# Solving Together

## We protect your cloud future

rackspace technology | Akamai

Rackspace Managed Security accelerates the time to detect and neutralize cyberattacks, mitigating the damage they can cause to your business. Advanced cloud security services help you stay one step ahead of attackers, with a multi-faceted security posture that encompasses people, processes and technology.

Akamai Edge Security solutions secure content, data and applications across all your data centers and cloud providers, so you can harness the power of a multicloud world while maintaining governance and control. Situated between you and potential attackers, Akamai stops attacks in the cloud, at the network edge, closer to attackers and before they can jeopardize your applications and infrastructure.

The combined capabilities of these two leaders provide businesses with comprehensive, multi-layered cybersecurity that is ideally suited to today's fast-changing multicloud reality. With security across the stack, Rackspace Technology and Akamai help prevent financial losses and reputational damage associated with potential breaches, while enabling the agility today's business environment demands.

### Surround and protect your entire architecture — core, cloud and edge

Rackspace Managed Security and Akamai Cloud Security team up to provide the following capabilities to customers across industries:

- **Protect apps and APIs:** Protect internet-facing apps and APIs deployed anywhere — in your data centers or in the public cloud.
- **Stop credential abuse:** Protect revenue, customer experience, and personal data from bots and fraud.
- **Move to Zero Trust:** Control corporate application access and protect users from targeted threats.

### Security tools and solutions

Rackspace and Akamai bring a broad range of solutions to bear on cutting-edge cybersecurity challenges, including the following:

- **Web application firewall** protects your web sites, web applications, and APIs from the largest and most sophisticated attacks.
- **DDoS protection** helps keep your applications and IT services available even through the largest attacks.
- **DNS protection** helps defend your authoritative DNS service from the largest DDoS attacks, DNS forgery and manipulation.
- **Bot management** delivers advanced bot detection to spot and avert the most evasive threats so you can implement a more effective bot strategy, bring scrapers under control, and mitigate credential stuffing.
- **In-browser threat protection** helps detect and mitigate web skimming, formjacking, and Magecart attacks that can lead to data breach, damage your brand, and subject your organization to substantial fines.
- **Secure enterprise application access** provides simple, secure remote access management that is easy for IT, provides inherently better security, and delivers an exceptional user experience.
- **Secure web gateway** enables security teams to proactively identify, block, and mitigate targeted threats such as malware, ransomware, phishing, DNS data exfiltration, and advanced zero-day attacks.
- **Identity cloud** is a fully SaaS-based solution that lets your customers create personal accounts on any device, gives them control and choice over the data they share, and protects them and your business from risk.
- **Managed security services** deeply roots our expertise and resources in your day-to-day security operations and offsets business risk.

**The number of distributed denial-of-service (DDoS) attacks in the second quarter of 2020 was three times higher than the amount recorded in the same quarter of 2019.[1]**

rackspace technology | Akamai

## Safety in the face of evolving threats

The prevalence and severity of cyberthreats expands every day, and protecting against them is mission-critical for businesses of every description. Rackspace Technology and Akamai can help guard your business against the dynamically evolving threat landscape.

- **Distributed denial of service (DDoS) attacks.** The number of distributed denial-of-service (DDoS) attacks in the second quarter of 2020 was **three times higher** than the amount recorded in the same quarter of 2019.[1]
- **Web application attacks.** In a recent ethical hacking study, penetration testers were able to breach **77%** of businesses through web application protection vulnerabilities.[2]
- **Application programming interface (API) attacks. 83%** of web traffic today is API-driven[3], and approximately 16% of organizations say their APIs are subject to daily injection attacks, with 15% experiencing data leakages as a result.[4]
- **Credential stuffing attacks.** In the third quarter of 2020 alone, **770 million** fraud attacks were made with ballot-stuffing techniques, which involve login attempts to web-based systems using stolen credentials.[5]
- **Script attacks.** Scanning the top 18,000 websites on the Alexa traffic list revealed that **70%** of the scripts running on those domains are from third parties, all of which are potential targets for JavaScript attacks.[6]
- **Zero trust security.** More than **70%** of organizations are considering adopting a Zero Trust security model following the COVID-19 pandemic and the associated transition to extensive remote work.[7]
- **Secure remote access.** Microsoft finds that, in response to the work-from-home paradigm shift, "Providing secure remote access to resources, apps, and data" is the **#1 challenge** reported by security leaders.[8]
- **Advanced persistent threats (APTs).** APTs represent the most critical cybersecurity challenges facing governments, corporations, and app developers; on average, it takes **240 days** to detect an APT-related breach.[9]

## When do you engage Rackspace Technology and Akamai?

At every stage of the digital transformation process, Rackspace Managed Security and Akamai Cloud Security offer a higher level of proactive security protection at lower cost than doing it yourself.

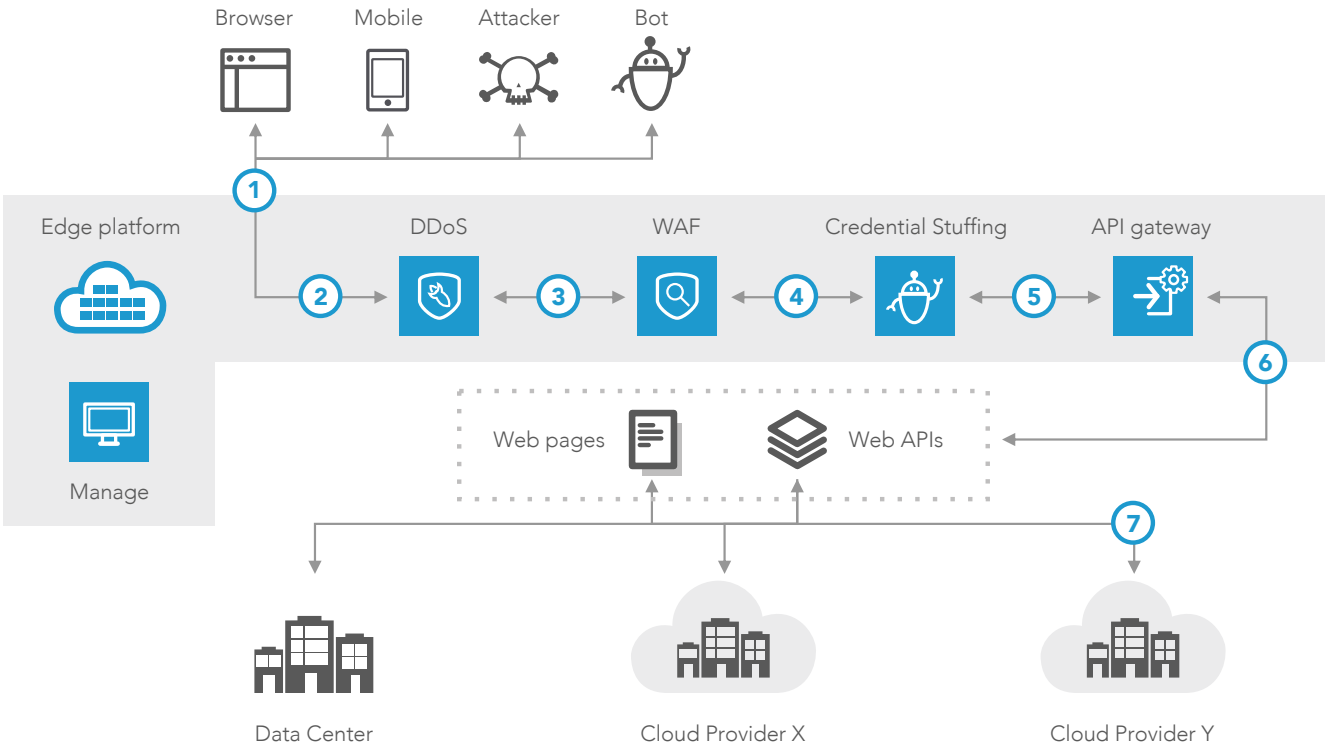
Engaging with Rackspace Technology and Akamai as early as possible reduces risk and improves TCO, enabling your business to move forward to its digital future with confidence, focusing on core competencies instead of security requirements.

## Security reference architectures

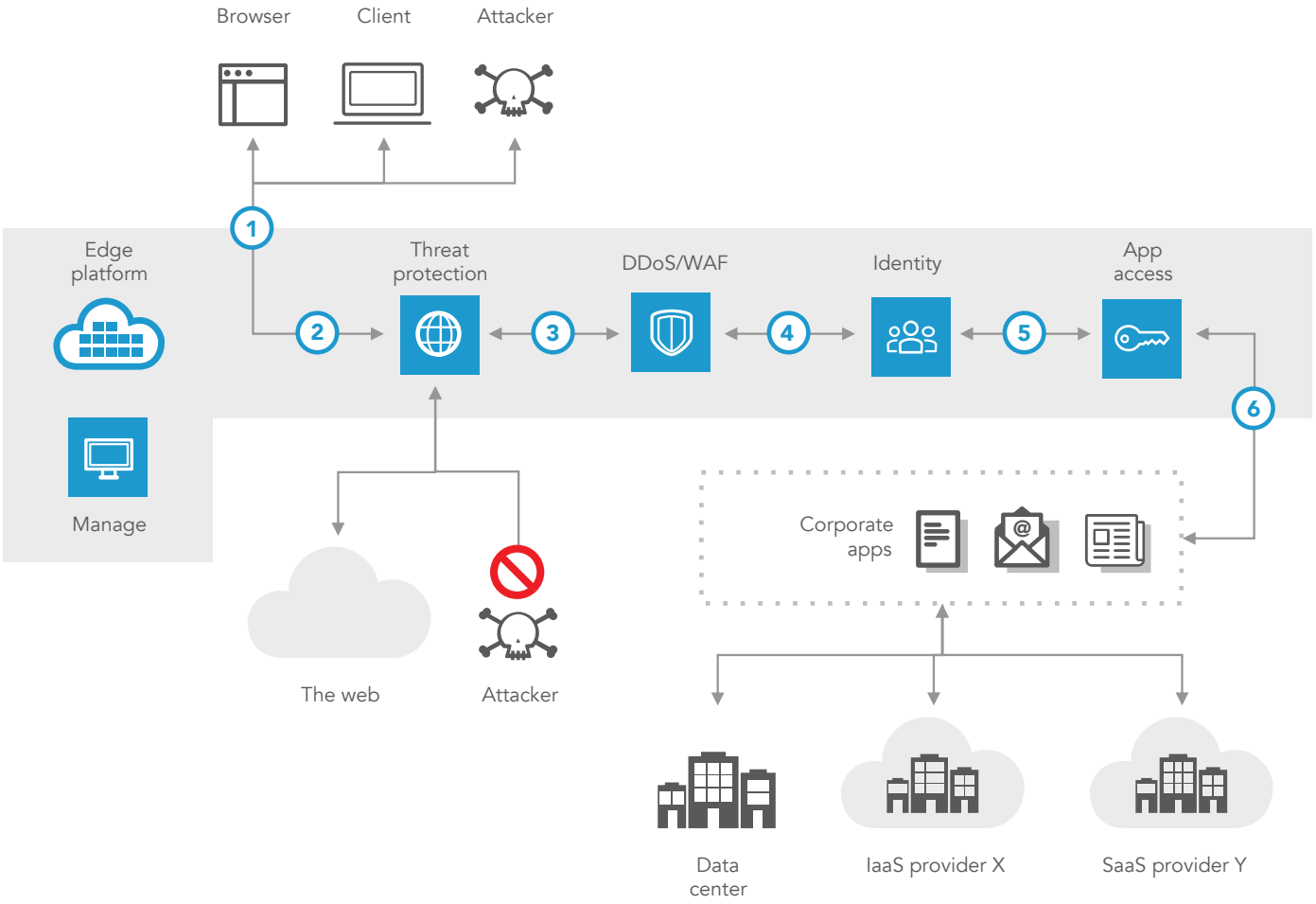
Security teams working to protect applications across multi-cloud environments need a single set of security controls that enable them to maintain a consistent security posture as well as scale their resources to meet changing business needs. The reference architectures shown here provide design patterns to help meet that goal.

**More than 70% of organizations are considering adopting a Zero Trust security model following the COVID-19 pandemic and the associated transition to extensive remote work.[7]**

### Securing multicloud



## Zero trust security





### Rackspace Contact

**Brian FitzGerald**
**Global Alliance Manager**
**brian.fitzgerald@rackspace.com**
**+1-(210)-312-3847**

### Akamai Contact

**James Bentley**
**Senior Partner Account Executive**
**jbentley@akamai.com**
**+1-(404)-442-6380**


[1] Dark Reading, August 10, 2020. "Q2 DDoS Attacks Triple Year Over Year: Report." https://www.darkreading.com/attacks-breaches/q2-ddos-attacks-triple-year-over-year-report/d/d-id/1338622.
[2] N. F. Mendoza, Tech Republic, August 13, 2020. "Report: Unskilled hackers can breach about 3 out of 4 companies." https://www.techrepublic.com/article/report-unskilled-hackers-can-breach-3-out-of-4-of-companies/.
[3] Akamai, February 2019. "[state of the internet] / security Retail Attacks and API Traffic Report: Volume 5, Issue 2." https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf.
[4] Ericka Chickowski, January 9, 2020. "API Security a Top Concern for Cybersecurity in 2020." https://securityboulevard.com/2020/01/api-security-a-top-concern-for-cybersecurity-in-2020/.
[5] Dark Reading, November 12, 2020. "Credential Stuffing Fills E-commerce Pipeline in 2020." https://www.darkreading.com/threat-intelligence/credential-stuffing-fills-e-commerce-pipeline-in-2020/d/d-id/1339435.
[6] Ido Safruti, Forbes, June 12, 2019. "Why SREs Should Worry More About Third-Party JavaScript." https://www.forbes.com/sites/forbestechcouncil/2019/06/12/why-sres-shouldworry-more-about-third-party-javascript/?sh=4515d6062f52.
[7] Robert Lemos, Dark Reading, July 13, 2020. "Zero-Trust Efforts Rise with the Tide of Remote Working." https://www.darkreading.com/perimeter/zero-trust-efforts-rise-with-the-tide-of-remote-working/d/d-id/1338343.
[8] Andrew Conway, Microsoft Security, August 19, 2020. "New data from Microsoft shows how the pandemic is accelerating the digital transformation of cyber-security." https://www.microsoft.com/security/blog/2020/08/19/microsoft-shows-pandemic-accelerating-transformation-cyber-security/.
[9] James Pita, TechBeacon. "Counter security threats with machine learning, real-time data analytics." https://techbeacon.com/enterprise-it/counter-security-threats-machine-learning-real-time-data-analytics.