SPONSORED CONTENT | WHITE PAPER

White paper

Don't Hit the Gas Without API Security Guardrails

IT leaders examine API security in retail, hospitality and travel

Retail, hospitality, and travel enterprises are rapidly adopting AI to power workflows that connect their companies with customers. The challenge is that the application programming interfaces (APIs) which connect systems have become a primary security attack vector. As a result, the need to protect assets and data about customer interactions has never been greater.

CIO

SPONSORED BY Akamai

White paper

Recent research from Akamai highlights these risks and offers key suggestions for mitigation. To fight and mitigate attacks, organizations need better coordination with business units. They should build full API inventories, limit public-facing APIs, and establish AI-specific protocols.

Exploring that research – and ways of reducing risk – was the focus of a recent *CIO* Foundry virtual roundtable, sponsored by Akamai. Nearly a dozen IT executives across security, infrastructure, compliance, and engineering functions participated.

> **Bad actors are swarming and building communities** to amplify malicious attacks and known vulnerabilities across domains.

Brent Maynard, Akamai's Senior Director of Security Technology and Strategy and a participant in the event, pointed to a 33% rise in global web attacks as new AI threats and vulnerabilities are emerging. Attackers increasingly use generative AI techniques to gain access to enterprise systems and data, he said.

A global apparel manufacturer and retailer noted that "bad actors are swarming and building communities to amplify malicious attacks and known vulnerabilities across domains."

APIs are the new attack surface

A growing number of AI-powered systems are accessed with unsecured APIs that are externally accessible and may use inadequate authentication. AI is fueling the technical advancement of threat actors through AI-driven malware, vulnerability scanning, attacks on AI-integrated systems, and sophisticated web scraping.

Akamai's Maynard issued a stark warning during the roundtable: "APIs are the new attack surface," he said.

Roundtable participants explored areas of vulnerability in their various enterprises. The two most mentioned: overall customer data / interactions and the challenge of insufficient API cataloguing. Too often organizations lack up-to-the-minute API inventories.

"We think we had a pretty good list," said one automotive technology IT director. "But we're finding interfaces that we didn't know about."

Maynard find this problem a lot throughout the retail and hospitality sector, as well as within other sectors. "It starts with discovery," he said at the event.

A hotel chain VP of IT stressed the critical importance of safeguarding the entire customer journey. In hospitality, companies increasingly use APIs to integrate workflows to generate a seamless customer experience. They link reservation data, historical guest information, the on-site guest experience, and payment information.

> The bad actors are using tools. **We are constantly playing catch-up.**

This executive was aware of API vulnerabilities. "The bad actors are using tools," he said. "We are constantly playing catch-up." As hotels and retailers increasingly rely on IoT devices, the 'blast radius' of attacks expands as these kinds of tools integrate with core workflows.

A retail IT director raised concerns that agentic AI agents calling internal APIs, create new intrusion risks. "That opens a can of worms on how intrusions can happen," he said.

Akamai's Maynard agreed: "With agentic AI calling internal APIs on behalf of users, it's critical [that] we rethink API contracts."

Best practices in API security

During the roundtable, participants not only explored the kinds of threats that are growing but also threat mitigation best practices. The group agreed: you should treat API agents as if they are untrusted apps. That means enforcing strict schema validation, using intent-based mediation, and tying every API call back to its user context.

Without these controls, enterprises may over-permission access, creating blind spots when it comes to accountability. "API contracts need to define

both what can be called and why," said Maynard.

During the roundtable, the VP of infrastructure at a major apparel firm talked about the need to involve a company's third-party technology providers. Vendors see all data including that from competitors; the enterprise sees only its own data.

So who is responsible as companies establish guardrails in application development: the enterprise or its technology providers? Are there lessons the vendor community can share without compromising individual company intellectual property? The application development process itself may help here. Enterprises can use their dev teams to do API audits.

Automation and speed

Speed is paramount. This is an area where automation helps. Said Maynard: "You need to look at things that give you fast control. You need to make sure you have real-time protection."

Added the global head of software at an international building technology device company: "We cannot wait until the damage is done. We need pattern detection that includes real-time monitoring."

The director of global enterprise architecture at a major beverage company posed the question that seemed to be on all participants' minds: "How do you ensure brand safety amid deepfake risks?" AI-enabled systems need specific instructions, and companies need to better manage API access.

"We define the topics, the tone, and the source material," said Maynard. "It's putting up guardrails before you ever hit the gas." ■

NEXT STEP: Strengthen your API defenses before attackers strike. Explore the *State of the Internet: Apps and API Security 2025* report to see where risks are rising and how to stay ahead.

Download the Report