AMPITO

Spotting Hidden APIs and Outsmarting DDoS Predators

An Adventurer's Guide to Securing Your Digital Safari

VERCARA
a digicert company

Welcome to the Jungle

(of Bits and Bytes)

Safari hats on, binoculars in hand - today's digital landscape can feel every bit as untamed as the savannah.

As technology leaders, you are responsible for venturing into this sprawling ecosystem, spotting elusive APIs, and safeguarding your environment from lurking predators like DDoS attacks. Much like real-world wildlife conservation, the health of your digital habitat depends on vigilant oversight, the right defensive gear, and a strategic plan.

In this whitepaper, we'll explore the hidden corners of your environment where APIs can roam unchecked, examine the potent threat of DDoS "predators," and introduce you to essential solutions, including those from Vercara, that will help you protect your business from harm.

Prepare for a trek through the grasslands and vines across 5 key areas that will equip you with the knowledge needed to thrive in your own digital safari.

Into the Wild:
Understanding the Safari Landscape

The Habitat: Your Expanding Digital Ecosystem

Like savannah grasslands stretching to the horizon, your organisation's digital ecosystem has grown in scale and complexity. APIs connect your applications, partners, and services - facilitating data exchange and enabling new features. While these routes improve customer experiences, they also create hidden pathways for potential threats. Overgrown or unmonitored APIs can quickly morph from helpful herd members to stealthy infiltrators.

Why APIs Are the Elusive Creatures of Cybersecurity

APIs serve as vital arteries, allowing data to flow between internal systems and external services. Yet, many enterprises remain unaware of all the APIs operating in their environment. If they lurk undetected, these "phantom APIs" can become prime targets for threat actors, allowing them to slip through defences unnoticed.

Just as any self-respecting safari guide would caution you to be aware of the creatures behind every bush, technology leaders must keep track of every API roaming across their organisation.

DDoS: The Pack of Predators on the Prowl

Distributed Denial of Service (DDoS) attacks are comparable to a coordinated pack of predators. They strike with overwhelming force, crippling your critical services by flooding networks or applications with malicious traffic.

With the relentless evolution of both network and application-layer attacks, it's not enough to scatter a few deterrents around. True resilience requires a robust, always-on defence that can adapt to new attack vectors.

The Elusive Creatures - Hidden APIs

The Rise of the Unseen

As organisations expand services, partner integrations, and microservices architectures, new APIs often spring up like watering holes in a remote corner of the savannah: unmapped and potentially dangerous. A single unprotected or undocumented API can open the door to data breaches, compliance violations, and reputational harm.

Key Business Impact

Unplanned Exposure:
A hidden API might bypass normal security checks, exposing sensitive data.

Shadow IT:
Development teams may spin up APIs without formal approval, leaving them undocumented.

Compliance Risks:
Regulations such as GDPR, PCI-DSS, or industry -specific mandates can be inadvertently violated by these 'unknown animals.'

Why It Matters Now

The proliferation of cloud services, agile development cycles, and rapid innovation has led to a surge in API usage. Yet, many of these routes remain off the official map. In the same way that missing data points can undermine a conservation study, missing APIs threaten your security posture. A single overlooked endpoint can become a quick path for attackers to infiltrate your ecosystem - often unnoticed until the damage is done.

Circling the Camp:
Fending Off the DDoS Hyenas

Coordinated Chaos

On a safari, a lone hyena might not pose a huge threat. But a pack, working in tandem, can overwhelm even the strongest prey. DDoS attacks operate in much the same way. They flood networks and applications with fake traffic, rendering your services inaccessible to legitimate users.

Business Consequences

Downtime:
Operational paralysis that can erode revenue, brand reputation, and customer loyalty.

Resource Drain:
IT teams scramble to contain the attack rather than focusing on strategic projects.

Escalating Tactics:
Attackers now deploy multi-vector attacks - targeting networks, applications, and APIs simultaneously to maximise disruption.

A Growing Menace

The sophistication of DDoS attacks has escalated, with threat actors shifting their sights to newer targets such as API endpoints. Organisations must prepare for attacks that strike unpredictably, often launching from massive botnets spread globally. In safari terms, it's not enough to set up a lone perimeter fence; advanced predators will find creative ways to breach weak points.

Taming the Threats with Vercara

Introducing Vercara's proven solutions

Vercara specialises in comprehensive API security and DDoS protection, equipping organisations with powerful tools to chart and protect their digital savannah. From pinpointing hidden APIs to fending off massive DDoS stampedes, Vercara's platform offers an integrated, adaptive shield.

API Security: Spot and Safeguard

Discovery & Visibility:
Automatically detect new or unapproved APIs, ensuring nothing remains hidden in the undergrowth.

Granular Control:
Enforce authentication, authorisation, and rate limiting policies based on real-time traffic patterns.

Threat Intelligence:
Leverage global insights to block suspicious calls before they reach critical endpoints.

DDoS Protection: Outsmarting the Predators

Global Scrubbing Centres:
Divert malicious traffic away from your infrastructure, ensuring genuine users can still access services.

Adaptive Mitigation:
Dynamic filtering methods that respond instantly to new attack vectors - even multi-vector assaults.

Scalable Infrastructure:
Handle sudden surges of traffic with ease, preventing disruptions no matter how large the attacking 'pack.'

The Benefits in Action

Consistent, Real-Time Oversight:
Gain a live feed of API usage and incoming threats, minimising blind spots.

Reduced Downtime & Incident Costs:
With advanced DDoS filtering, you keep your services running, preserving revenue and customer trust.

Stronger Compliance Posture:
Automated tracking and policy enforcement help you maintain industry and regulatory standards.

From Exploration to Execution: The Next Steps

Running a secure, thriving digital environment can feel like leading an expedition through unfamiliar territory. Hidden APIs and prowling DDoS attackers add complexity and risk at every turn. Yet, with proper planning, layered strategies, and the right security partner, like Vercara, you can transform these threats into manageable challenges.

Next steps

1. **Evaluate Your API Footprint**
   Conduct a thorough inventory of existing endpoints.
2. **Assess DDoS Readiness**
   Development teams may spin up APIs without formal approval, leaving them undocumented.
3. **Explore Vercara**
   Discover how their integrated platform can protect you from stealthy APIs and relentless attackers.
4. **Establish an Ongoing Strategy**
   Security isn't static; plan for continuous adaptation as threats evolve.

In the end, a secure digital safari isn't just about avoiding attacks - it's about empowering your organisation to innovate freely, confident that you can outmanoeuvre both hidden vulnerabilities and the most tenacious of predators.

By partnering with Ampito and leveraging Vercara's industry-leading solutions, you'll be well-equipped to navigate the savannah and emerge not only unscathed but triumphant.

About Ampito

Ampito specialises in delivering secure, future-ready IT solutions that help businesses tame the complexities of digital transformation. Whether you're eyeing hidden APIs or fending off DDoS attacks, our expert team works closely with industry-leading providers, like Vercara, to design tailored security strategies that keep your operations safe and sound. Partner with us, and let's explore the digital safari together.

info@ampito.com

+44(0)330 056 4070