform being used, the organization might get charged additional fees for these requests, too.

When an external security solution is combined with a CDN, a substantial number of fees can be charged during traffic processing.



02. An in-cloud security solution and CDN

Instead of using an external security solution and CDN, an alternative approach is to use an internal solution (running directly in the customer's VPC) while also using the CDN from the same cloud provider. Here the traffic flow is different, and usually much less expensive for the organization. Let's examine the same hypothetical traffic flow for this configuration.

An incoming request arrives at the CDN. As discussed above, the CDN serves it immediately if possible, or serves it after being filled by the origin, or forwards it to the security solution for filtering before it arrives at the origin.

For requests served by the CDN, the organization will still be charged a CDN egress fee.

However, many or all of the other fees can often be eliminated, especially when organizations use the CDN and backend infrastructure from the same provider.

For example, AWS does not charge a fee to fill its CloudFront CDN if the "filler" is an AWS EC2 instance or an S3 storage bucket, but it does charge a fee if the origin "filler" is a compute or storage resource from another provider.

For this architecture, there are also no ingress/egress charges associated with the security solution, because within the organization's cloud environment, no ingress/egress occurs.

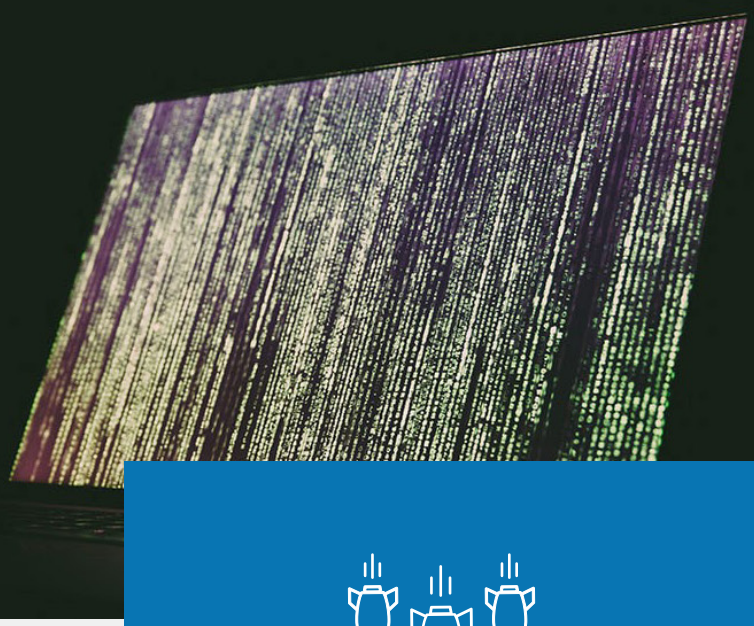
Summary

Compared to a typical external security solution and CDN, using an internal security solution combined with the cloud provider's CDN can dramatically reduce expenses over time.

The Benefits of Cloud Security Partnerships

In addition to these strategies, there is another significant way for an organization to save money. Security providers that have strong existing relationships with the top-tier cloud providers can extend special offers. These partner arrangements include, among other things, substantial discounts on CDN usage. So, if an organization uses a security provider with such an agreement, and has all its infrastructure on the same provider, they might enjoy a discount on these fees. In some cases, these savings can be more than 50%.

Avoid Lost Revenue from “Collateral Damage” when Attacks are Aimed at Others



Modern DDoS attacks can occur at dramatic scales, reaching into the Gbps or even Tbps range.

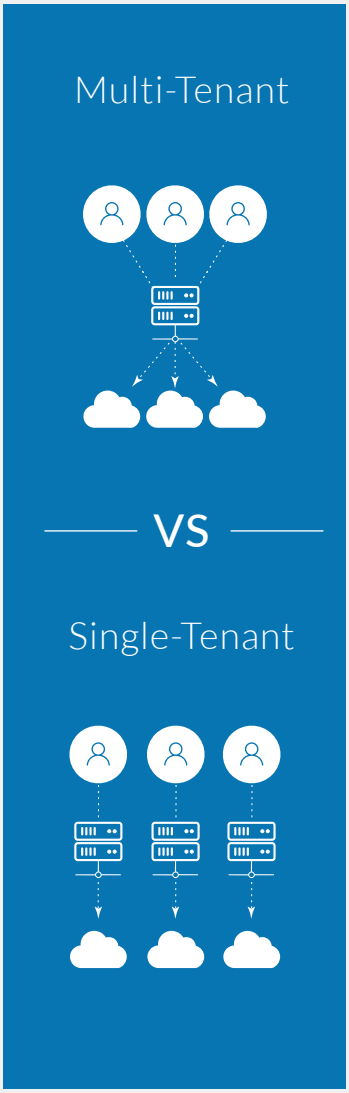
If your organization becomes the target of such an attack, and your security solution is unable to defeat it, the loss of revenue can be substantial.

Clearly, it is imperative to maintain robust defenses against these attacks. Indeed, there are many security vendors offering DDoS mitigation services, which can all seem very similar to each other.

However, there is a crucial, although often overlooked, distinction among them. Some DDoS services contain an inherent vulnerability to attacks that other services do not.

As discussed previously, most web security products are provided as external solutions. Almost always, these solutions are multi-tenant; a large number of customers share the same security infrastructure.

Even during normal times, many organizations can experience a loss rate of six figures per hour of downtime; during the most important periods (such as Black Friday weekend for ecommerce stores), a large-scale DDoS event can be ruinous.



When an attack occurs, multi-tenancy has important implications.

An attack on one customer will affect ***all*** customers sharing that same infrastructure. In other words, your organization can be affected by an attack that is aimed at a completely different organization.

When this occurs, it is an opaque event. The attack traffic will not appear in your logs or monitoring tools. You will not know that an attack is occurring, nor will you know the organization that is being attacked. All you will know is that your traffic filtering is not performing as expected, and thus your web applications are not being fully responsive to your users. Perhaps the most frustrating aspect is that there will be nothing you can do to mitigate this situation.

None of this occurs when using a single-tenant solution.

Here, you cannot be affected by volumetric attacks aimed at any one of hundreds, or even thousands, of other organizations. And if a DDoS attempt does occur, you will know exactly what is happening, you will see the countermeasures being taken, and you will have control of the situation.

Summary

On today's Internet, it is necessary to maintain robust defenses against DDoS attacks. For most organizations, the potential costs of coming under attack are substantial.

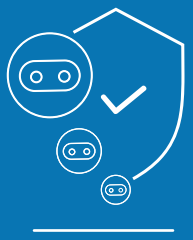
Therefore, it is important to eliminate any vulnerabilities created by your choice of vendors. Multi-tenant security solutions include some inherent exposure to receiving "collateral damage" during a DDoS attack. Selecting a dedicated, single-tenant solution will avoid these vulnerabilities.

Eliminate Hidden Expenses Created by Threat Actors

Some attacks, such as DDoS, are designed to inflict immediate and obvious damage to the target. Other attacks are more subtle, and frequently are not recognized by the victim; over the long term, these can cause much more harm.

Almost all web attacks today use malicious bots in one form or another. Many of these bots are straightforward to identify, and most security solutions can block them. However, over the last few years, threat actors have developed bots that are much more sophisticated, which can masquerade as human users while performing hostile actions.

These modern bots can cause a great deal of harm to the victim, in a variety of ways. To illustrate this, here are three examples.



Many malicious bots are not intended to bring down a website. Instead, they quietly collect information, or they perform other hard-to-detect activities.

Without a robust security solution that includes advanced bot recognition capabilities and deep analysis of web traffic, these bots can operate unhindered. This can have significant financial implications.

Three Real-World Examples

01.

An international airline changed to a new web security solution which can identify and block the latest-generation bots. The airline quickly discovered that a large portion of its traffic—millions of web and mobile API requests per month—consisted of scraping and inventory-denial bots which had been issuing queries for flight schedules, ticket prices, and so on.

Blocking this traffic produced immediate savings:

- **Reduced cloud egress traffic costs** because data was not being returned to the bots
- **Reduced size and usage of data storage for traffic logs**
- **Reduced usage of compute resources**
- **Reduced fees paid to third-party flight data providers** (e.g., GDS)

Blocking these bots has produced a total savings of

$600,000
per year

02.

A large, diversified ecommerce company has thousands of apps, services, microservices, and mobile API backends. The company deployed a security solution with advanced bot detection; this revealed that hostile bots were causing losses of **over $1,000,000** per annum due to user account hijacking, creation of fraudulent "stealth" accounts, content spamming, promotional tool abuse, shill bidding, and more. Today, malicious bot traffic is automatically excluded from the company's applications and endpoints.

03.

An IT solution provider discovered that much of its incoming traffic was being generated by hostile bots. The provider's system automatically responds to requests with SMS messages; blocking the bot traffic now saves a substantial monthly amount in reduced SMS costs alone.

Summary

Many web security solutions cannot identify the latest generations of hostile bots to prevent them from abusing their customers' applications and APIs.

In the modern threat environment, correctly detecting and blocking these bots will not only remove security vulnerabilities, it will often result in significant savings as well.

Eliminate Hidden Costs within the Security Infrastructure

Another source of potentially hidden expenses is the business model of the security vendor(s).

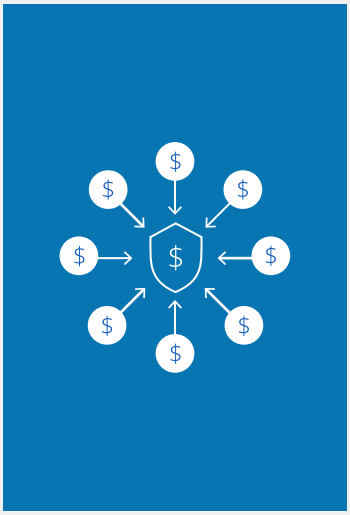
The major cloud platforms offer a variety of security tools. However, the providers are not in the business of creating robust security products; instead, their purpose is to attract cloud customers and encourage more infrastructure usage.

Some of these tools are free, while others are not. However, none of them provide complete protection, nor are they meant to. For many organizations, these tools can be useful in limited roles, but they must be augmented by more robust products from third-party sources.

As for the third-party vendors, many offer limited-scope products and services: for example, DDoS protection, or a WAF. Therefore, organizations must purchase products from multiple vendors in order to achieve complete protection.

- **Most "all-in-one" vendors don't truly offer a unified, complete solution.**
- **Most vendors charge separately for many of the items in their security toolkits.**
- **Most "all-in-one" solutions advertise their base price, which does not cover all of the additional line items.**

Almost always, this is more expensive than purchasing a single comprehensive solution. It also requires more internal resources for training, management, communication, and support.



Some vendors offer all-in-one solutions. However, even among these, there is another important factor. Most all-in-one vendors don't truly offer a unified, complete solution. Instead, most charge separately for many of the items in their security toolkits. Paid add-ons and subscriptions can be required for anything from application access control or access management, to threat feeds, DNS services, bot detection, behavioral analysis, or input validation. In addition to this, different vendors often have different pricing structures based on the customer's use case: for example, some vendors charge extra for multiple subdomains, SSL certificates, and so on.

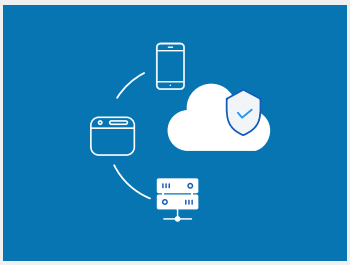
Unfortunately, most "all-in-one" solutions advertise their base price, which does not cover all of these additional line items. For these vendors, the price for complete security is usually significantly higher.

Summary

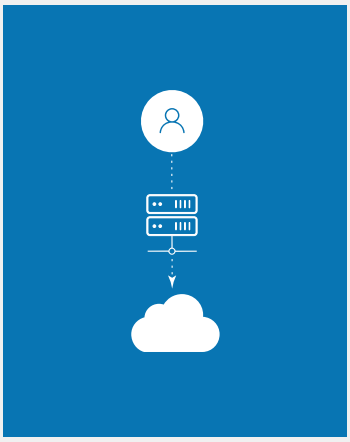
Limited-scope security products usually create a higher TCO (total cost of ownership). As for the all-in-one solutions, due diligence is required; be sure to calculate and understand the true TCO for your use case.

For many organizations, the optimal approach is to adopt a true all-in-solution—one that provides comprehensive protection for a flat price. This can result in considerable savings, while still providing robust security.

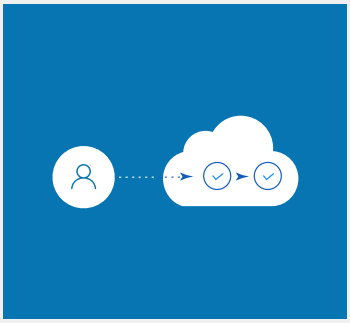
Conclusion: Reducing Costs While Staying Secure on the Cloud



In the modern threat environment, effective protection is essential. Moving workloads to the cloud does not change this, because the major cloud platforms operate under a "shared responsibility" model; they provide secure infrastructure, but the security of your sites, apps, and services is your responsibility alone.



Security vendors offer a variety of products and services, but their architectures, capabilities, and cost structures can vary widely. Organizations using traditional datacenters can minimize expenses and security risks (and in some cases, increase performance as well) by avoiding multi-tenant solutions in favor of a dedicated single-tenant solution, ensuring that your chosen solution can detect the latest-generation bots, and selecting an all-in-one solution that does not charge extra for capabilities, modules, intelligence feeds, subdomains, SSL certifications, etc.



In addition to these savings, even more financial benefits are available to cloud-using organizations which have adopted a powerful unified web security solution: one that runs natively within your VPC (rather than as an external traffic filtering service), and that has partnership arrangements with the top-tier cloud platforms, thus providing you with substantial discounts on infrastructure costs.

Web security can be expensive, but as discussed in this white paper, it doesn't need to be. Organizations which perform their due diligence can enjoy substantial savings while simultaneously maintaining a stronger and more performant security posture.

About Reblaze

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

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 VPC deployment ensures maximum privacy, performance and protection. Reblaze customers include Fortune 500 companies and innovative companies across the globe.