TRACEABLE

SOLUTIONS BRIEF

Zero Trust API Access (ZTAA)

Traceable's Zero Trust API Access actively reduces your attack surface by minimizing or eliminating implied and persistent trust for APIs.

Why the Next Evolution of Zero Trust MUST include API Security

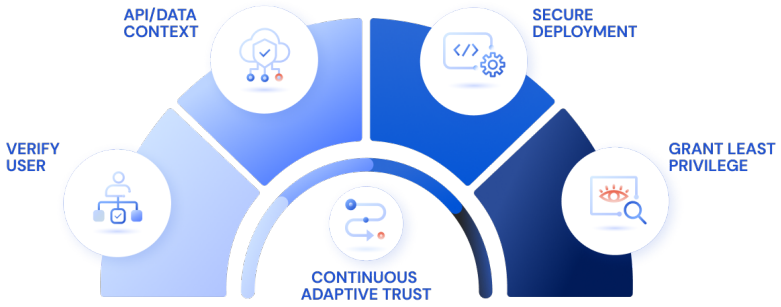
Zero Trust Security is often associated with network and identity access management. However, while those solutions are important and necessary, the evolution in infrastructure and the onset of new attack surfaces require us to expand our perspective and include the API layer in Zero Trust strategies.

1. Most current API security solutions are only looking at the edge -- you can't achieve full context or Zero Trust level protection from there.

2. Today's cloud-based, API-driven, microservices-based applications, all extensively operate using APIs to communicate between users and NPEs (non-person entities) to apps, and between apps and app components.

3. Expanding Zero Trust concepts to the API layer helps ensure Zero Trust coverage of applications at the communications layer of the application stack.

Given these realities, it's now time to expand Zero Trust to include the API layer for complete protection.



SOLUTION HIGHLIGHTS

Dynamic Data Access policies stop data breaches in their tracks: Quickly and easily create policies with out-of-the-box templates or customize policies based on organization needs.

Continuous Adaptive Trust for real-time threat prevention: The right access for the right users and entities, at the right time, thereby protecting the business and its sensitive customer data.

Intelligent Rate Limiting for API abuse prevention: Provides enhanced protection against API DDoS attacks, reduces load on backend APIs, honors SLAs, and reduces costs often associated with 3rd party APIs.

API Security solutions are essential to aligning Zero Trust thinking with the realities of today's application architectures and extending the Zero Trust security model to the full application stack.

The enduring success of Zero Trust is due to its flexibility, focus, and ability to deliver results. Zero Trust architectures use multiple security layers and technologies, such as network and identity access management and user, application, and workload security, to protect enterprise assets. These models "trust no one," assuming adversaries are already present or able to access different parts of the application and infrastructure stack. As a result, systems continuously verify users, devices, and access attempts.

The model works because it provides a simple and repeatable methodology that teams can use to continuously enhance security. IT teams discover and prioritize assets, map and verify transactions, develop Zero Trust standards and designs, implement new systems, and report on and maintain them, over and over.

Using this approach, Zero Trust architectures enforce security policies across networks, clouds, and endpoints, simplifying management processes and standardizing access and security across use cases.

By doing so, Zero Trust technologies segment networks to prevent attackers' lateral movement and protect business-critical data, applications, and infrastructure from unauthorized access and usage.

However, to date, APIs have been largely neglected by Zero Trust models. In addition, digital transformation demands and DevSecOps processes at organizations have created new gaps and vulnerabilities attackers can exploit.

Many security solutions such as Web Application Firewalls (WAFs) only scan the edge. However, organizations are increasingly pushing technology and services past the perimeter. IT teams are using or developing cloud and microservices-based applications and leveraging APIs to connect to partners, customers, and other third parties.

APIs connect applications and their various components and also communicate between users, non-person entities (NPEs), and other applications. It's not an overstatement to say that APIs are everywhere, connecting almost everything.

Expanding Zero Trust security concepts to the API interface and implementation layers ensures that communication services get the same protection afforded to other resources.

ZERO TRUST API ACCESS:
API SECURITY BEYOND LAYER 7

Traceable's Zero Trust API Access (ZTAA) actively reduces your attack surface by minimizing or eliminating implied and persistent trust for your APIs.

As the industry's first and only solution in the market, ZTAA enables seamless and secure API access with dynamic data access policies, continuous adaptive trust, and intelligent rate limiting - all without sacrificing user experience.

Dynamic Data Access

With Traceable, you can detect and classify the data that APIs are handling, to apply proper access control policies. These policies define which users and roles can access different data types, at what times, from what geolocations and from what client types. This includes sources like bots, residential proxies, and anonymous VPNs. With dynamic data access policies, you can quickly and easily create policies with out-of-the-box templates or customize policies based on organization needs.

Intelligent Rate Limiting

API rate limiting enables organizations to control the incoming traffic to an API by automatically limiting the number of requests that the API can receive within a given period of time. After the limit is reached, the policy rejects all requests from that source, thereby avoiding any additional load on the backend API.

Intelligent rate limiting factors in the rates for users, proxies, bots, and the business function of APIs. This provides enhanced protection against API DDoS attacks, reduces load on backend APIs, honors SLAs, and reduces costs often associated with 3rd party APIs. Access to APIs and sensitive data is therefore proactive and automatic, preventing API abuse.

Continuous Adaptive Trust

Traceable's ZTAA provides security that continuously adjusts to the organization's threat landscape. This is achieved through real-time, context-based authentication and authorization for API access (both users and machines).

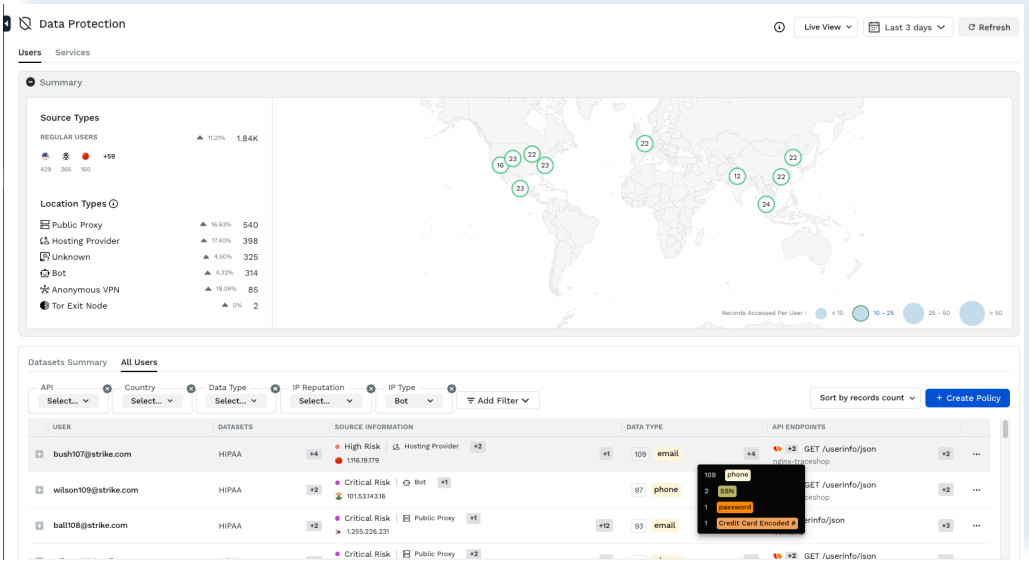
Traceable can stitch APIs, as well as the data and user context via flexible data collection options. This ensures that adaptive trust is enforced for APIs at the edge, as well as for all internal services, and 3rd party APIs.

The result is the right access for the right users and entities, at the right time, thereby protecting the business and its sensitive customer data.

Security Enables Innovation

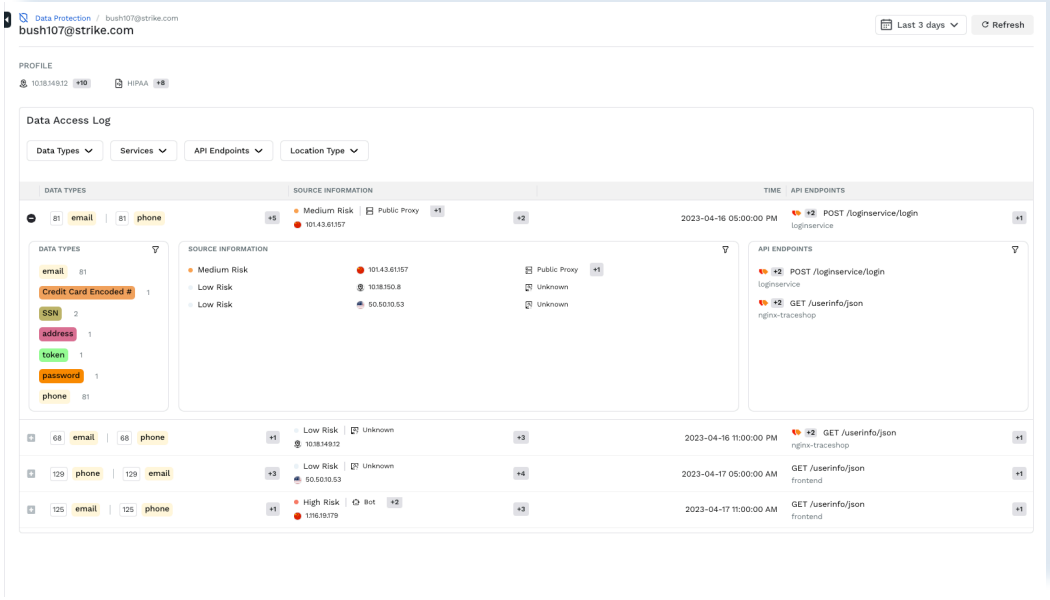
When combined, Zero Trust Security and API Security create a holistic and robust security approach that actively mitigates the risks associated with accessing sensitive data via APIs. This comprehensive approach helps protect sensitive information and fosters a secure environment for innovation and growth. Organizations can now confidently offer new products and services, turning security from a hindrance, to a catalyst for accelerated growth.

Data Protection and Data Access Logs

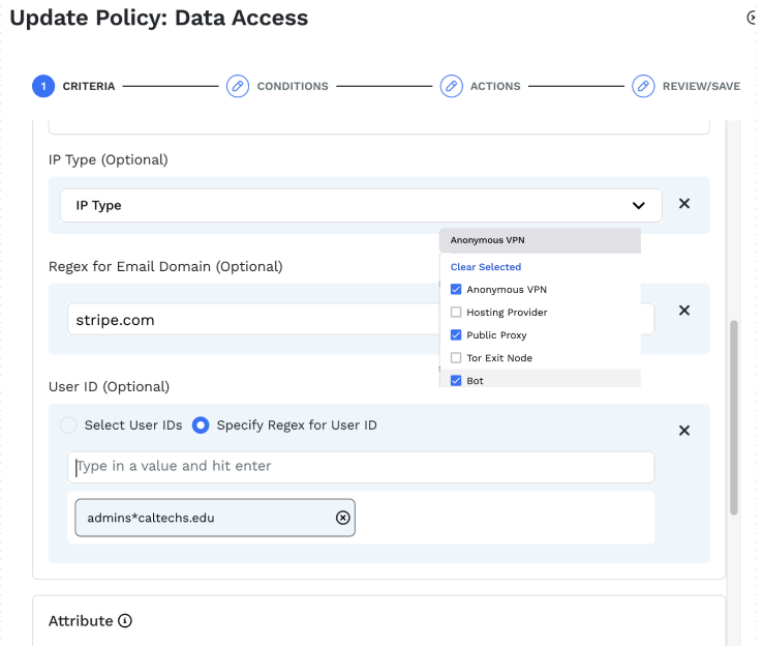


The Data Protection and Data Access views, give a single pane of glass of user access to APIs. The notion of who is the user accessing the API, is being brought in from the user attribution and the authentication flow. Once that happens, you can see in these views, the users from different domains. This is where you can see the patterns of access from different users, different domains, or different IP or location types, as well as the volumes of data being accessed.

This ultimately helps teams to understand which Zero Trust policies are potentially needed.

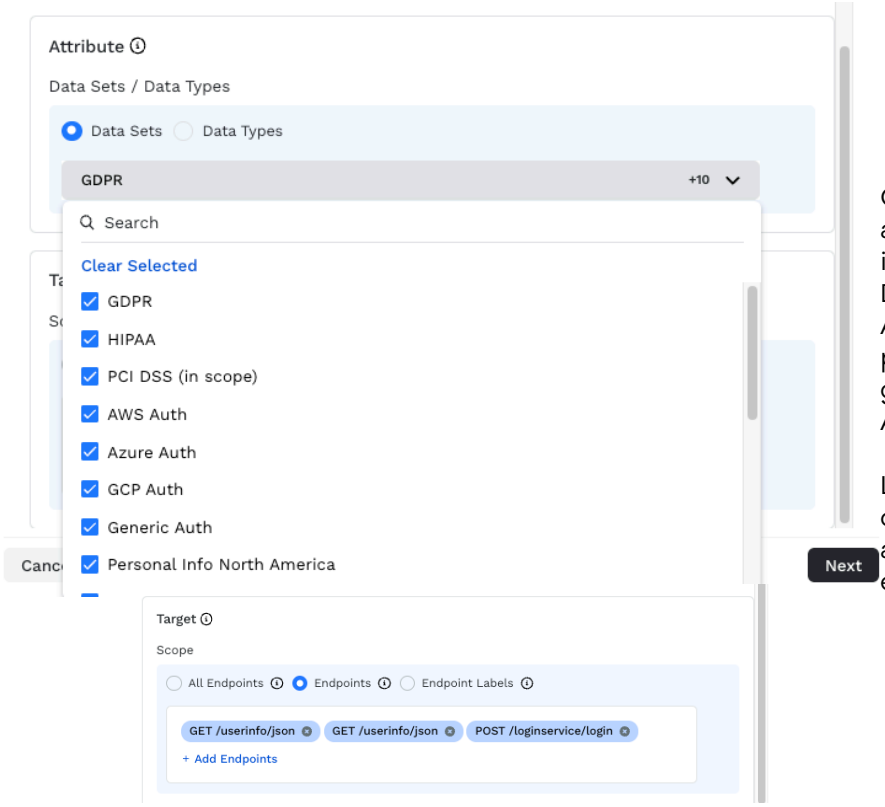


Data Access Policies



After looking at the data access patterns, you can begin implementing Zero Trust policies.

This includes granular user ID-based policy enforcement, with the ability to choose the access levels of specific domains and individual email addresses.



Choose numerous data sets to apply to data access policies, including GDPR, HIPAA and PCI DSS compliance, as well as AWS Auth, Azure Auth, GCP Auth, and personal information for different geolocations, such as North America and the European Union.

Limit or expand the scope by choosing specific endpoints, or applying to all endpoints in your environment.

Traceable is the industry's leading API security company that helps organizations achieve API protection in a cloud-first, API-driven world. With an API data lake at the core of the platform, Traceable is the only intelligent and context-aware solution that powers complete API security - security posture management, threat protection and threat management - across the entire software development lifecycle - enabling organizations to minimize risk and maximize the value that APIs bring to their customers.