ORACLE® Dyn

RELENTLESSLY PROTECTING THE EXPERIENCE

Oracle Dyn Web Application Security

Start with a Secure, Intelligent Edge

DDoS attacks. Botnets. Malicious hackers. The internet can be a dangerous place—and it's growing more volatile all the time. Attackers have access to an ever-widening range of sophisticated tools designed to exploit weaknesses in your defenses. Simply guarding your perimeter is no longer enough. Today's businesses require dynamic, modern security solutions that automatically detect and thwart incoming attacks before they reach your websites and applications.

Oracle Dyn Web Application Security is the answer. With advanced bot detection and mitigation capabilities, DDoS protection, and a powerful, cloud-based web application firewall (WAF), Oracle Dyn Web Application Security relentlessly defends your internet-facing services against inbound cyberthreats. Whether your sites and applications are hosted on your premises or in a hybrid or multicloud environment, Oracle Dyn Web Application Security strengthens your security posture from edge to core.

The Power of an Integrated Platform

To keep websites and internet-facing applications safe, today's businesses require an advanced, cloud-based security platform that offers protection across a wide range of cyberthreats. It need to be "always-on" and fully managed 24/7/365 by security experts trained to monitor and mitigate threats on your behalf. "By 2023, more than 30% of public-facing web applications will be protected by cloud web application and API protection (WAAP) services that combine distributed denial of service (DDoS) protection, bot mitigation, API protection and WAFs," according to Gartner. Oracle Dyn Web Application Security provides a full complement of integrated security solutions. Unlike point products that only offer protection for specific attack types, our integrated platform extends your security posture to protect against a wide range of attack vectors targeting your web applications.

A significant portion of all cyberattacks are directed at web applications. In fact, attacks on web applications are the number one cause of data breaches.

Source:
Verizon: Data Breach Investigations Report, 2017

Advanced Web Application Security

Cybercriminals use sophisticated attack techniques and botnets that can exponentially increase their capabilities. To combat this ever-evolving threat, you need the right tools and expertise on your side. The Oracle Dyn platform provides an integrated set of security defenses that can rapidly adapt to new threats. It's fully managed and backed by a dedicated, global security operations center (SOC). At the heart of the solution we deliver key capabilities, including:

- Over 300 rules, spanning OWASP top 10 web application security risks
- Flexible, configurable rules and compliance-based rulesets
- Automated threat identification and recommended WAF rule actions
- Extensible APIs to integrate into security information, event management (SIEM) and third-party applications

Supervised Machine Learning

Automated security solutions that rely on artificial intelligence (AI) and machine learning (ML) are important concepts for fighting sophisticated cybersecurity threats. Bad actors are already using automation, bots, and AI. Oracle Dyn Web Application Security gives you the power to fight fire with fire.

Faster Time to Automated Threat Detection

Oracle Dyn Web Application Security leverages supervised ML to dynamically and automatically update your security posture. Based on patent-pending ML algorithms and coupled with threat intelligence and big data analytics, the Oracle Dyn platform inspects web traffic in real time to identify threats and anomalies and dynamically update security postures accordingly.

Web Application Firewall

Cybercriminals can easily overwhelm or breach an organization's perimeter-only defenses. Our cloud-based security platform expands your defenses globally and thwarts attacks of all sizes. The Oracle Dyn WAF combines a powerful group of protection mechanisms designed to address the specific requirements of today's multicloud and hybrid cloud IT environments.

Our WAF features include:

- Cloud-based, highly scalable, global workload resources
- Automated threat detection
- Hundreds of configurable rulesets
- Shared, global threat intelligence
- Support for custom rulesets
- Integrated, platform-based solution that includes API security, bot management, and DDoS protection

Bot Management

Bots are everywhere, accounting for more than half the traffic to some sites.[1] Some bots are good for your business. Some are bad. But they all need to be managed. Traditional, on-premises WAFs typically lack advanced techniques needed to combat the increasing level of sophistication we see in today's bots. Our WAF's bot management capabilities include:

- Access control, IP rate limiting, request limiting, and good bot whitelisting
- Advanced bot detection techniques such as JavaScript challenge, human interaction challenge, and device fingerprinting to identify and block bad bots
- Supervised machine learning techniques that fuel the industry's most innovative and effective solution for mitigating bot-based attacks

API Security

API endpoints, an often-overlooked liability, have become a weak link in today's enterprise networks. Unlike traditional API protection solutions, our API security is integrated into our platform, easily deployed, and managed 24/7. Continuous monitoring and tuning of API security policies ensure the highest level of API security.

Capabilities and benefits include:

- Advanced validation techniques
- Stronger protection than IP rate limiting alone

1 Source: Ponemon Institute, 2017

- Mobile app integration
- In-depth reporting and analytics
- Cloud-based WAF means no new hardware to install or manage

DDoS Protection at the Application Layer

Application layer DDoS attacks (Layer 7) are dangerous. They consume server, application, origin, database and search index resources, as well as ecommerce components, and API endpoints.

Oracle Dyn protects applications from Layer 7 DDoS in real time with algorithms designed to detect and block bad bots while allowing legitimate user traffic to access internet-facing endpoints. Our application security platform eliminates the threat of Layer 7 attacks and ensures that server and application resources are always available to legitimate clients.

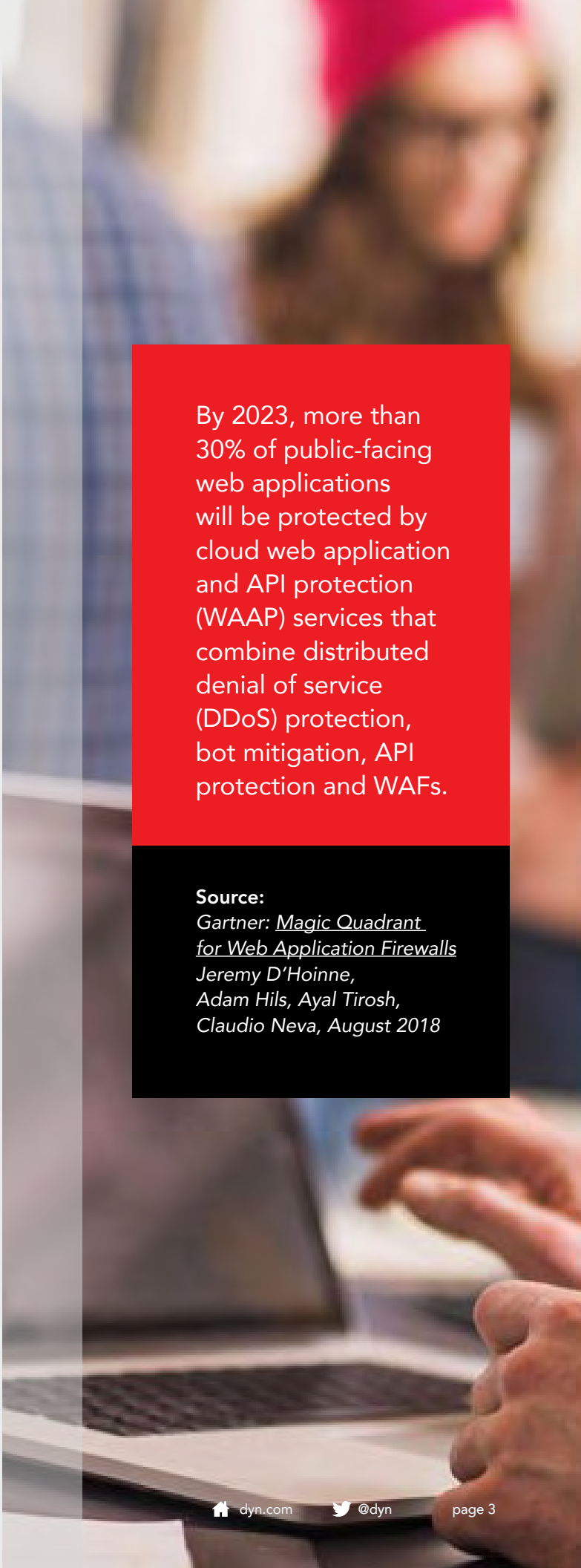
Web-connected Network Security

Cybercriminals use large botnets made up of thousands of infected devices to launch larger DDoS attacks, over longer periods of time, targeting several areas between users and web applications. Oracle delivers cloud-based protection to mitigate volumetric (Layer 3/4) DDoS attacks. With the ability to detect and mitigate flooding attacks in less than one minute, networks, servers, and applications are completely protected against DDoS-induced outages.

DDoS Protection at the Network Layer

The Oracle Dyn solution detects and mitigates high-volume, Layer 3/4 DDoS attacks closest to the source, ensuring the availability of your network resources even when under sustained attack. Benefits include:

- Extremely fast time to mitigation with RapidBGP™
- < 60 seconds between detection and mitigation using automated BGP routing
- Lowest latency impact even when under DDoS attack
- Surgical mitigation by diverting attack traffic to the Oracle Dyn DDoS protection cloud
- Geographically dispersed DDoS mitigation centers



By 2023, more than 30% of public-facing web applications will be protected by cloud web application and API protection (WAAP) services that combine distributed denial of service (DDoS) protection, bot mitigation, API protection and WAFs.

Source:
Gartner: Magic Quadrant for Web Application Firewalls
Jeremy D'Hoinne, Adam Hils, Ayal Tirosh, Claudio Neva, August 2018

Managed Security Service

Many IT and security leaders today leverage managed security services that include 24/7 SOCs to reduce the strain on internal teams, while effectively managing and mitigating threats to their organizations. Implementing the right policies on your own in the right way, and constantly monitoring and evolving your security posture is a daunting task—one you don't have to worry about with Oracle Dyn Web Application Security. Our managed security services form a critical line of defense in protecting your organization's assets, data, operations, and reputation. Our managed security model enables you to:

- Take advantage of cloud economics, shared intelligence, and real-time expertise
- Eliminate the need to invest in more human and technical resources
- Supplement internal resources dedicated to ongoing solution management and maintenance

Unmatched Protection

Oracle Dyn provides a complete, integrated application security solution managed 24/7 by top cybersecurity experts. Our platform-based approach enables your business to defeat the broad spectrum of application attack vectors you're most likely to encounter.

Key differentiators include:

- Multitenant, cloud-based services with globally-distributed POPs
- Geographically dispersed Layer 3/4 DDoS mitigation centers
- Globally dispersed security operation centers monitoring and mitigating attacks 24/7
- Powerful AI and proprietary ML algorithms
- Shared threat intelligence, including big data analytics
- Backed by industry-leading security and network operations centers

The Oracle Dyn Web Application Security platform is the industry's most innovative and integrated solution available—leveraging supervised machine learning and automation to proactively combat the broadest range of cyberattacks targeting your networks, websites, and applications.

ORACLE® Dyn

Oracle Dyn, an Oracle Cloud Infrastructure global business unit (GBU), helps companies build and operate a secure, intelligent cloud edge, protecting them from a complex and evolving cyberthreat landscape. Our managed Web Application Security, DNS, and Email Delivery services are powered by a global network that drives 40 billion traffic optimization decisions daily. More than 4,500 customers rely on Oracle Dyn edge services, including preeminent digital brands such as Netflix, Twitter, CNBC, and LinkedIn. Deployed as standalone solutions or fully integrated with Oracle Cloud Infrastructure, Oracle Dyn edge services are the key to delivering resilient, high-performance sites and applications. For more information, visit dyn.com.