Labris
NETWORKS

BUSINESS PROFILE

ABOUT
LABRIS NETWORKS

Labris Networks was founded in 2002 and headquartered in Ankara, Türkiye with offices in Istanbul. Labris Networks specializes in DDoS Mitigation, Next Generation Firewalls, Unified Threat Management, Centralized Cyber Security Management, Regulatory Compliances and SOC/CERT Services. The company offers products and services to different industry verticals which include government, IT & telecom, military, financial services, healthcare, education and others. The company has a diversified clientele across geographic regions such as Eastern Europe, MEA, CIS and East Asea in 20 countries. Being one of the Common Criteria EAL4+ certified global security gateway brands; Labris products protect enterprises, brands, government entities, service providers, and mission-critical infrastructures.

The emergence of the intelligent economy, harsh global competition and rapid technological advance has placed innovation as vital to competitiveness. Therefore, we use innovation as a mechanism by which we produce new products, processes and systems required for adapting to changing market trends. Innovation represents our competitive advantage, supported by our “Speed”, “Supportive”, “Sage”, and “Safe” mainstream capabilities. Labris Networks has been listed as the Innovation Champion of Türkiye (2014) and global finalist (2015) of the EU IMP3ROVE Innovation Program.

HOW WE WORK

Labris will stand by you against all threats you may encounter in cyber warfare today and tomorrow and will ensure the security of your network.

These high-quality security products have been developed to detect real-time threats and create a smart shield against applications, viruses, spam, malware and APT (Advanced Persistent Threat) level attacks.

Labris not only protects your network with advanced products, but also meets your highest security needs with the support services it offers.

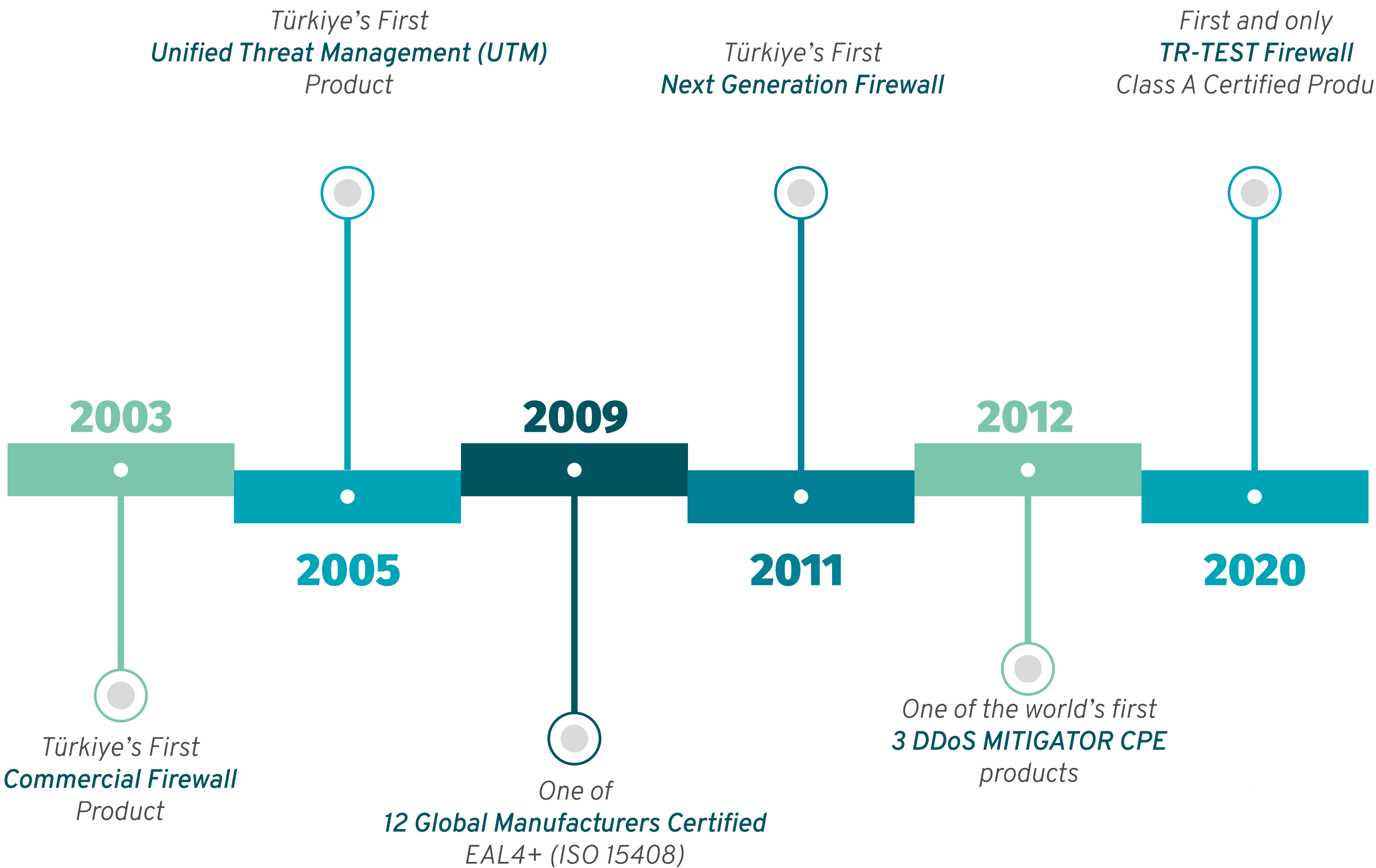
Labris
NETWORKS

REMARKS

Labris is the first and only manufacturer and product families in its field with the competence and maturity of foreign products.

Labris is the first company in Türkiye to acquire international certification (ISO 15408 EAL4+).

Labris is the first and only manufacturer in its field with Domestic certification scheme TR-Test Firewall A Level certification.



2003

Türkiye's First
Commercial Firewall
Product

2005

Türkiye's First
Unified Threat Management (UTM)
Product

2009

One of
12 Global Manufacturers Certified
EAL4+ (ISO 15408)

2011

Türkiye's First
Next Generation Firewall

2012

One of the world's first
3 DDoS MITIGATOR CPE
products

2020

First and only
TR-TEST Firewall
Class A Certified Product

INDUSTRIES

Military & Government

This sector is targeted by:

- *Foreign powers trying to spy on or adversely affect a global competitor*
- *Hacktivists who want to make a political statement*
- *Cybercriminals try to monetize the vast amount of personal information in central government and local databases.*

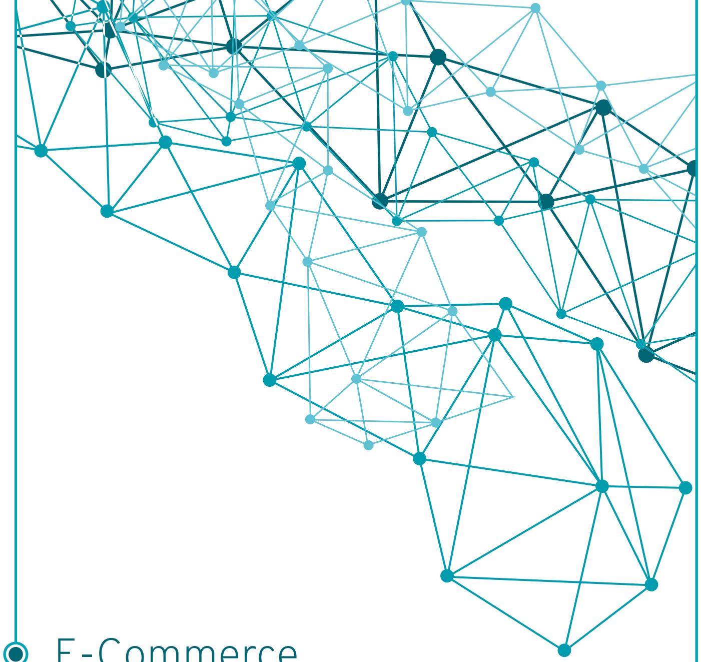
The security of the Government and Military's information resources is essential to ensuring the integrity of their operations. Cyber security operations are conducted to protect data, networks, net-centric capabilities, and other designated systems by detecting, identifying, and responding to attacks against networks

Telecommunication

Some potential cyber security threats for the telecommunications industry include:

- *Advanced persistent threats (APTs)*
- *Ransomware attacks*
- *Internet of Things (IoT) security threats*
- *Social engineering attacks*
- *Business continuity attacks like DDoS*
- *Cyber attacks by state actors*

Telecommunications operators manage the underlying infrastructure, so a cyber attack can have a huge and far-reaching impact. Even a false accusation of a cyber attack can cause a telecommunications company to shut down essential services that consumers and customers rely on. Another typical high-impact target is customer data. This private information is a tempting target for cybercriminals or insiders trying to blackmail and steal money from customers.



E-Commerce

Top Security Threats to E-Commerce Sites

- *Phishing*
- *Malware and ransomware*
- *SQL injection, Cross-site scripting (XSS)*
- *Data theft E-skimming*

E-commerce sites will always be a hot target for cyber attacks. For prospective thieves, these are treasure troves of personal and financial data and for businesses of any size, the cost of both data loss and a breach in customer trust can be devastating for businesses of any size.

Game

Some common cyber threats and how they affect gamers

- *In-game cheats and mods*
- *Personally Identifiable Information(PII) leaks*
- *Phishing attacks*
- *DDoS attacks on real time gaming*
- *Malicious payloads and Malware*

Cyber attacks are successful when game software has cyber security flaws or when users are tricked into giving away valuable information. Game developers must understand the importance of including cyber security when developing and maintaining games to ensure data is kept secure and the game continues to run as expected. Incorporating cyber security protocols into all aspects of the game and observing game data reduces the risk of successful cyber attacks.

PRODUCTS

Labris UTM

Labris UTM Series next generation network security devices provide you with integrated security against internet-based threats that are developing and becoming more complex day by day, while also meeting your legal obligations under GDPR and such laws. Labris Next Generation UTM features:

- *Application Control*
- *Filter+ and IPS+ Modules*
- *Central User Directory, Labris Wauth+ (Hotspot)*
- *Instant Traffic Monitoring (Network Visibility)*
- *Log Analysis (Log View)*
- *Secure Link/Line Load Balancing/SD-WAN*
- *L2/L3/L7 VPN*
- *Integrated Reporting*

HARPP
ddos mitigator

HARPP DDoS Mitigator devices ensure that your network and business are safe against DDoS attacks that threaten your business continuity and online presence.
The device's state-of-the-art DDoS Attack Protection Functions provide high-level protection to your DNS and Web infrastructure with normalization, blocking and protocol-specific security methods.
In addition, priority protection functions work proactively at all times, day and night. HARPP DDoS Mitigator devices around the world create a vast real-time security intelligence network that is instantly accessible.

Labris MNG

Labris Centralized Management (Labris MNG) appliances are designed to manage your Labris network infrastructure on a carrier grade scale.
By using Labris MNG appliances it is easy to,

- Monitor your Labris Networks devices and health status
- Push network policies on a global namespace, domain or user group basis
- Monitor VPN connections in a distributed environment
- Get the management console of specific devices easily

Labris Wauth+

Labris WAUTH+ can offer flexible solutions according to the guest user type and guest authorization scenario of each institution.
It offers wide range of authentication methods for guest and provide interfaces all guest users can be viewed through.

SERVICES

Security Operations Center

In our Security Operations Center (SOC), we closely monitor your devices, cyber attacks, and security events. Our teams which include Cyber Warfare Labs (CWL) staff, analyze possible security vulnerabilities and make provisions. Thus, we protect what's valuable for you with our provisions and the technology developed by us.

Close Security Support

Our Close Security Support (CSS) team monitors the alarms coming from your systems 24/7 and provides the close support that you need to use your infrastructure in the most effective way. When you purchase a Labris product, you also benefit from the advantage of having the most suitable SLA standard for your business.

Cyber Warfare Lab

Labris Networks conducts intense inspections of world-wide and critical networks with its installed devices and sensor networks. These studies are converted into technological infrastructure and signatures, and distributed to devices by Labris Networks' security events research center Cyber Warfare Lab™.

There are six defined activities in the scope of the HARPP DDoS CERT.

Service Activation

Analyzing the existing environment as a whole and planning for HARPP DDoS Mitigator placement.

Tuning

The aim of tuning to generate an Application Anomaly Signature (AAS) specific to customer services to prevent DDoS and minimize the false positives.

7x24x365 Monitoring

All HARPP DDoS Mitigator devices are connected to HARPP SOC as a part of this service for ensuring continuous monitoring. Service levels are continuously monitored and incident handling is done according to the agreed SLA's.

Monthly Service Review

This part of the service ensures that HARPP DDoS protection is updated with the changes to the applications themselves and the user/client characteristics. HARPP CERT Team reviews the customer environment on a monthly basis and ensures that DDoS protection is effective and not causing false positives.

Attack Mitigation

All HARPP DDoS Mitigator devices are connected through HARPP SOC and monitored. If there is an incident recognized as a DDoS attack, this is immediately seen by the HARPP DDoS CERT Team and attack mitigation starts.

Post Incident Reporting

After major incidents, there is a specific report prepared as a result of that event. This report can be directly sent to upper management as an expert review and used to explain the incident and how it was handled.

labrisnetworks.com

CLOSE SECURITY
IN CYBER WAR

7 · 24 · 365
GLOBAL SUPPORT

info@labrisnetworks.com