Servium

Barracuda

PROTECT YOUR CROWN JEWELS

Barracuda Opinion White Paper

+44 (0)303 334 3000 | www.servium.com | hello@servium.com

PROTECT YOUR CROWN JEWELS

The bar is high to justify anything other than cloud-first for applications like email and CRM, but it's a different proposition for custom or legacy apps. There are huge benefits to be realised from exploiting the public cloud though, not least shifting to a modern architecture where new technologies can be enjoyed. It also means you can share in the next big leap in tech without the burden of infrastructure upgrade.

Despite the benefits and its growing popularity, there is still significant reticence from enterprise customers in using the public cloud to host their applications. Fears over security persist and multiple polls highlight this sentiment. For example, in a recent survey by Oracle, two thirds of Infrastructure as a Service (IaaS) users said using online infrastructure makes it easier to innovate, had cut their time to deploy new applications and services, and had significantly reduced on-going maintenance costs. However, half also said that they believe IaaS isn't secure enough for most critical data.

It's hardly surprising this perception lingers when stories like US telecoms operator Verizon leaving 14 million subscriber records unprotected on Amazon S3 continue to break, or indeed Microsoft's confirmation that the frequency of attacks on cloud users has increased by almost 300 percent in the past year alone.

GDPR has set the tone for stricter data privacy regulation, and for some, migration of critical applications and data, arguably the 'crown jewels', to the public cloud is getting kicked into the long grass.

50% of IaaS users say it isn't secure enough for most critical data - Oracle

Your app, your responsibility

Unfortunately, the reality to date of operating applications in the public cloud does little to dispel the perception. There is a naïve belief that hosting apps on IaaS means the provider is responsible for security. Of course, there are huge market incentives for cloud service providers to place a higher priority on security than is typical for enduser organisations, but this only extends to their infrastructure and any services they deliver using it, not any security measures necessary to protect your application – those are your responsibility. There is substantial market confusion over this point, which is why there are headline-grabbing stories of organisations who have experienced a breach in the cloud; the result of poorly protecting the workloads they have put there. It's no surprise then that Gartner predicts that by 2020, 95 percent of cloud security failures will be the customer's fault, not the provider's.

New era, new architecture

Thinking you can continue to use the same protection measures in the cloud as you do on-premise is a flawed starting point. Next-generation firewalls used on-premise in the datacentre are tightly integrated solutions that scale vertically as security demands change. The layers, networking protocols and services next-generation firewalls normally control typically do not exist in the cloud or at best are significantly different. So, in this new cloud era, trying to run security controls in the way you always have and using traditional perimeter-based security tools will do little to protect cloud workloads, even becoming an obstacle that slows you down and erodes some of the benefits of the cloud service you use.

Securing data and applications that reside in the cloud therefore requires a different approach to enable mission-critical services, high-value data, and intellectual property to make the move. In a public cloud architecture, security needs to be loosely coupled and ready to scale horizontally with the elastic nature of the IaaS you'll be consuming. Continuing to use traditional protection measures in cloud-based deployments is as simple as choosing the wrong tool for the job.

Introducing the Cloud Generation Firewall

As you look to scale and automate in the cloud, you'll also need a method of data protection that offers the same attributes. Barracuda Networks has pioneered a new approach to secure cloud workloads and apps called the Cloud Generation Firewall.

It can feel like a minefield of considerations for anyone new to the public cloud - budgeting, licensing, and metering all enter the equation as do strange new concepts like meshed networks. Barracuda Cloud Generation Firewalls, and in particular, the Web Application Firewall (WAF) have been created to help you overcome these challenges and fully embrace the potential of the public cloud.

The rest of this paper shares our view on how this is made possible:

Engineered for the cloud

The Barracuda WAF is engineered for the cloud. Critically, unlike traditional firewalls it is created on a software-based architecture rather than a hardware-based architecture. Deployed as an inline security service, the function of the firewall is designed to natively integrate with the infrastructure of your cloud provider and the management and monitoring fabric they use. It delivers a frictionless management experience and next to no latency overhead for the operational experience of the app.

Interestingly, the mega-cloud providers have recognised the importance of complementary security solutions to the future of their own business models. However, beyond the Cloud Generation Firewalls seen from Barracuda there is much frustration felt by them about the lack of innovation occurring in the wider security vendor community. To counter the lack of movement from major security players and in a bid to overcome mainstream security concerns, some cloud providers are actively modifying their architectures to try and better accommodate legacy security technologies.

Organisations should think through the actual security controls they need to cover, and use tools that leverage the agility and elasticity of cloud infrastructure — both technically and commercially.

In doing so, cloud providers are knowingly slowing down their architectures and negatively impacting the customer experience compared to cloud-friendly solutions, like those available from Barracuda.

Protecting thousands of applications

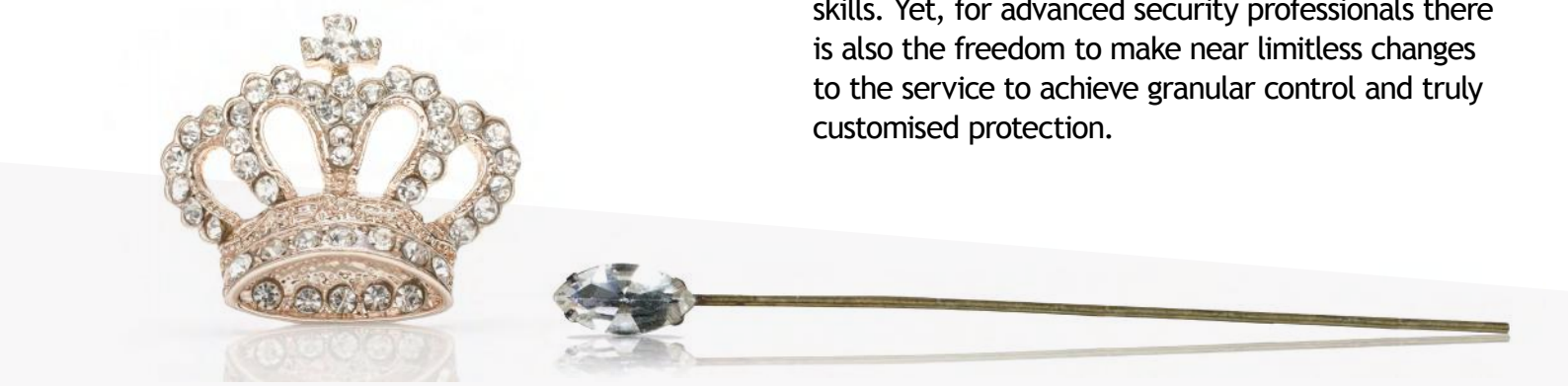
The Barracuda Web Application Firewall has secured thousands of production applications against more than 11 billion attacks since 2008. Every bit of this know-how and expertise is powering a web service built to protect web apps deployed in the public cloud.

Matched to your provider

Importantly, Barracuda Cloud Generation Firewalls are independently verified security solutions for a number of leading public cloud providers including Amazon Web Services, Google Cloud, and Microsoft Azure. The result is carefully crafted security controls that match precisely with the deployment best practices at play in the environment you are moving to, all of which can be managed through the same management console used to administer your IaaS.

The Barracuda WAF:

- No.1 WAF for Amazon Web Services
- No.1 WAF for Microsoft Azure



Ultra-fortification for web apps leaves no gaps

The Barracuda WAF is considerably more than a firewall – it's like calling a computer a calculator! It offers extraordinary security by intercepting both incoming and outgoing network traffic. It is capable of monitoring Layer 5, 6 and 7 network traffic and will inspect your web application traffic in fine detail, down to the data in a field, in a form, on a page of a site. Incoming traffic is scrutinised for malware, advanced persistent threats, application cloaking, geofencing, and other IP controls, plus the service defends against application-based DDoS attacks. Conversely, outbound data is screened to prevent sensitive information from leaving the network and entering the outside world, including credit card data, private records, or any other customised intellectual property. Through policy-driven management, it leaves no gaps in your public cloud security posture.

No specialist know-how necessary

The beauty of the Barracuda WAF is that it requires little in the way of specialist security knowledge to deploy a comprehensive and functional security solution. Templatised deployments based on common use cases and application scenarios offer a speedy route to web app protection. This includes pre-prepared policies for screening inbound and outbound traffic flows. Also by using the Barracuda Vulnerability Manager, which is a free tool, your site can be scanned for security risks. Then pairing it with the Barracuda Vulnerability Remediation Service, enables the WAF's configuration to be automatically updated with the findings of the scan, further reducing the need for specialist security skills. Yet, for advanced security professionals there is also the freedom to make near limitless changes to the service to achieve granular control and truly customised protection.

Cloud compatible commercials

In an on-premise infrastructure, being ready to scale usually means sizing and licensing for the highest demands and accepting the wastage of overprovisioned licenses and redundant capacity during non-peak times.

Applications running in the cloud will consume varying levels of resource during peak and non-peak times and the security measures they harness is one of those resources. Predicting resource usage can be tricky just as it is on-premise, so as a cloud service itself, the Barracuda WAF comes with the option of metered billing. This is usage-based billing that ensures protection stays in step with your application workload and automatically scales with it to meet demand. It means quality of service is always ensured and there are never any wasted licenses as you only ever pay for traffic secured and nothing else.

For more static environments there are other options for Pay-as-you-go (PAYG) and Bring-you-own-license (BYOL) where organisations may be using the WAF as a physical or virtual appliance on-premise and want to transfer this license to the cloud.

Ready to facilitate the rise of DevOps

With the rise of DevOps as an important team within many businesses, the public cloud has become the primary location for building new apps. DevOps teams want to remain agile and create their own security frameworks and then easily build them into the processes they follow. The Barracuda WAF has a full featured API interface which means it can be integrated into a host of DevOps tools and Continuous Integration and Continuous Deployment workflows - literally becoming part of the code building process. It ensures security controls can be automated at every stage of the app building process through development, test, staging, to production. And thanks to the metered billing, you only pay when the firewall sees test or production traffic.

Deploy whether you are live in the cloud or not

Helpfully, the Barracuda WAF can be activated at any time, not just when you're in flight with migrating an app to the public cloud. As such, for organisations who are already using public cloud services to host web apps there is no reason why the WAF cannot be activated to protect existing workloads. To avoid any confusion, if you are already running applications in the cloud, a conversation over security should be encouraged.

Fast-track to the cloud

Cloud Generation Firewalls present an exciting opportunity by offering enterprise organisations the peace of mind they have been searching for to better utilise the capabilities of the public cloud. Barracuda is clearing the way to migrate all sorts of apps to the cloud, safe in the knowledge that they are as secure on cloud as off it. The Barracuda WAF overcomes most, if not all of the hang ups commonly felt about the security posture of running critical apps and data in the public cloud, and opens the door to all sorts of benefits previously considered out of reach for certain business applications.

TIME TO CUT THE WAFle

Don't just take our word for it, try it for yourself and put the Barracuda WAF to the test. We're offering a 30-day free trial to protect and secure a public cloud workload of your choice.

THE NEXT STEP

Alternatively, if you're not yet ready for a trial, we'd love to show you the service working for real in a live demo or by showing you how to use the Barracuda Vulnerability Manager to scan your site and see how safe your application currently is.

To accept the trial, see a demo or to arrange a scan, contact your Servium Account Manager, email us at hello@servium.com or call on +44 (0)303 334 3000.

ABOUT SERVIUM

Servium is dedicated to creating great IT experiences - we seek to win the hearts and minds of IT strategy-makers, professionals and users. Our attitude is that no challenge is too big, no detail too small. We tackle both the ordinary and the extraordinary with the same focus and originality of thought that ensures solutions make a difference. It means we're one partner ready to assemble all the technology and know-how every medium to large organisation relies on. Matched by straight-talking, real-world experience and amazing service, our customers enjoy exceptional value; the product of the best innovation, latest thinking and a thriving ecosystem of technical experts.

Servium | Barracuda