NETFOUNDRY

SOLUTION BRIEF

PROTECT AGAINST OWASP'S TOP 10 API THREATS

The explosion of global API usage has led to a corresponding increase in API vulnerability and actual attacks.

WHY IS THIS IMPORTANT?

From banks, retail, healthcare, and transportation to IoT, autonomous vehicles and smart cities, APIs are a critical part of modern mobile, SaaS and web applications, and can be found in customer-facing, partner-facing, and internal applications. By nature, APIs expose application logic and sensitive data such as PII and because of this have increasingly become a target for attackers. This brief focuses on understanding and mitigating the unique security risks of APIs to ensure rapid innovation is possible.

OWASP API THREATS TOP 10

API 01: Broken object level authorization
API 02: Broken user authentication
API 03: Excessive data exposure
API 04: Lack of resources and rate limiting
API 05: Broken function level authorization
API 06: Mass assignment
API 07: Security misconfiguration
API 08: Injection
API 09: Improper assets management
API 10: Insufficient logging and monitoring

SEPARATING API SECURITY FACT FROM FICTION

API attacks are growing by 681% and costing businesses up to $75B annually. The severity of these vulnerabilities is only increased by prevailing myths around API security perpetuated by traditional "box and wire" solutions. The biggest misunderstanding is the idea that the broadness of threats outlined by OWASP requires a wide range of solutions to mitigate against them, more specifically a full-stack effort, encompassing many of the components involved in the API request/response path. ***This is simply not true***.

THE CLOUDZITI DIFFERENCE

CloudZiti is the only private Zero Trust API Cloud. The software only, cloud-native solution protects against the top OWASP API vulnerabilities without incurring the expense and complexity of managing obsolete network hardware. It is designed to build security and networking into the heart of the development and delivery pipeline by closing all of your inbound firewall ports and making your API gateways, servers, and endpoints unreachable from the networks.

STRENGTHEN & SIMPLIFY SECURITY

Private API clouds take API endpoints off the Internet, while allowing API clients to continue to use Internet access

IMPROVE BUSINESS AGILITY

Reduce business costs and vendor lock-in through agnostic design patterns, simplicity, and automation

MITIGATE SOLUTION SPRAWL

Eliminate complex and expensive "bolted-on" infrastructure and processes for bespoke solutions and use cases

HOW CLOUDZITI ADDRESSES OWASP'S TOP 10 API THREATS

At the core of the Top 10 OWASP API threats, and also the greatest API vulnerability, is the public-facing edge - API servers or API gateways. CloudZiti enables organizations to take API edges off the Internet and available only to authorized endpoints without VPN clients or whitelisted static IP addresses. The following chart offers a comparison between the effectiveness of flawed, traditional solutions (network firewalls, WAFs, and API gateways) and CloudZiti.

✓ = competitive advantage

	NETWORK FIREWALL, WAF, API GATEWAY	CLOUDZITI ZERO TRUST API CLOUD
01: Broken object level authorization **02: Broken user authentication**	Network firewalls only prevent attacks from known attackers, and only after their IPs are added to access control lists. WAFs only work if the authorization problem is previously known and widespread enough to be added to the WAF (usually not the case and only after initial damage). API gateways do not detect most authorization issues.	CloudZiti proactively shields the endpoint which is exposing the attacked object, so the vulnerability can not be exploited from the networks. It adds independent authentication and authorization, so the attacker needs to simultaneously break the API authorization, CloudZiti's API authorization, and gain access. ✓
03: Excessive data exposure	When the API developer needs to expose too many object properties or rely on the API client to do all the filtering, then none of these solutions are very valuable for authorized users.	CloudZiti uniquely ensures that only authorized API clients can connect, limiting the attack surface. If an authorized API client exploits this vulnerability, then it 'quarantines' and sometimes disarms the threat entirely - it can not attack laterally, 'phone home', etc. ✓
04: Lack of resources and rate limiting	This can be addressed by all the solutions. CloudZiti ***simplifies this problem*** by limiting the attack surface - eliminating all the requests from unauthorized API clients which add noise for API operators relying on other outdated solutions. ✓	
05: Broken function authorization **06: Mass assignment**	The other API security solutions do not help at all for this vulnerability. If the API developer needs to implement complex access control policies, or use mass assignment to bind client data and data models without granular filtering, then it is mainly up to the developer to prevent authorized users from finding holes or modifying object properties.	CloudZiti helps by minimizing the attack surface and noise - ensuring that unauthorized attackers can not take advantage of function level authorization issues or mass alignment issues to modify object properties. ✓
07: Security Misconfiguration	Network firewalls are irrelevant in dealing with these misconfigurations. Some WAFs or API gateways may be able to detect commonly misconfigured HTTP headers, unnecessary HTTP methods, or permissive cross-origin resource sharing (CORS).	CloudZiti proactively shields the misconfigured endpoint so the vulnerability can not be exploited from the networks, and the developer has time to fix it. It minimizes the blast radius. If a misconfiguration is exploited by an authorized API client, and it results in malware which then needs to use the network to do damage, CloudZiti effectively quarantines it. ✓

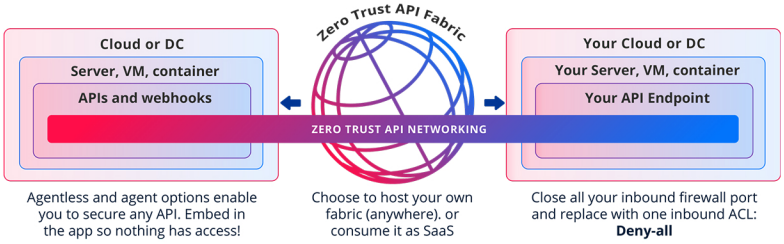
CONTINUED ON NEXT PAGE

= competitive advantage

	NETWORK FIREWALL, WAF, API GATEWAY	CLOUDZITI ZERO TRUST API CLOUD
08: Injection	Network firewalls are irrelevant in dealing with injection threats. Some WAFs or API gateways may be able to detect some common injection flaws, such as SQL, NoSQL, and Command Injection .	CloudZiti proactively shields the API endpoint or gateway, such that the injection flaw can not be exploited from the networks, and the developer has time to fix it. It minimizes the blast radius. If an injection flaw is exploited by an authorized API client, and it results in malware which then needs to 'phone home' in order to do damage, CloudZiti effectively quarantines it.
09: Improper assets management	Network firewalls, WAFs, and API gateways are largely irrelevant in the context of assets management attack vectors. These debug endpoints often look the same as the production API infrastructure.	CloudZiti proactively shields all endpoints from network-based risks, therefore protecting against these threats and mitigating issues such as deprecated API versions and exposed debug endpoints.
10: Insufficient logging and monitoring	Network firewalls, WAFs, and API gateways are largely unhelpful for the management threat because they are mainly outside of the interaction between API infrastructure and management systems. Furthermore, those systems can amplify the problem because they do not block unauthorized users from trying to access the API at L3/L4. The resultant noise created is one reason why API breaches often take over 200 days to identify, and often are found by third parties rather than internal teams.	CloudZiti helps in multiple ways, including API producers extending their zero trust network to include monitoring, management, and logging systems. This means attackers can not "move laterally' between these systems, preventing both infection and spread. Because it blocks unauthorized users before they reach the firewall, WAF, API gateway or API server, the amount of logs to analyze can be decreased by 8x to over 2200x.

ZERO TRUST API CLOUD ARCHITECTURE

CloudZiti fits in with existing WAN and API gateway architectures without needing separate VPN clients or firewall entries for each API client. It replaces the complex firewall ACLs with one inbound rule: deny-all, while API consumers still use the Internet without VPN clients or whitelisted static IP addresses. No infrastructure deployment is required.



ABOUT NETFOUNDRY

NetFoundry delivers the CloudZiti private API cloud – the world's first programmable, cloud native, zero trust network with near unlimited scale, concurrency, and performance. CloudZiti allows users to embed private, zero trust overlays as code, so even the most security-conscious API clients can connect to APIs without VPNs or private network connections. NetFoundry transforms secure networking into a developer platform and provides the flexibility of SaaS and open source options. The cloud-native, API-first approach enables customers to leverage existing solutions and tooling, in both options.