NAAD Products

Convenient, but Impenetrable

- NAAD network security products offer a new level of communication security in organizations. These products are specially designed and built for the purpose of connecting sensitive networks in organizations that maintain national vital infrastructure.

- These products, in addition to establishing security by using an exclusive architecture that can make penetration into the organization almost impossible, have a very simple user interface and can be installed and used simply in any complex network.

- Dena and Damavand are in the category of network gateway security products and have been produced with the aim of preventing the penetration of the attacker into the organization and preventing the leakage of the organization›s sensitive information. These mentioned products connect various local networks of the organization with a very high security level.

NAAD, the provider of mission-critical products in the field of network security

Ensuring the security of sensitive infrastructures of organizations by relying on the technology edge

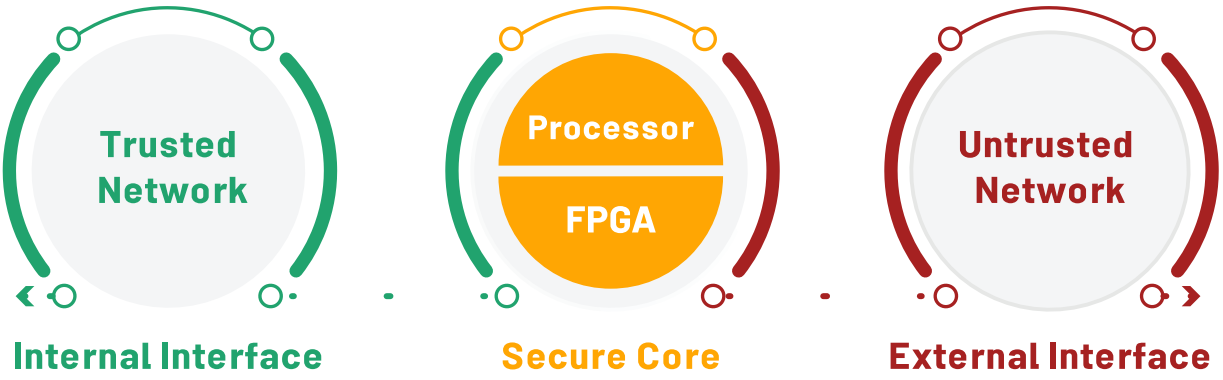
Suitable for the expansion of air-gapped networks and remote connection to sensitive networks

Why are NAAD products impenetrable?

- The main feature of NAAD network security products compared to other products in the market is the implementation of sensitive parts on these products, including the cryptography part in the form of hardware and on FPGA. Due to this type of design, these products are resistant to many attacks that target software systems, and also provide the possibility of implementing special custom crypto algorithms for organizations.

- In addition to the hardware part, in the main core of the product, there is a processor for executing complex protocols, on which a software program is executed. In order to maintain high security in this part, a bare-metal design is used. In this type of design, no conventional operating system is used, and the software is implemented directly by re-implementing small parts of the operating system.

- The architecture used in NAAD network security products, which is a combination of hardware and software, simultaneously takes advantage of the benefits of software and hardware (Hardware-Software Co-Design). With the combination of the strengths of each, it has created impenetrable products. The main features of this architecture are the use of FPGA in hardware and bare-metal design in software, which greatly reduces the risk of intrusion and vulnerability.



Two categories of products for two different needs:

Damavand product category:

The product of this category is suitable for use in organizations or datacenters (enterprise environment) and has the ability to create communication for several people at the same time.

Dena product category:

This type of product is similar to Damavand products in terms of functionality, but it has smaller dimensions and is suitable for personal use in a portable or stationary form.

Current infrastructure problems of organizations:

1 The high cost of hardening network by isolation/air-gap methods

Some of the current infrastructures of sensitive centers in the world are physically separated from the environment. Dark fiber and dedicated links are used in common isolation methods. These methods have some problems, including high maintenance costs and high expansion costs (financial and time). Sometimes they also create complex problems due to geographical and civil reasons.

If these infrastructures use hardware-based high-security methods, it will be possible to add new networks at a much lower cost.

2 Existence of various types of vulnerabilities in software hardening (MPLS, VPN Server, etc.):

Hardening by software application methods creates weak points, including vulnerability in the software supply-chain in the system, which is the cause of many cyber attacks.

3 Impossibility of remote connection of specialized employees of the organization:

In the infrastructure architecture based on physical isolation, it is not possible to connect to the organization›s networks remotely. For example, the senior experts of the organization need to have access to the main network on sensitive occasions during non-office hours. This need has been resolved with the help of the individual products group (Dena).

4 Difficulty of using security products:

Some organizations buy products to secure their own network, but do not use this product due to inappropriate support and difficulty in configuration. This issue has been considered in the user experience designs of NAAD products. For this reason, simple user interfaces with the ability of quick configuration have been utilized.

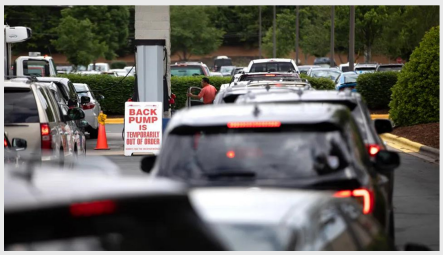
5 The possibility of a backdoor in unsafe products:

One of the concerns of organizations that use untrusted security systems is the existence of a way of penetration inside the devices by the equipment manufacturer itself. The use of safe security systems eliminates this concern.

Attack on Iran`s fuel network

In this attack, the smart fuel system was unavailable for a while, which resulted in a lot of media coverage. In many attack methods, the first step is to infiltrate the organization`s internal network. If the system prevents penetration, it stops the attacker in the first step.

Attack on the Colonial pipeline fuel supply network in United States in 2020

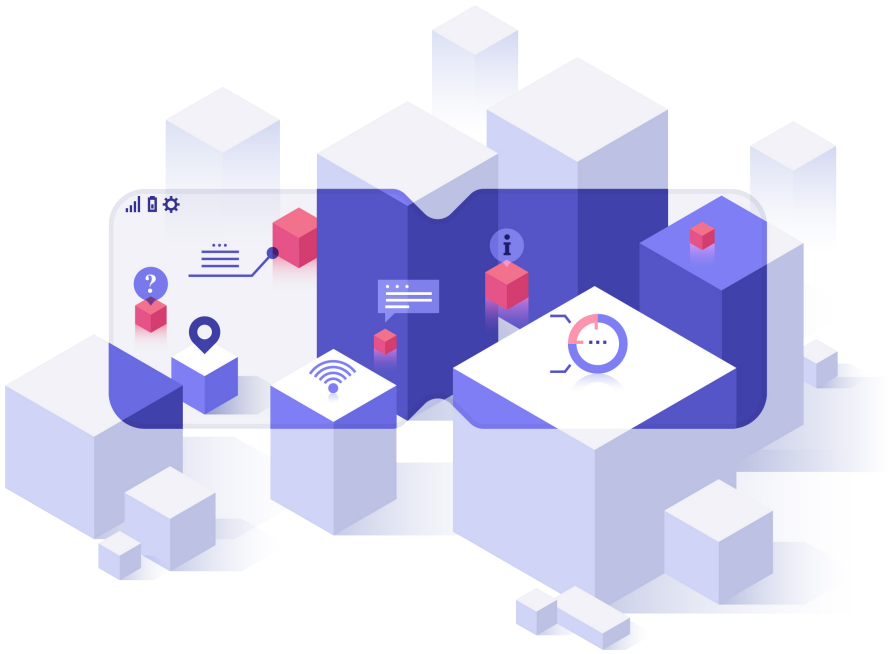


In this attack, the fuel supply system in the Southeastern United States was disabled for several hours. This attack occurred through the penetration of the organization`s network and the vulnerability of the internal network. The proposed security by means of hardware is completely suitable and safe for this type of attack.

zero day vulnerabilities:

These types of vulnerabilities cause the most dangerous attacks on systems. Zero-day is a kind of software vulnerability that the software maker is not yet aware of or has not yet succeeded in providing a solution to solve it. Every year, a large number of exploits caused by zero-day vulnerabilities are executed on systems and cause great damage to them.

The probability of finding these vulnerabilities is proportional to the size of the software, and for this reason, the bare-metal architecture in NAAD products is much safer against these attacks.



Why should we use NAAD products?

1 Low-cost and fast expansion of the internal network:

To add a new branch to the organization and connect it to the internal network, it is enough to connect the new branch to the internal network by installing the Damavand product as the gateway and performing its initial settings.

2 Security products with innovation in architecture:

The security of NAAD products is based on its architecture and design method, and it is fundamentally different from other security methods.

3 Continuous support and security of products by the expert team:

The security control team of the NAAD company is constantly in the process of hardening and security testing, and they ensure the security of the product during use.

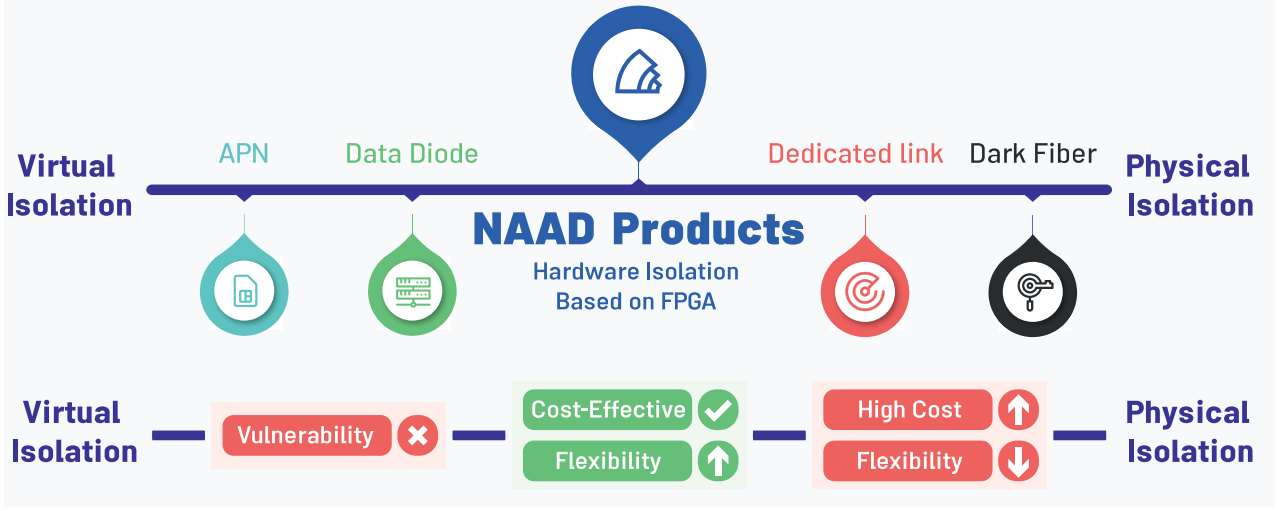
4 Simple configuration (Play & Plug):

The design of user interfaces is in a way that provides the user with the possibility of quick setup and setting of the device in various conditions.

5 Possibility of remote connection of specialized employees of the organization:

By using Dena in companion with the Damavand product, it is possible to have a remote connection for some employees without reducing the security of the main network.

Types of network isolation methods:



The current methods of isolating sensitive networks are divided into two categories: Physical isolation and virtual isolation. Products such as VPN servers, using a Linux operating system in the main part of their processing, are classified as virtual isolation. These products are not safe from the vulnerabilities of the operating system and other dependent packages, even if they have secured their original software.

On the other hand, approaches such as the use of dark fiber or dedicated links for network security are classified in the category of physical isolation.

As mentioned, these approaches incur a lot of costs in expanding and maintaining the access to the organization network. Another problem is inflexibility and interruption in the workflow of the organization.

NAAD products, which are made with a special architecture, offer a different method of isolation in the hardware layer, which can be a suitable substitute for physical isolation. These products, which have a secure hardware-software core, are based on FPGA in the hardware part, and bare-metal design is used in the software part.

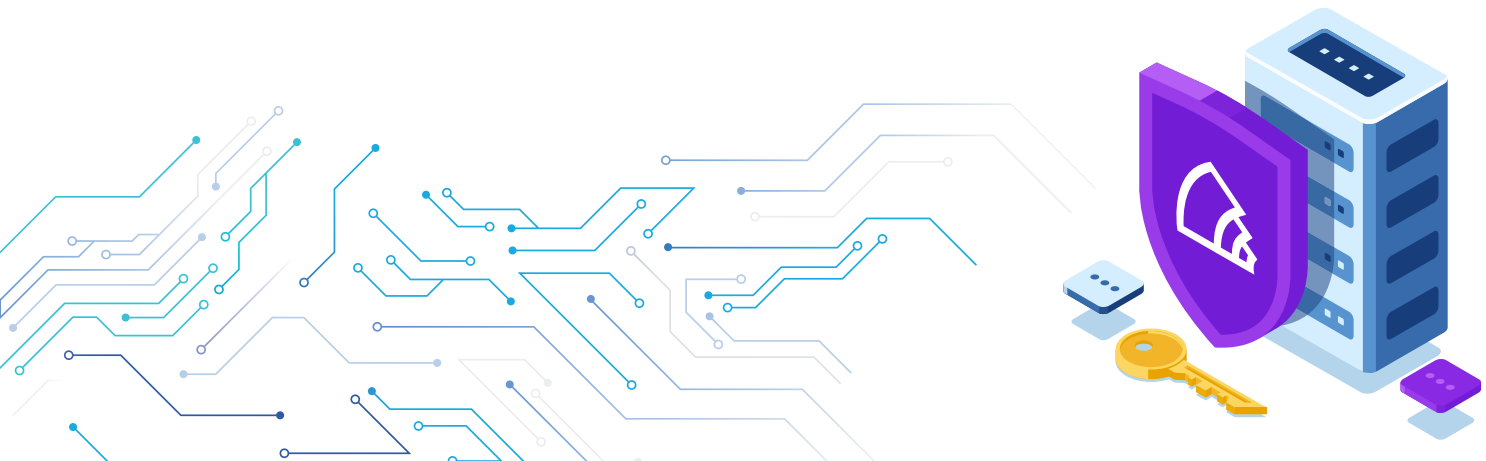
Sharif Secure-minded innovators, NAAD, has been established by a number of academic fellows and researchers of Sharif University of Technology in 2014 with the aim of securing the national vital infrastructures.

So far, this company has succeeded in moving towards its mission by securing the communication infrastructures of sensitive organizations in Iran.

Dena Desktop

Dena Portable

Type		Dena Desktop	Dena Protable
Baremetal architecture (very small OS+ Software foot print)		Yes	Yes
Tunneling	Encrypted Traffic Throughput	16 Mbps	16 Mbps
	Simultaneous tunnel instances	1	1
	Layer 3 tunneling (tun)	Yes	Yes
	NAT traversal	Yes	Yes
	Tunnel Cryptographic Algoritms	RSA 2048/4096 AES GCM 256 ECDH	
	Post-Quantum security (Handshake static key)	Yes	Yes
	Certificate-based tunnels	Yes	Yes
	2 Factor Authentication	Yes	No
Interfaces	Internal Interface	1* 10/100Eth	3G/4G/LTE
	External Interface	USB	WIFI & USB
Security	Side-Channel security	Yes	Yes
	Custom ECC Curves	No	To be negotiated.
	Custom Algorithms	No	To be negotiated.
Tamper	Encrypted Flash	Yes	Yes
	Firmware integrity check	Yes	Yes
	Internal RTC	Yes	Yes
	Temper Resistant	No	Yes



Damavand

Family		200 Mbps	1 Gbps		
Type			Base	Standard	Premium
Tunneling	Encrypted Trafic	200 Mbps	1 Gbps	1 Gbps	1 Gbps
	PPS	16 Kpps	1 Mpps	1 Mpps	1 Mpps
	Simultaneous instances	120	120	120	240
	tun support	Yes	Yes	Yes	Yes
	tap support	Yes	Yes	Yes	Yes
	NAT traversal	Yes	Yes	Yes	Yes
	Handshake StaticKey	Yes	No	No	Yes
Networking	VLAN	Yes	No	No	Yes
	External Interface	1x GigEth - RJ45			
	Internal Interface	1x GigEth - RJ45			
HSM	Certificates	Yes	No	Yes (max.150)	Yes (max.300)
	2 Factor Authentication	Yes	Yes	Yes	Yes
	PKCS11	Yes	Yes	Yes	Yes
	Side channel security	Yes	Yes	Yes	Yes
	Cryptographic Algorithms	RSA 2048/4096 AES GCM 256 ECDH			
	Custom ECC Curves	No	No	No	No
	Custom Algorithms	No	To be negotiated.		
Encrypted Flash		Yes	Yes	Yes	Yes
Firmware integrity check		Yes	Yes	Yes	Yes
Zeroization		Yes	Yes	Yes	Yes
Internal RTC		Yes	Yes	Yes	Yes
Audit Log		No	No	No	To be negotiated
Monitoring		No	No	No	To be negotiated

info@naadsecure.ir
+98 9124701183
www.naadsecure.ir
021-66013542