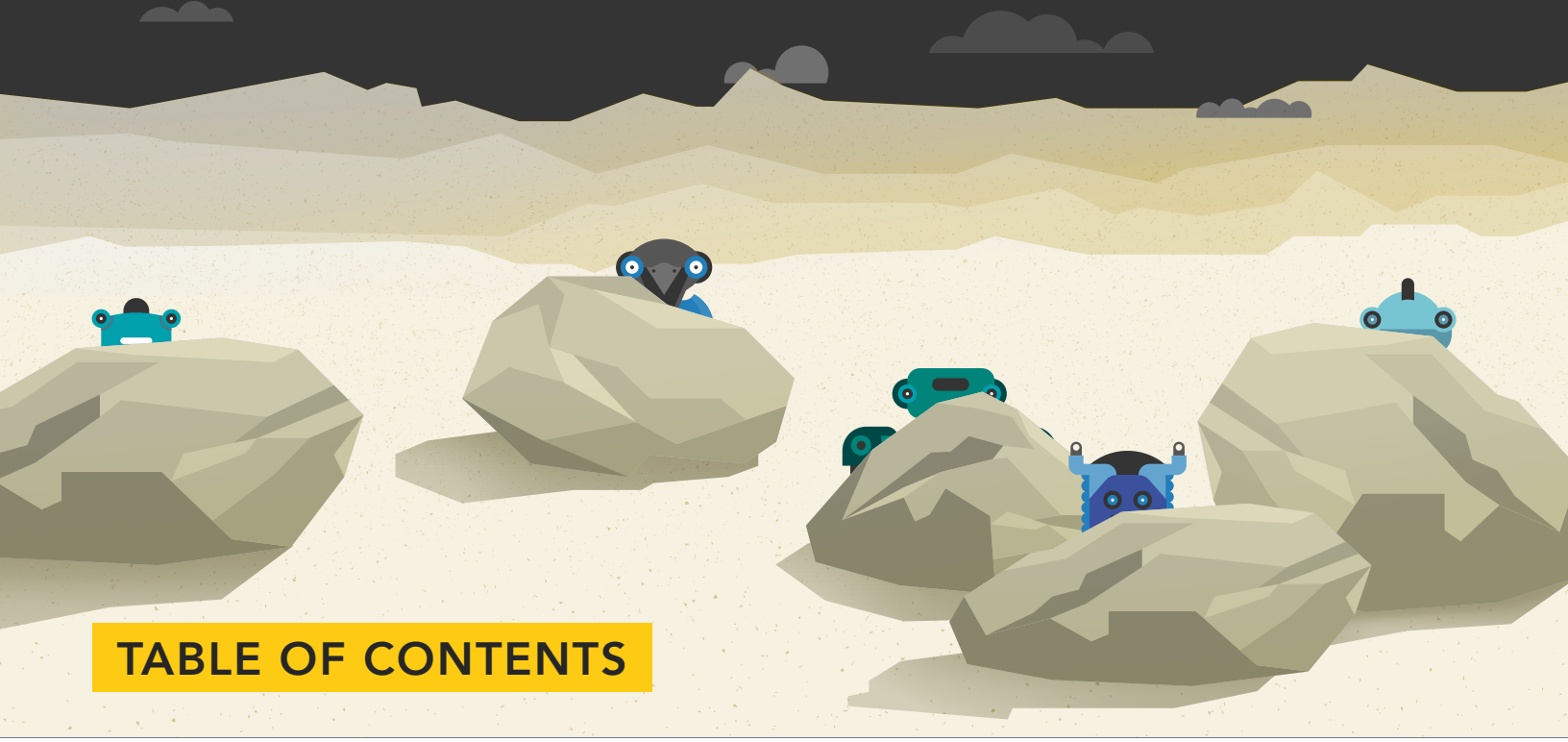
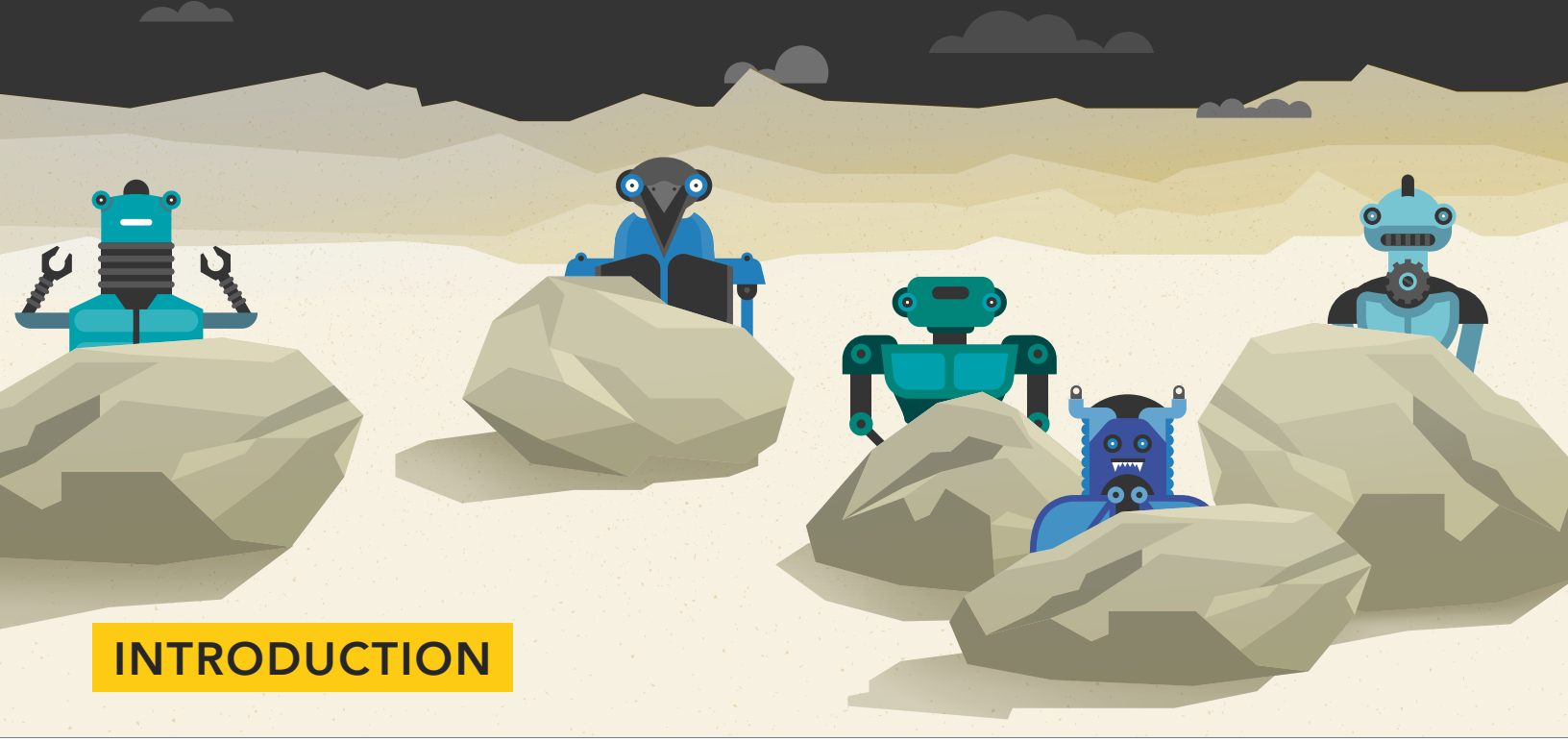
# Intelligent Web Application Security

## NEUTRALIZING THE BOT EPIDEMIC IN TODAY'S THREAT LANDSCAPE



# TABLE OF CONTENTS



# INTRODUCTION

**All corners of the IT infrastructure are vulnerable to cyberattack. But applications that are exposed to the Internet are particularly at risk. IT organizations have put much-needed focus on securing the network's endpoints, but web applications are also exposed and exploited, giving cybercriminals access to critical infrastructures and data. A major perpetrator of these evolving threats is bots.**

Today's cyberattacks aren't limited to an individual attack vector, an individual system, or an individual company. Threat actors can spread malicious content and execute attacks all over the world, crossing borders—and industries—in a matter of seconds. Through the use of bots, these threats are becoming more sophisticated, proliferate faster, and are increasingly difficult to detect. In this environment, organizations can no longer rely on static controls. Nor does a simple web application firewall provide sufficient protection. Web application security has to evolve to include a dynamic, advanced bot management solution.

CHAPTER 1

# NAVIGATING A CHANGING THREAT LANDSCAPE

**According to a recent Spiceworks survey, 78% of respondents say they've had a security issue. They've seen DDoS attacks alone increase 25% from 2016 to 2017.**

In response to these growing threats, organizations surveyed say that about 73% of their web presence is now covered by a web application firewall. Despite this layer of protection, 45% of respondents are concerned about sensitive data being exposed, and only 19% feel completely prepared for a web attack.

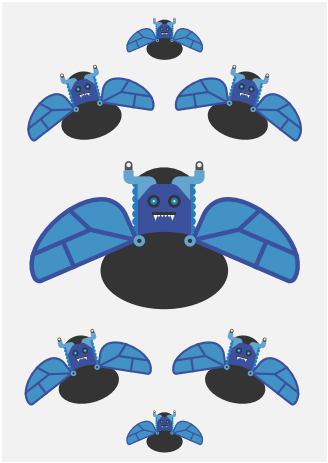
These concerns are well founded. The 2018 Verizon Data Breach Investigations Report (DBIR) revealed that web application attacks are the primary cause of data breaches today.[1] The problem is two-fold. First, web app attacks are more advanced than ever, utilize a wide range of techniques and technologies such as bots, change on a daily basis, and are getting harder and harder to detect, Second, traditional web application security solutions are not designed to address this multi-faceted problem.

Navigating this advanced and dynamic threat landscape requires equally advanced and dynamic technologies and best practices. Organizations have to acknowledge the risk that web app attacks represent—and prioritize web app security accordingly.

CHAPTER 2

# FIVE THREATS YOU SHOULD CARE ABOUT

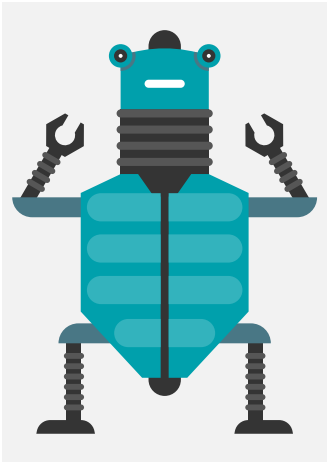
**Web application threats take many different forms—and are designed to carry out many different functions. Here are five of the most prevalent web app threats.**



## DDoS Attacks

According to the 2018 Verizon Data Breach Investigations Report, DDoS attacks are the #1 security incident reported in 2017.[1] And yet only 17% of the Spiceworks survey respondents feel completely prepared for a DDoS attack. DDoS attacks can result in everything from a poor user experience to taking you offline completely, both of which translate to significant revenue loss and can result in a diminished brand reputation. For organizations with high transaction volumes, a DDoS attack can have a massive effect on revenue within a matter of minutes.

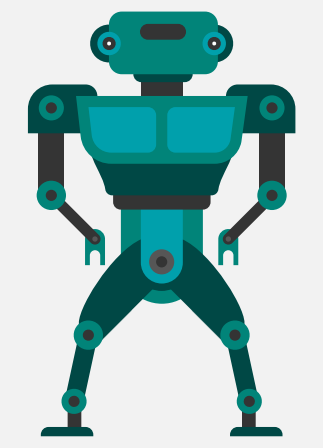
Advanced DDoS attacks like "Memcached" can hit a website with more than a terabyte of fake network traffic.[2] This attack exploits vulnerable memcached programs used by many IT admins to cache their web-server session data in order to accelerate site performance. In an always-on marketplace, occasional latency is inconvenient. The latency—or service outage—created by large-scale DDoS attacks is unacceptable. With the use of amplification services like memcached and the growing size of botnets, organizations can expect to see a steady rise in the size and scale of DDoS attacks.



## Malicious Bots

Bots have been growing as a percentage of website traffic since 2012.[3] They have the power to steal information, infect systems, and take applications offline. The proliferation and increased complexity of bots have made them a central player in the most effective attacks today. In addition, even the most benign bots consume valuable bandwidth and CPU, driving up costs and creating poor user experiences.

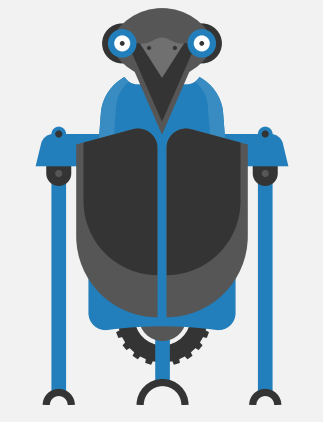
Examples of malicious bots include spam/email bots, impersonator bots, zombie bots used to create a botnet, download/transfer bots, spy bots, scraper bots, and click/ad fraud bots. Exactly how powerful are they? Necurs and Gamut alone are responsible for 97% of spam email on the internet today.[4] But traditional web application firewall (WAF) technology is not effective against bot-based attacks—or against the volume of traffic that bots can generate. The only way to combat the growing bot epidemic is to utilize a WAF that incorporates advanced bot mitigation and management techniques.



## Web Application Attacks

Despite widespread use of web application firewalls, web app attacks continue to grow, increasing 69% in Q3 2017 over Q3 2016.[5] In fact, they increased 30% just from Q2 2017 to Q3. Weak applications are particularly vulnerable, as are the databases that live downstream from them.

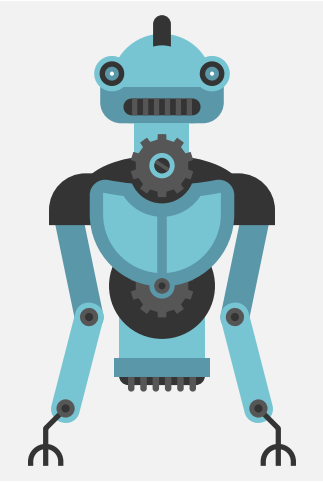
The most common web application attack vector in Q3 2017 was SQL injection (SQLi) attacks, which place malicious code in SQL database statements, including code that can completely destroy a database.[5] These attacks are particularly brutal because they can scale easily and can be automated to locate any vulnerable system, as opposed to attacking specific targets.



## API Attacks

Machine-to-machine communications between mobile apps and devices and backend API servers are subject to the same vulnerabilities as websites. Without the HTTPS protection of web traffic, these communications turn any mobile device into a potential attack entry point, including serving as a gateway for DDoS attacks.

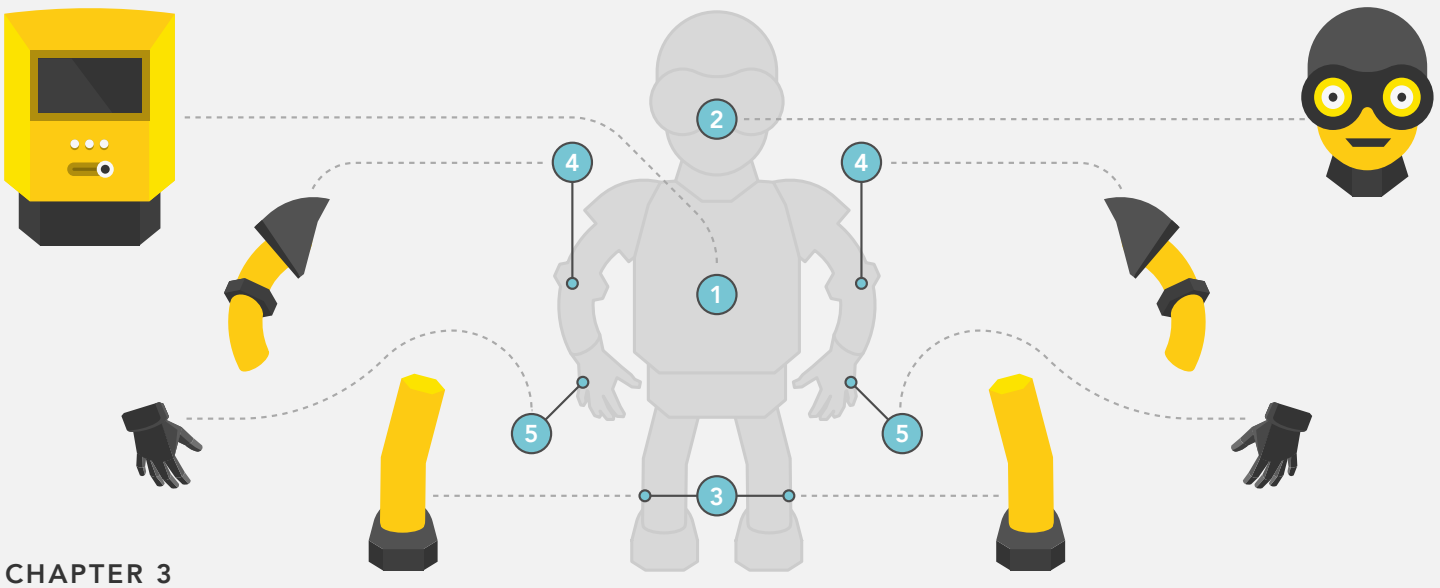
APIs expand the available attack surface significantly—and can expose sensitive data as well. "Input parameter attacks" are used for this exact purpose, manipulating vulnerable applications by introducing malicious input that is then executed without first being validated. Basic web application firewalls are not designed to prevent these attacks.



## Malware Uploads

Despite increasingly elaborate security measures, websites can still be easy targets for malware uploads, including ransomware. 2017 has been described as "The Year of Ransom," and 2018 is poised to retain the title as hackers perfect their ransomware delivery techniques.[6] The five largest ransomware attacks in 2017 were WannaCry, NotPetra, Locky, Crisis, and JAFF, and both Locky and JAFF were distributed by the botnet Necurs.[7]

Whether a site is designed to allow user uploads or not, systems and data are vulnerable to a wide range of malicious assaults via malware, and most web application firewalls have no context for handling them. These solutions often miss malware uploads because they aren't designed to examine payloads.




CHAPTER 3

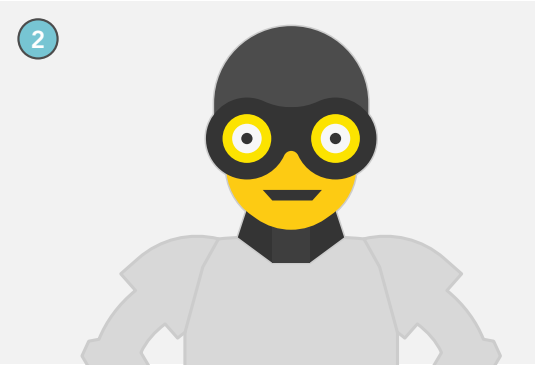
# CONSTRUCTING AN INTELLIGENT SECURITY SOLUTION

**Addressing these and other advanced threats requires more than a standalone web application firewall. It calls for an intelligent approach to web app security—one that includes advanced bot mitigation and management technologies such as pattern recognition to fight sophisticated threat actors. What does intelligent web app security look like? It's a comprehensive set of tools that provide extensive coverage that is easy to manage. It enables application-specific cybersecurity controls for customized protection that meets the unique requirements of a demanding environment.**

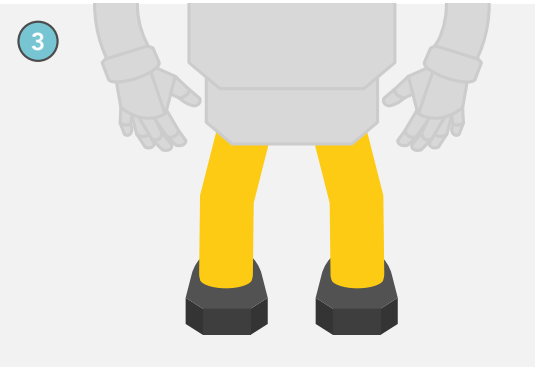
The Spiceworks survey revealed that 75% of organizations in North America manage their cloud security in-house. These organizations may not have the bandwidth or expertise to stay on top of rapid security changes. An intelligent approach to web app security can help by allowing organizations to:

- Use an integrated platform that includes bot management, API security, DDoS protection and malware protection

- Replace antiquated and obsolete security systems

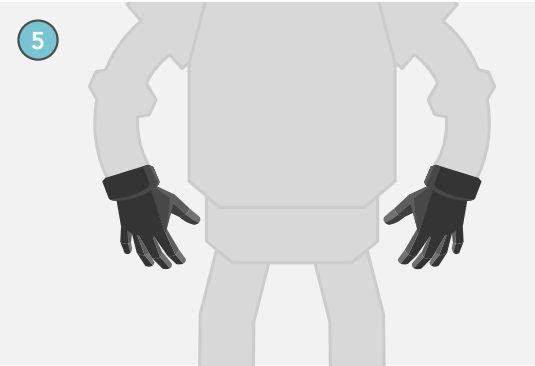



- Move key security capabilities to the cloud




- Leverage the expertise of cybersecurity experts on-demand


- Stay continuously armed with the latest web app security technology




CHAPTER 4

# INTRODUCING ORACLE DYN WEB APPLICATION SECURITY

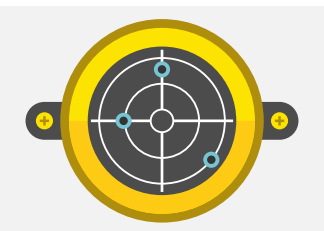
**The Oracle Dyn Web Application Security Suite protects web applications and their underlying networks and databases with a comprehensive portfolio of solutions. The Oracle Dyn Web Application Security Suite goes beyond basic web application firewall capabilities, providing multiple tools on one integrated platform:**

## Oracle Dyn Bot Manager:

An essential security tool that detects and blocks malicious bot traffic, validates and prioritizes authorized user traffic, prevents content and price scraping, and protects against web-based phishing, spam, chatbots, click fraud, credential stuffing, vulnerability scans, and code injections.

## Oracle Dyn Web Application Firewall:

A proven, cloud-based web app firewall provided as a fully managed 24/7 security service, with granular access controls, geo and URL blocking, unlimited DDoS mitigation, real-time threat intelligence monitoring using global threat databases, and pre-built rulesetsfor PCI DSS, CAPEC, and others.



## Oracle Dyn DDoS Protection:

A monitoring and proprietary signaling solution with fully automated 60-second mitigation, subnet and single IP protection, extensive transit and peering capacity, and unlimited usage—monitored and managed 24x7 by top cybersecurity and DDoS experts.

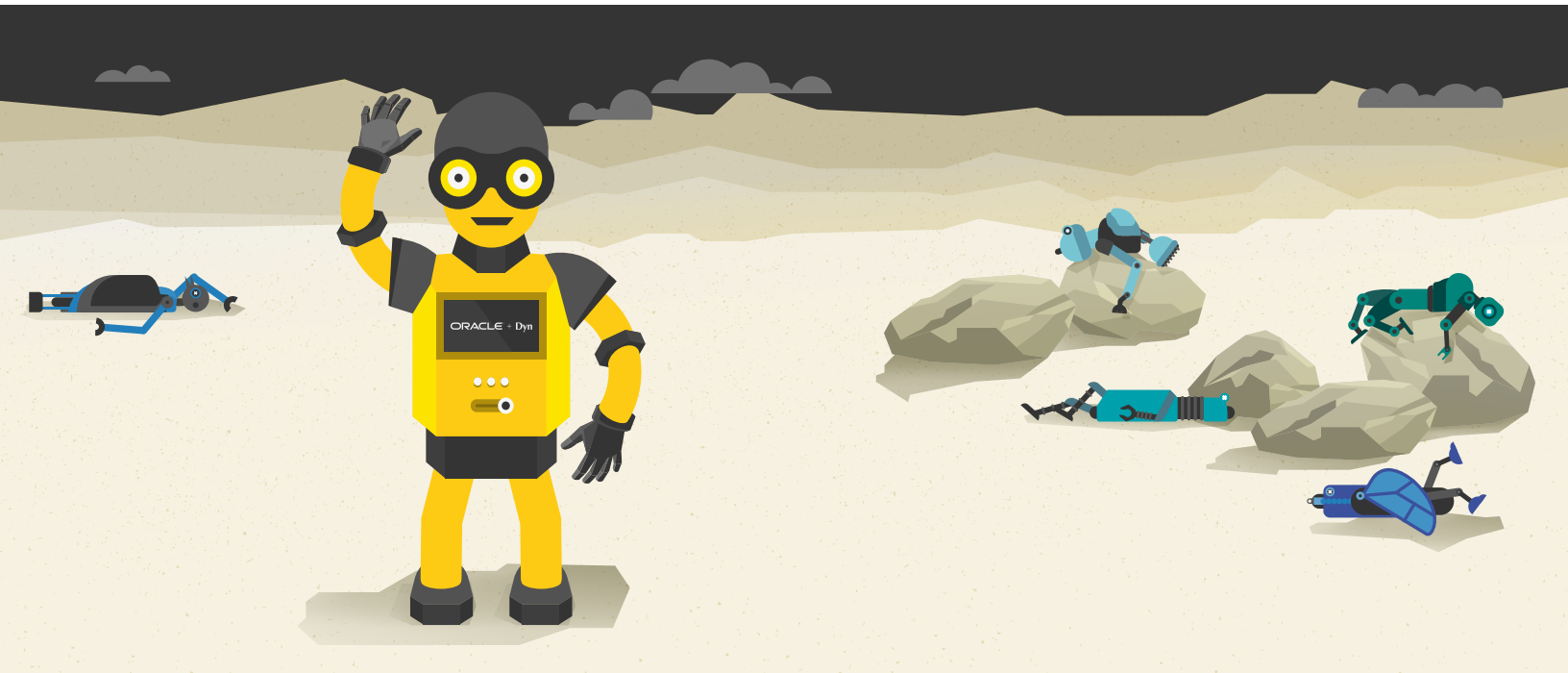
### Oracle Dyn API Security:

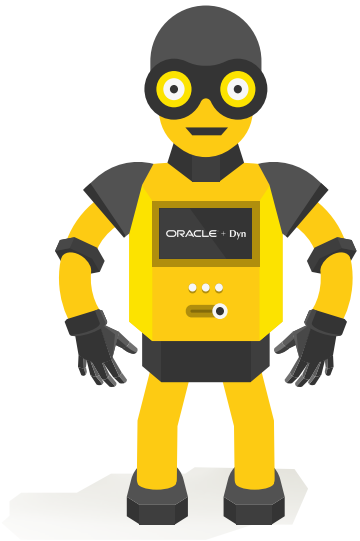
A cloud-based solution designed to protect API calls for native mobile apps and server-to-server communication, with advanced token-based validation techniques, full access control, rules designed specifically for API security, and in-depth reporting and analytics.

### Oracle Dyn Malware Protection:

An enterprise-class, cloud-based, fully managed security solution that provides unparalleled insight, visibility, and control over uploaded files to websites, ensures only legitimate traffic reaches your critical web applications, and detects and blocks malware and other malicious web traffic—all with no performance impact.

Bots are wreaking havoc on the Internet, and the Oracle Dyn Web Application Security Suite provides highly effective protection through elegantly designed solutions for every aspect of the bot epidemic. As a managed cybersecurity solution that operates 24x7x365, the Oracle Dyn Web Application Security Suite offers global coverage, automation, detection, and mitigation of advanced cyberthreats. It can help your organization navigate today's threat landscape by providing the intelligent approach to web application security that you're looking for.






# NEXT STEPS

**Ready to find out how the Oracle Dyn Web Application Security Suite can protect your organization from today's complex digital threats?**

START HERE

## About the Spiceworks Survey

Oracle Dyn commissioned Spiceworks to conduct a survey in February 2018. This survey targeted IT decision-makers, including IT directors, IT managers, and other IT staff, to understand current perceptions and practices around security, including web application security. Survey results included responses from approximately 200 participants in North America and EMEA who work at organizations with 250 or more employees.

## Sources


[1] "2018 Data Breach Investigations Report," *Verizon*, 2018. www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

[2] Vaughan-Nichols, Steven J., "Memcached DDoS: The biggest, baddest denial of service attacker yet," *ZDNet*, March 1, 2018. www.zdnet.com/article/memcached-ddos-the-biggest-baddest-denial-of-service-attacker-yet

[3] Glaser, April, "Internet traffic from bots surpassed human-generated traffic in 2016," *Recode*, May 31, 2017. www.recode.net/2017/5/31/15720396/internet-traffic-bots-surpass-human-2016-mary-meeker-code-conference

[4] Cimpanu, Catalin, "Necurs and Gamut Botnets Account for 97% of the Internet's Spam Emails," *BleepingComputer*, March 12, 2018. www.bleepingcomputer.com/news/security/necurs-and-gamut-botnets-account-for-97-percent-of-the-internets-spam-emails/

[5] Rayome, Alison DeNisco, "Report: Web application attacks up 69% in Q3 2017, here's what to do," *TechRepublic*, November 28, 2017. www.techrepublic.com/article/report-web-application-attacks-up-69-in-q3-2017-heres-what-to-do/

[6] Herberger, Carl, "Cyber Security Predictions," *Security Boulevard*, December 12, 2017. https://securityboulevard.com/2017/12/cyber-security-predictions/

[7] "The Five Largest Ransomware Attacks of 2017," *InfoSec Institute*, January 18, 2018. http://resources.infosecinstitute.com/five-largest-ransomware-attacks-2017/#gref