

**ORYXLABS**



**DNS FIREWALL**

**SIMPLIFY  
DNS BASED  
SECURITY**

PRODUCT BROCHURE



# THE THREAT LANDSCAPE

The Internet delivers enormous value to organizations by connecting our computers, phones, and other devices allowing us to work, collaborate and innovate. However, when a user or device connects to a malicious website, the results can be catastrophic: intellectual property theft, compromised customer data, and business disruptions.

Following the pandemic-driven adoption of hybrid work, the attack surface has expanded, and the frequency and impact of attacks is growing at an alarming rate.

Heavy reliance on cloud for both personal and business purposes has further increased the importance of web security.

Let's consider some common DNS based attacks:

- » Use of DNS for complex multi-stage attacks using different techniques such as Domain Generated Algorithms (DGA)
- » DNS tunnelling
- » DNS typo squatting
- » DNS amplification
- » DNS rebinding attacks
- » DNS spoofing
- » Other ever-evolving attacks that operate at the DNS layer

Nearly 90% of malicious incidents make use of the Domain Name System (DNS) – the global address system for websites.

What's to be done? By improving the security of DNS operations, the vast majority of cyber attacks can be prevented even before a user or device visit a malicious domain.

## 50+

Content categories

## 99%+

Active web coverage

## 15ms

Low latency

## 100%

Uptime

Scan this QR code to  
learn more about our  
products



**DNS FIREWALL**  
BEST DNS BASED  
PROTECTION



# OUR SOLUTION

DNS FIREWALL takes a state-of-the-art approach to help your organization defend against DNS-based attacks.

Cost-effective and easy to operate, our solution monitors all outgoing DNS traffic from an organization's on-premise and remotely operated computers, tablets, smart sensors and equipment – ensuring those endpoint devices do not access dangerous website.

Implemented from a single software platform with no new hardware requirements, DNS FIREWALL uses machine learning, artificial intelligence and advanced algorithms to assess, in near-real time, the destination of all outbound DNS traffic.

If a device attempts to access a website we've identified as malicious or any other website displaying suspicious characteristics, the access is blocked.

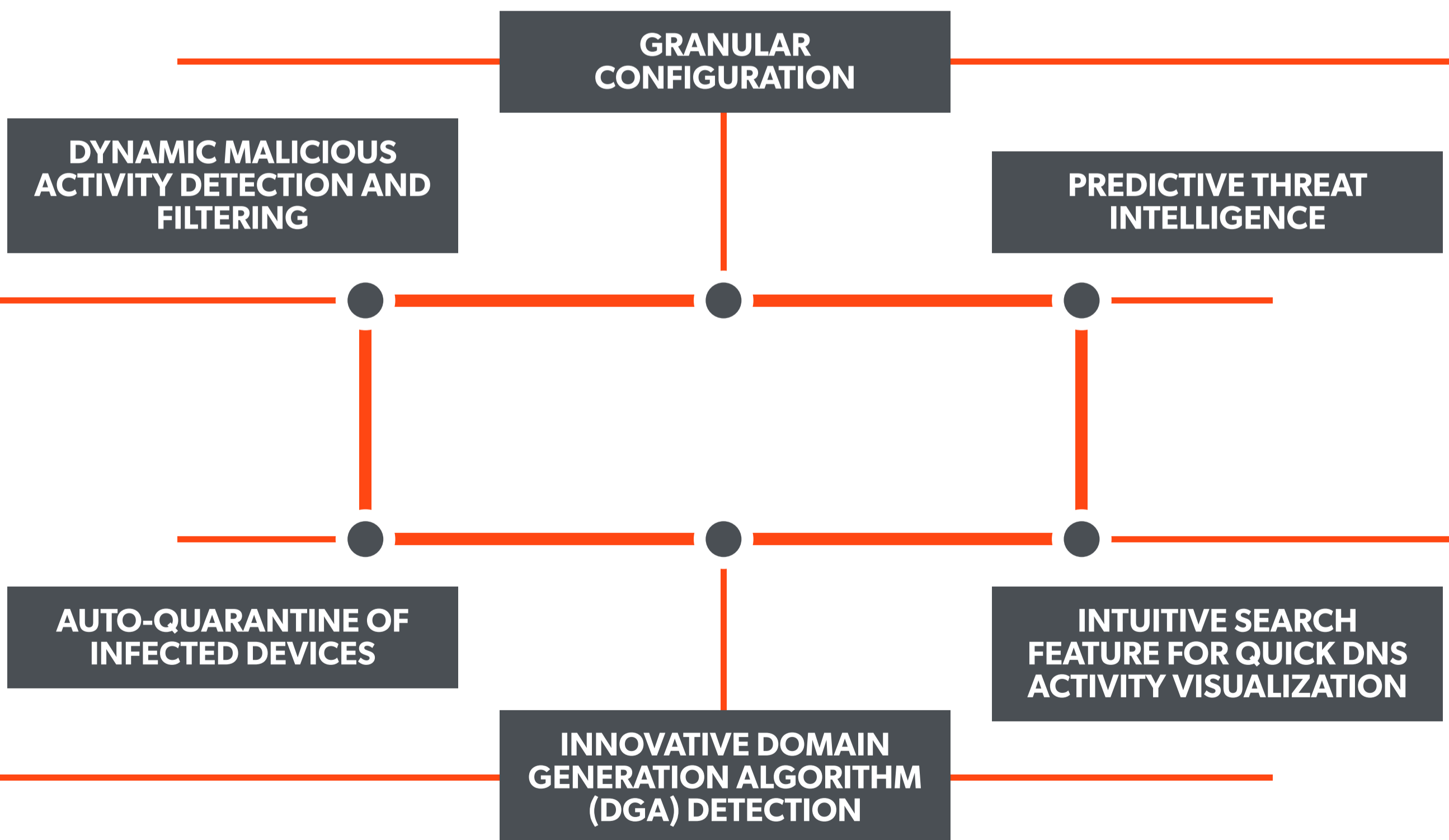
As a result, the flagged website is prevented from executing or installing phishing attacks, ransomware, spyware, crypto mining malware, and exploit kits, or connecting to command and control servers.

The solution also constantly monitors all devices for possible compromise, containing and isolating those devices from the internet and the rest of the organization's network.

Ability to visualize all DNS requests logs across an organization in near real-time in a single location.

In addition, executive dashboards and detailed reports allow security professionals to uncover valuable insights from DNS traffic.

# UNIQUE FEATURES



## KEY BENEFITS

### » HIGH AVAILABILITY AND LOW LATENCY

Globally distributed DNS network, ensuring 100% uptime. Low latency (less than 15 ms), ensuring optimized DNS resolution performance.

### » EFFECTIVE DNS PROTECTION OUTSIDE OF ENTERPRISE NETWORK

Roaming clients to protect devices (Windows, Mac OS X, iOS, Android) even when they are outside the corporate network. Quarantine infected roaming clients to prevent spread of infection.

### » UAE SOVEREIGN

The only sovereign-owned UAE entity providing DNS-focused cyber solutions, a critical consideration, given the solution's visibility into all customer DNS requests.

### » SCALABLE

Designed to scale, our product is built to grow seamlessly alongside your organization and its needs.

### » ACCURATE MALWARE DETECTION AND CONTENT CLASSIFICATION

Best-in-class malware detection and content categorization, ensuring minimal operational overheads dealing with false positives (< 0.5% false positive rate)

### » EASE OF DEPLOYMENT WITH SUPPORT FOR MONITORING MODE

Deploy in under 10 minutes across an entire organization. Manage your enterprise DNS traffic in real time.

### » CUSTOMIZATION

Flexible enough to enable different product customizations to meet unique organizational or operational requirements and requests.

### » EASE OF INTEGRATION WITH SIEM

Correlate DNS request data with other critical events in the organization to uncover valuable insights.

## SERVING YOUR ORGANIZATION

Low latency and high availability ensure DNS Firewall has no impact on the network performance and operations of an organization.

Independent third-party validations confirm latency of less than 15 milliseconds, significantly lower than global benchmarks.

A highly accurate malicious DNS detection engine allows key security personnel to focus on important initiatives and not spend precious time on dealing with false positives.

DNS FIREWALL helps your organization reduce the risk of business disruption and reputational harm caused by security breaches or theft of customer data.

Globally distributed resolvers ensure high availability while guaranteeing optimal performance anywhere across the Globe.

With 24x7 operations in the background, DNS FIREWALL ensures your organization can focus on your core operations.

”

Cybersecurity agencies in United States, United Kingdom and elsewhere, with access to the most advanced solutions, are mandating DNS-focused protections for their governments, national security and critical infrastructure.

”

# ORYXLABS

## WHO WE ARE

ORYXLABS was founded in Abu Dhabi in 2020 with a passion for cybersecurity-focused engineering.

A proudly diverse staff hailing from 22 different countries with backgrounds ranging from national defense to world-renowned top software engineering organizations joined together to develop best-in-class security solutions.

We leverage research and innovation to provide solutions in four key areas:

- » Cyber Security Assessment
- » Monitoring
- » Prevention
- » Improvement

When combined, ORYXLABS solutions provide a holistic approach to situational awareness and attack mitigation.

## OUR MISSION

Our mission is to equip cybersecurity teams with first-in-class intelligence and technical solutions that continuously assess, monitor, and improve environments to mitigate ongoing or future attacks.

## WHY US

As an agile and innovative company focused on cybersecurity, we pride ourselves on crafting highly tailored solutions to meet our clients' exact needs, not "one size fits all" products like our competitors in the domain.

With our combined experience in deep learning, AI, vulnerability research and big data, and partnerships with world-renowned subject matter experts, you can rest assured our solutions are built and run on information that is timely and accurate.

**MOST INNOVATIVE  
CYBERSECURITY  
COMPANY**



**TOP CYBERSECURITY  
SOLUTIONS  
PROVIDER**



**ORYXLABS**

21st Floor, Aldar HQ  
Al Raha Beach  
P.O. Box: 33289  
Abu Dhabi, UAE

**[oryxlabs.ae](http://oryxlabs.ae)**