Ebook:

5 REASONS WHY YOU NEED A CLOUD-NATIVE WEB APPLICATION FIREWALL (WAF)

ORACLE® Dyn

dyn.com ☎ 603 668 4998 @dyn

5 Reasons Why You Need a Cloud-Native Web Application Firewall (WAF)

DDoS attacks. Bad bots. Web server vulnerability exploits. The list of threats to websites and internet-facing applications grows longer all the time. Malicious hackers are constantly targeting web servers, IoT devices, and other internet-connected endpoints to crash sites, steal data, and wreak havoc on your IT infrastructure. The best way to protect your business from harmful incoming web traffic is to block it with a powerful web application firewall (WAF).

But it’s important to know that the WAF market is changing fast. While many companies rely solely on appliance-based WAF solutions, the market requirements for web application security are clearly shifting toward an edge security platform approach that combines a variety of protections suited to distributed hybrid and multicloud environments.

“By 2020, standalone WAF hardware appliances will represent fewer than 20% of new WAF deployments, which is a decrease from today’s 35%,” IT analyst firm Gartner predicts in its August 2018 Magic Quadrant for Web Application Firewalls. “By 2023, more than 30% of public-facing web applications will be protected by cloud web application and API protection services that combine distributed denial of service (DDoS) protection, bot mitigation, API protection, and WAFs. This is an increase from fewer than 10% today.”

Here's a quick look at the five main reasons why many organizations are adopting cloud-native WAF solutions:

1. They scale with your business.

Scalability is a major factor to consider when evaluating WAF solutions. That's because a WAF is typically configured as a reverse proxy, which means it serves as the entry point—the last line of defense—before incoming web traffic hits your website and internet-facing applications.

A key benefit of cloud-native WAF solutions is that they leverage the power and scalability of massive edge networks with globally distributed points of presence to ensure minimum latency and maximum coverage. If incoming web traffic sharply increases for any reason, you can rest assured that a cloud-native WAF will leverage its underlying cloud infrastructure to rise to the challenge and quickly isolate your endpoints from incoming threats.

Did you know...

not all cloud WAF solutions are created equal?

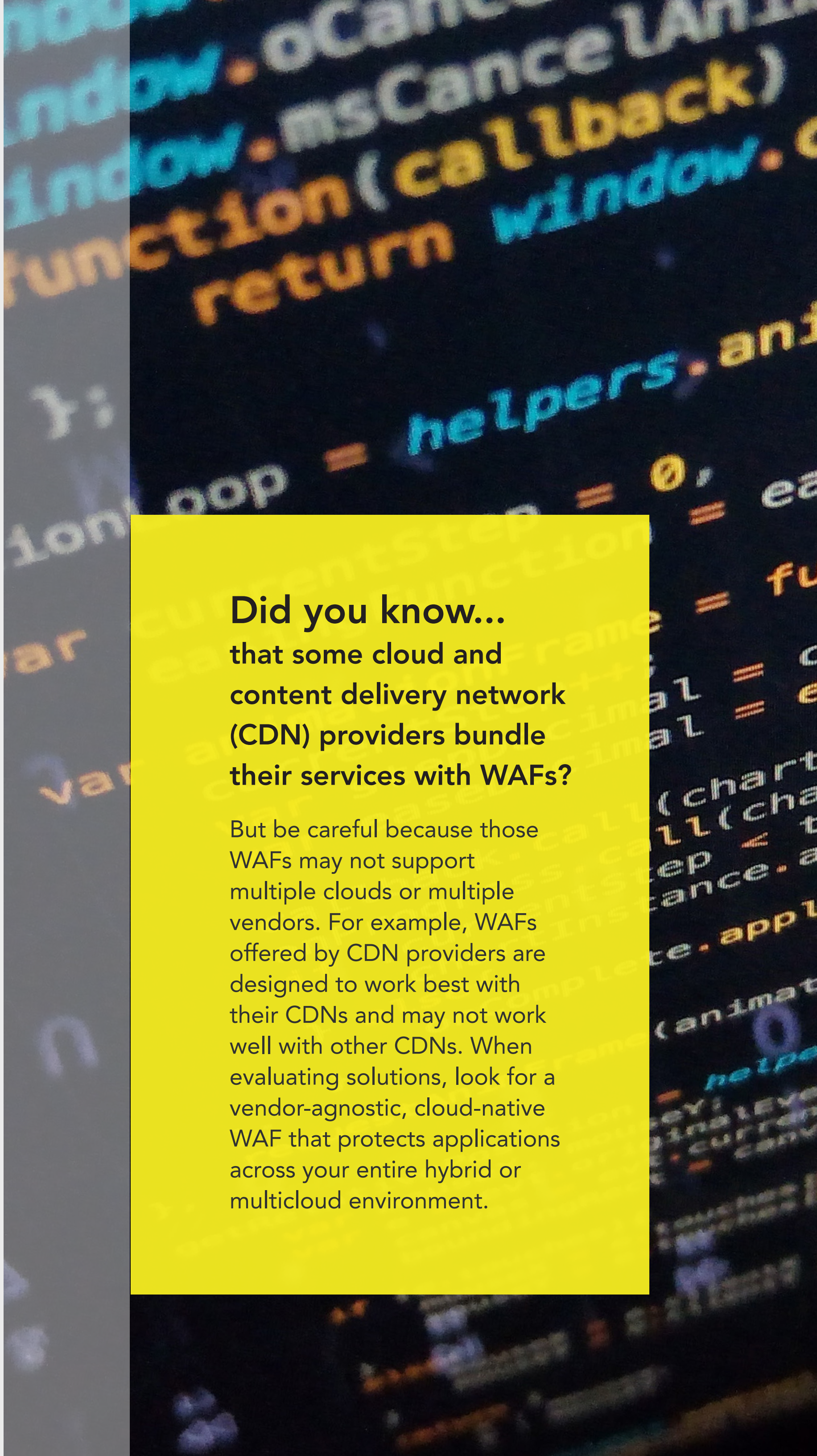
Many providers offer WAFs as part of a virtual machine (VM) cloud architecture. But cloud-hosted VMs do not scale as easily as true, cloud-native WAFs. When evaluating WAFs, be sure to look for a purely cloud-native solution that's supported by a global cloud infrastructure.

2. They block attacks outside your perimeter.

The further away a cyberattack is from your internal infrastructure when it's identified and mitigated, the better. One benefit of a pure, cloud-native WAF is that it blocks malicious traffic long before it reaches your network. But it's not only far away in terms of geographic distance—it's also physically disconnected from your internal infrastructure. It's separated by secure layers that are independent from where websites and applications are hosted, regardless of whether they're hosted on your premises or in the cloud. Once under the protection of a cloud-native WAF, your applications will only accept traffic from secure WAF nodes, completely isolating your endpoints from incoming cyberthreats.

3. They provide the best security for multicloud deployments.

Most companies today embrace hybrid or multicloud computing strategies. The best cloud-native WAFs are vendor-neutral, which means they can protect your network edge from malicious traffic regardless of how many public cloud or on-premises infrastructure providers you use. The right cloud-native WAF will provide you with an independent platform for securing all websites and internet-facing applications no matter where they reside.



Did you know...

that some cloud and content delivery network (CDN) providers bundle their services with WAFs?

But be careful because those WAFs may not support multiple clouds or multiple vendors. For example, WAFs offered by CDN providers are designed to work best with their CDNs and may not work well with other CDNs. When evaluating solutions, look for a vendor-agnostic, cloud-native WAF that protects applications across your entire hybrid or multicloud environment.

4. Managed services ease your burden.

The best cloud-native WAFs are managed 24/7 by a team of experienced internet security experts who monitor your environment and recommend proven threat mitigation steps when issues arise. The benefits of managed WAF services include significant risk reduction. They also reduce your management burden because WAF configuration, monitoring, tuning, and incident response is handled for you. Continuous monitoring protects your business from unplanned downtime and the resulting damage to your brand's reputation. Additionally, managed services enable you to spend more time focusing on your core business and improving the bottom line.

5. They have low total cost of ownership.

Cloud-native WAFs provide the highest level of web application security without a major upfront investment in resources or ongoing costs related to maintenance, hardware replacement, and software upgrades. Cloud-native WAFs offer ease of deployment and predictable subscription pricing, which makes it easier to plan your annual budget.

Why Oracle WAF?

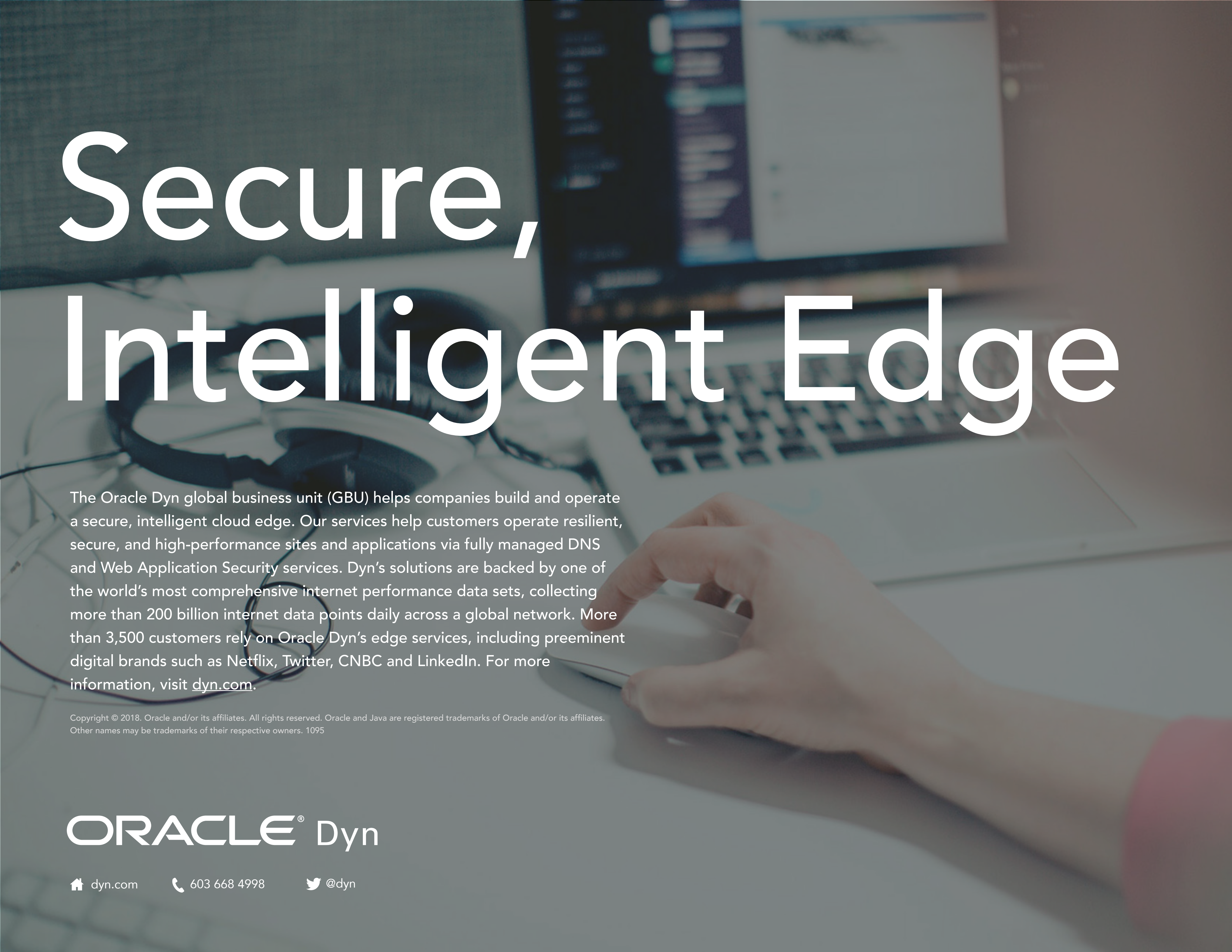
Oracle WAF is the right choice for any business that wants to tighten security at the web application layer. Oracle WAF is 100 percent cloud native and vendor agnostic, which means it can protect your entire hybrid or multicloud environment regardless of where internet-facing applications are hosted. It's monitored 24/7 by our security operations center experts, and it leverages the power of automated threat identification and a global cloud infrastructure with points of presence spread over the world.

Checklist: Key questions to ask when selecting a cloud-based WAF

If you answer "yes" to the following questions, you'll know you've found the right cloud-based WAF solution.

1. Can it protect internet-facing applications across your entire hybrid or multicloud environment?
2. Is it a true cloud-native solution and not simply an appliance or a WAF that is deployed as part of a VM cloud architecture?
3. Is it an extremely scalable, cloud-native WAF that is supported by globally distributed points of presence?
4. Will it isolate your infrastructure from cyberthreats by ensuring that web applications only accept traffic from WAF nodes?
5. Is it managed 24/7 by a team of internet security experts?
6. Can the WAF provider support your requirements for bot mitigation and API protection now and in the future?
7. Does it offer predictable subscription pricing without requiring a major upfront investment in equipment?

Ready to make the move? Visit: dyn.com/waf



Secure, Intelligent Edge

The Oracle Dyn global business unit (GBU) helps companies build and operate a secure, intelligent cloud edge. Our services help customers operate resilient, secure, and high-performance sites and applications via fully managed DNS and Web Application Security services. Dyn's solutions are backed by one of the world's most comprehensive internet performance data sets, collecting more than 200 billion internet data points daily across a global network. More than 3,500 customers rely on Oracle Dyn's edge services, including preeminent digital brands such as Netflix, Twitter, CNBC and LinkedIn. For more information, visit dyn.com.

ORACLE® Dyn

dyn.com ☎ 603 668 4998 @dyn