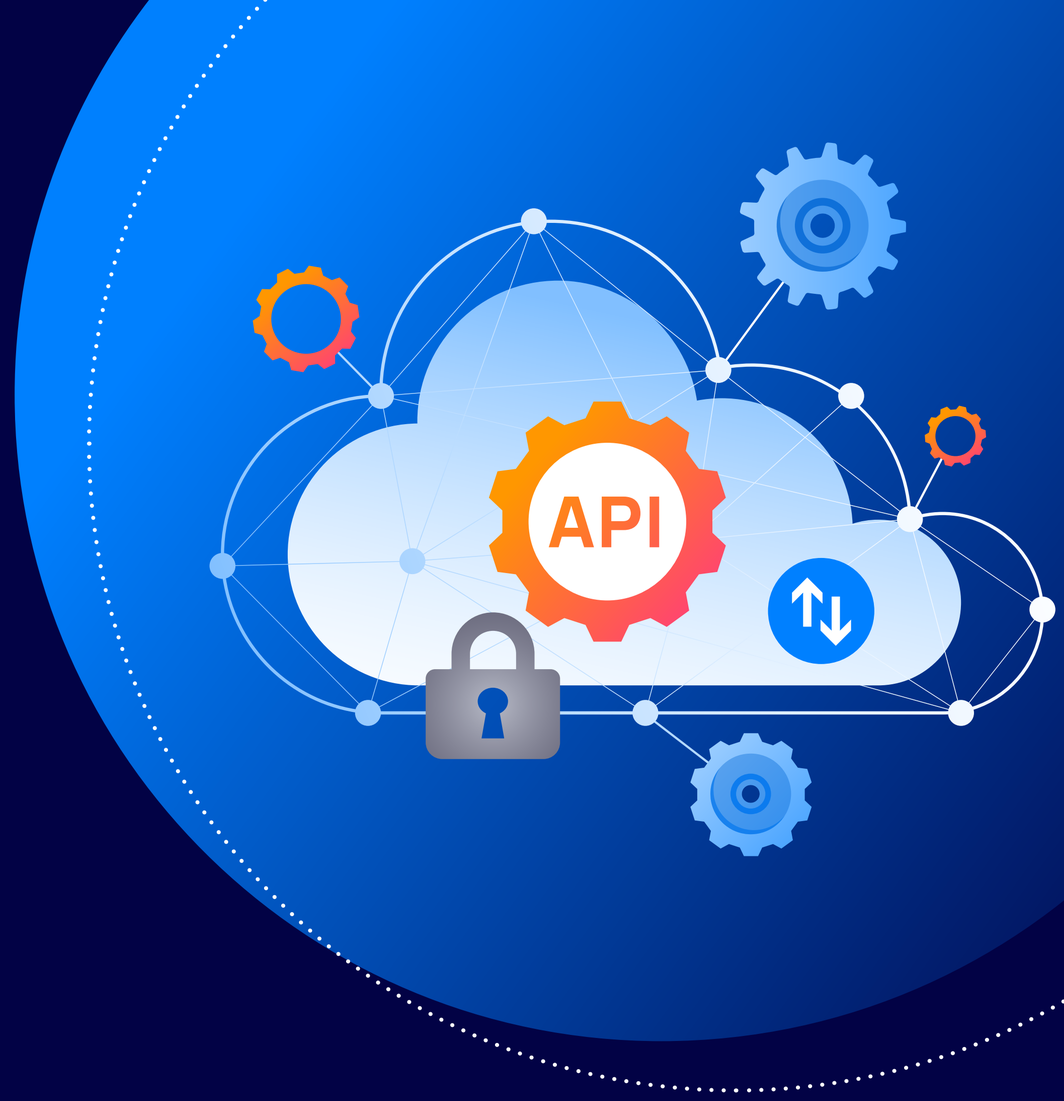
orca security



API Security Q&A

featuring Forrester's Sandy Carielli

FORRESTER®

We sat down with Sandy Carielli, Principal Analyst at Forrester, for a webinar as a guest speaker discussing API security. We then kept Sandy for a Q&A deep dive into the top API attack vectors, the cloud security landscape, and more.

INTERVIEW WITH

Sandy Carielli

Sandy is a Principal Analyst at Forrester advising security and risk professionals on application and product security, with a particular emphasis on the collaboration among security and risk, product management, application development, operations, and business teams. Her research covers topics such as proactive security design, protecting modern and emerging application architectures, protection of applications in production environments, and embedding security throughout the product lifecycle.

What are some of the reasons that you see API security as being such a critical need for organizations?

APIs offer new opportunities for customer engagement and can lead to new business models with additional revenue streams. We are seeing tremendous growth in API adoption — according to Forrester's 2022 Business Technographics Developer Survey, 31% of developers say that their firms have public APIs, and 35% say that their firms have B2B APIs. However, security leaders' existing approaches to protecting customer facing applications don't adequately cover APIs. We have seen a number of high profile breaches due to insufficiently protected APIs. As firms realize that their existing application protections don't cut it, they are actively looking for API security solutions.

What are some of the top attack vectors and threats you are hearing from clients when it comes to API security?

Clients are concerned about many of the attack vectors detailed in the OWASP API Security Top 10. Not surprisingly, authentication and authorization are key areas of concern, as they have been the cause of a number of high profile API related breaches. Lack of proper authorization let Peloton users pull any other user's account data, for example. More recently, the Optus breach was due to an unauthenticated API. Of course, it's difficult to apply proper authentication and authorization to APIs if you don't know they are there — many firms express concern about shadow APIs and struggle to get a handle on their API inventory.

What are some of the first needs that organizations should address as they start to secure their APIs? And what would be some more advanced steps they could take?

When I speak with clients about API security, we almost always start with discovery and inventory. Many organizations have thousands or tens of thousands of APIs. Some even have more than that. Unfortunately, those numbers often include rogue and unmanaged APIs — those APIs are not properly secured. So an early step is improving API inventory so you know what to protect. In the early days, firms may also use API specifications to generate rules for allowing or rejecting API traffic, but this is dependent on having up to date specifications. As firms become more mature, they should work at protecting both north-south and east-west API traffic and have a process for tracking and analyzing different API versions.

OWASP API Security Top 10

1. Broken Object Level Authorization (BOLA)
2. Broken User Authentication
3. Excessive Data Exposure
4. Lack of Resources & Rate Limiting
5. Broken Function Level Authorization (BFLA)
6. Mass Assignment
7. Security Misconfiguration
8. Injection
9. Improper Assets Management
10. Insufficient Logging & Monitoring

Where does API security fit within the wider cloud security landscape, particularly as it relates to cloud native applications?

API security is certainly not limited to cloud based applications, but many firms that build applications API first also deploy in the cloud. A given cloud workload may consist of one or more API endpoints — these could be public APIs, B2B APIs, or even internal APIs. In order to protect communications among cloud workloads, you must manage and secure the API traffic to and from those workloads.

When it comes to APIs, how can development and security teams work together to maintain efficiency while adhering to security and compliance requirements?

Security and development must align on the types of data shared via various APIs and ensure that the appropriate authentication and authorization controls are in place to prevent PII or other sensitive data from getting into the wrong hands. It's also important to keep API specifications up to date so that security can use them to analyze API traffic for anomalies. While developers may have API management tooling to generate specifications, it's easy for them to become outdated — security teams can help by analyzing API traffic, identifying disparities between API traffic and existing specifications, and generating updated specifications.

Learn more about API security & Orca's capabilities

Watch the on-demand webinar featuring guest speaker Sandy Carielli, Principal Analyst at Forrester. We dive into the top API security challenges and threats, strategies, and Orca's API security capabilities.

Watch Webinar

About Orca Security

Orca Security is the pioneer of agentless cloud security that is trusted by hundreds of enterprises globally. Orca makes cloud security possible for enterprises moving to and scaling in the cloud with its patented SideScanning™ technology and Unified Data Model. The Orca Cloud Security Platform delivers the world's most comprehensive coverage and visibility of all risks across the cloud. With continuous first-to-market innovations and expertise, the Orca Platform ensures security teams quickly identify and remediate risks to keep their businesses secure.

Connect your first account in minutes:
https://orca.security or take the free cloud risk assessment.