

TELECOM ATTACK DISCOVERY SERVICES

Identify and defend against sophisticated cyberattacks

ATTACKS ARE EVOLVING

Where basic filtering and assessment services were once sufficient, technical progress in hacking techniques means operators need to distinguish and protect against much more sophisticated cyberattacks and bypass methods.

The iBASIS Security iQ360™ portfolio offers cloud-based threat detection and protection to ensure faster incident identification, investigation, response, and defense whether the attack targets the core operator network or the subscriber.

iBASIS's Telecom Attack Discovery (TAD) services provide a comprehensive 360 degree suite of security analytics and protection.

The multi-module security solution is hosted on the iBASIS network and fully managed by iBASIS security experts.

TAD combines the power of best-in-class signaling intrusion detection with a business intelligence (BI) module, which turns security monitoring and signaling traffic analysis into a clear and easy process. This can be coupled with the Traffic Screening Module Firewall to allow fast and effective protection.

TAD and Firewalls can work independently of each other: if an existing firewall is already installed on the mobile operator infrastructure, the iBASIS TAD can provide hassle-free firewall rules updates via APIs.



KEY BENEFITS

Full protection for Diameter, SS7, and GTP vulnerabilities with Next Generation Firewalls

Access to unmatched security threat database

Quick deployment and rules customization at initial setup

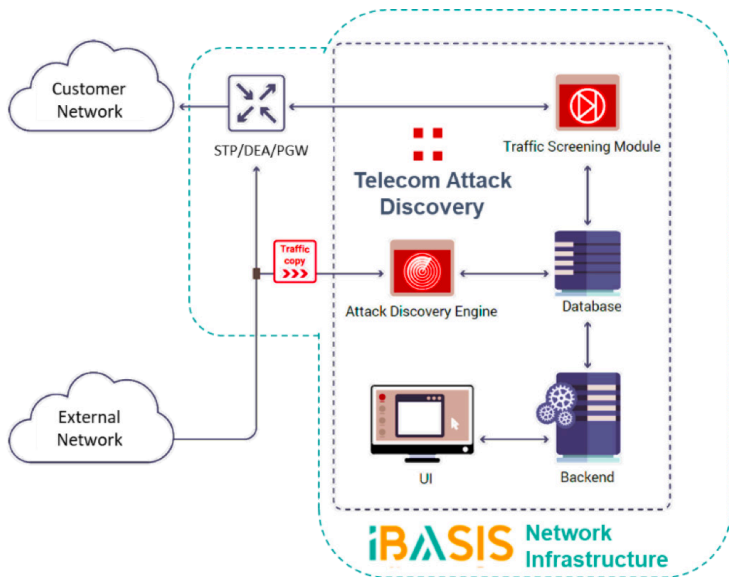
Automatic Rules updates through APIs possible

Powerful and flexible rules management interface

Maximized revenues and minimized losses from security attacks

BE THERE FIRST

Looking for a customized solution?
Talk to one of our specialists
at info@iBASIS.net.



Please note: if your traffic is not exclusively carried by iBASIS, the solutions can still be delivered. iBASIS experts will get involved and consult with you to make the right design choices. Please feel free to ask your account manager.

iBASIS TAD KEY BENEFITS

- Real-time security monitoring and filtering
- Comprehensive identification of all types of threats
- Continuous updates to stay ahead of hackers
- Access to telecom & signaling security experts

iBASIS TAD provides real-time security monitoring and filtering to introduce signaling network perimeter protection as a service. The TAD's rich analytics, reporting, and alerting capabilities allow immediate actions to be taken as threats occur.

TAD is continuously updated by market-leading research that is often used subsequently to define industry security recommendations, so the technology stays ahead of the market and ahead of hackers.

TAD gives iBASIS customers access to exceptional industry security intelligence, world class signaling intrusion detection, and the ability to protect their networks. Protection is offered via either hosted firewall capabilities or insights to implement customized filtering on existing devices such as Signaling Transfer Points, Diameter Edge Agents, and Signaling Firewalls. This can even be automated via APIs if required.

In monitoring mode, TAD is purely passive and does not introduce any latency. In firewall mode, all traffic activity is controllable by the individual operator and, coupled with the monitoring visibility, and with a simple GUI, all filtering can be easily assessed in detail before and after application.

At service delivery, TAD will be tailored to the operator network for maximum accuracy and minimal false positives to ensure a premium service.

As telecom security is still a niche skill set, the service provides comprehensive support with access to genuine industry experts for information and advice.

TAD's knowledge base includes the identification of all forms of malicious activity, including:

- Critical sensitive data leakage
- Subscriber's location tracking
- Voice calls and SMS interception
- Fraud
- DoS to a subscriber
- Disruption to the mobile network or mobile network elements

REAL-TIME MONITORING FOR EARLY THREAT DETECTION

TAD's security intelligence knowledge base is continually updated to recognize ever developing attack patterns. The security research driving the knowledge base is the same being used by industry bodies to develop their recommendations.

When attack scenarios with a specific problem are shared with GSMA or with a vendor, the TAD is also updated. This allows operators to detect malicious threats at the earliest possible stage, enabling reaction before breaches occur.

ADVANCED ANALYTICS FOR RAPID INCIDENT RESPONSE

TAD provides rich analytics and reporting capabilities to facilitate fast and effective response.

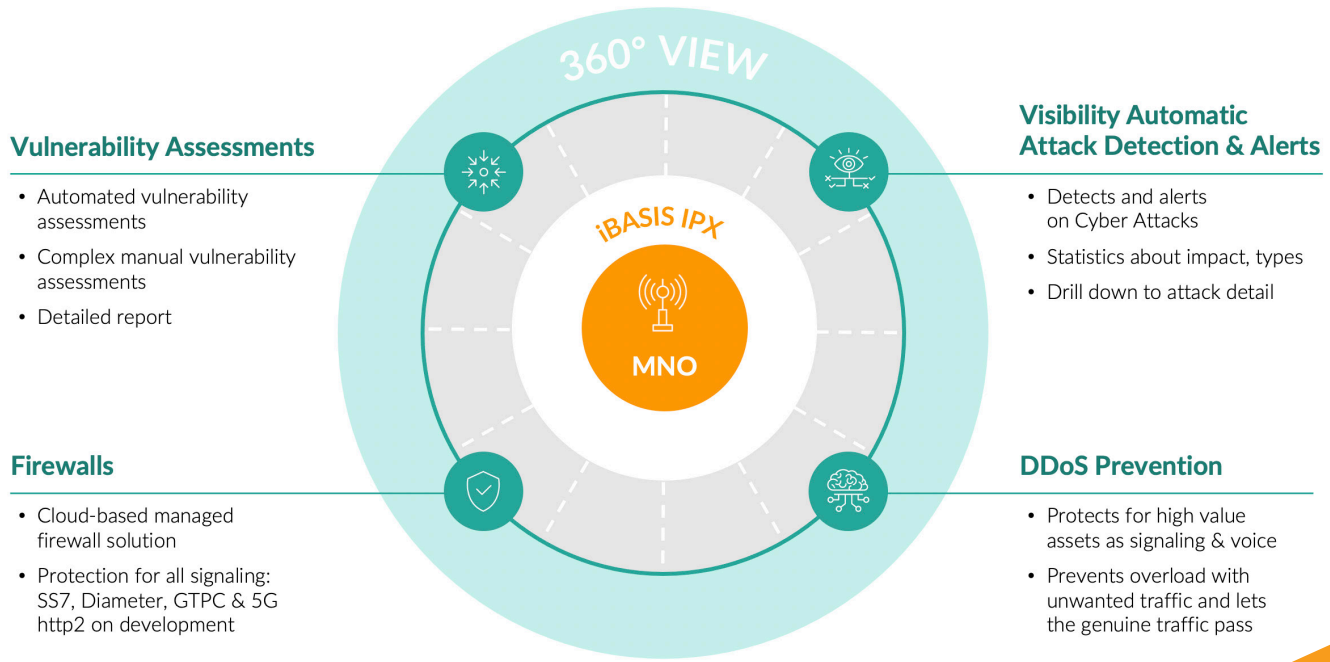
The user interface displays aggregated data on comprehensive and easy to understand dashboards, with the ability to generate actionable attack-related reports and alerts.

The instinctive and comprehensive system supports operator staff to mitigate attacks and perform real-time, or retrospective, incident investigation.

INTUITIVE NAVIGATION AND ADVANCED FORENSIC CAPABILITIES

To ensure the richest benefit from security visibility, users may wish to have access to enhanced filtering mechanisms for fast and intuitive navigation. TAD provides filtering, grouping, and sorting capabilities by multiple criteria for instant attack impact. The user can also customize views by adding or removing attributes to display the exact information their role requires.

360 INTELLIGENCE TO DETECT, PREVENT, AND DEFEND AGAINST SECURITY ATTACKS



Vulnerability Assessments

- Automated vulnerability assessments
- Complex manual vulnerability assessments
- Detailed report

Visibility Automatic Attack Detection & Alerts

- Detects and alerts on Cyber Attacks
- Statistics about impact, types
- Drill down to attack detail

Firewalls

- Cloud-based managed firewall solution
- Protection for all signaling: SS7, Diameter, GTPC & 5G http2 on development

DDoS Prevention

- Protects for high value assets as signaling & voice
- Prevents overload with unwanted traffic and lets the genuine traffic pass

The iBASIS Security iQ360™ portfolio is a hosted and fully managed 24/7 solution for attack detection, signaling firewall, and DDoS rule management.

The cloud-based platform sits on the iBASIS network, which eliminates the need for multiple upfront mobile operator network investment and intensive project deployment.

The solution relies on in-depth visibility, monitoring, and attack detection complemented by automatic rule updates against continuously evolving threats and access to one of the largest telecom threat databases.

For signaling firewalls already installed on customer's premises, automatic rule updates via APIs enable superior monetization of existing investments.

The iBASIS security portfolio leverages best-in-class partnerships in cyber security and DDoS protection and ensures optimized efficiency to customers' security teams through one single point of contact.

Combined with its unique anti-fraud platform, iBASIS delivers a holistic approach to security, based on 360-degree solution intelligence to fully protect the global operator's network.

ABOUT iBASIS

iBASIS is the leading communications solutions provider enabling operators and digital players worldwide to perform and transform. Powered by Tofane Global, iBASIS is the first independent communications specialist, ranking third largest global wholesale voice operator and Top 3 LTE IPX vendor with 700+ LTE destinations. iBASIS today serves 1,000+ customers across 18 offices worldwide.

CORPORATE HEADQUARTERS

10 Maguire Road, Building 3
Lexington, MA 02421

T +1 781 430 7500

F +1 781 430 7300

E info@iBASIS.net

For more information, please visit
iBASIS.COM