FENROR7

LATERAL MOVEMENT CYBER SOLUTIONS

AVOID THE UNNECESSARY COSTS OF LATE THREAT DETECTION

Reveal undetected cyber threats as they move

Using existing technologies, detecting cyber threats takes months, resulting in global annual losses estimated at hundreds of billions of dollars with financial firms, technology, utilities and energy companies taking most of the hit.

Costing tens of thousands of dollars a day, undetected cyber attacks can get costly if they are not detected quickly.

Reveal undetected cyber threats as they move

Fenror7 developed lateral movement detection engines based on an innovative approach to detecting internal cyber attacks.

Using our lateral movement detection products, companies can reduce the time it takes them to detect internal threats from months to hours.

Near immediate detection provides more time for prevention and significantly reduces costs related to the attack.

Reveal undetected cyber threats as they move

Why Fenror7

Lateral Movement Detection

Organizations never intentionally provide direct access to their crown jewels from the outside.

Even highly targeted and focused attacks require the attackers to move laterally throughout the organization's network, exploiting vulnerabilities in software, hardware and even business processes as they close in on their ultimate target within the organization.

A new approach to threat detection

Many existing security products focus on providing automatic prevention of attacks. While these methods may work in small scale settings, they do not work in large scale due to the inherent gap between a full lock down of a network, and the organization's ultimate goal of conducting business.

If large scale automated prevention of crime doesn't work in the "real world", why would computer networks be any different?

Focusing on the fundamental concepts of an attack

Our products work at the network level, detecting fundamental attack concepts based on an attacker's need to move laterally within the enterprise. Effective detection of traces of these attack concepts provides early warning that lets security teams shut down the attack before the attackers achieve their goals

Agentless out of band solution

Fenror7's products run completely out of band and do not require installation of agents on your devices to provide fast and accurate detection, while automatically supporting any type of device connected to your network.

Reveal undetected cyber threats as they move

Consistent early detection

By focusing on detecting attack concepts instead of exploited vulnerabilities, Fenror7's lateral movement detection engines require less updates compared to other solutions, and are less sensitive to constant changes in attack trends and zero-days.

Whether your enterprise's network consists entirely of workstations and servers, or if it also includes your vehicle fleet or coffee machines, Fenror7 will provide the same consistent early detection every time.

You own your data

Fenror7 believes that your data and what goes on in your enterprise belongs to you, and only you. We developed a detection technology that can detect threats even over encrypted networks, and we do not mandate that you "share with the community".

Plug & Play

Developed by hackers and CISOs, our detection technology was designed from the ground up as a simple plug & play lateral movement detection product, based on a simple architecture that does not rely on complicated sandboxes, test environments or network benchmarking to provide easy to read alerts and reports.

Secure by design

Fenror7's products are secure by design and run on fully patched and hardened Linux servers connected to your network in an out of band architecture that provides the highest level of security possible.

Our products

Fenror7 multi-site enterprise solutions

Fenror7's multi-site enterprise solutions provide a single management point for multiple engine servers.

Our scalable multi-site solution is designed for large enterprises with data centers spread out over multiple geographic locations, and consists of a multi-site management server and detection engines based on our stand-alone W-series servers.

Series		E-1000	E-2000	E-3000	E-4000	E-5000
Base configuration[1]	Multi-site management server	E-1000m	E-2000m	E-3000m	E-4000m	E-5000m
	Included W-1000e detection servers	0	0	5	8	20
	Included W-500e detection servers	0	4	3	2	5
	Included W-200e detection servers	4	2	0	2	5
Supports fiber optic capturing interface?		No	Yes	Yes	Yes	Yes
Maximum number of supported detection servers[2]		20	50	150	200	300
Typical organization[3]	Number of employees	1,000 employees	5,000 employees	20,000 employees	100,000 employees	200,000 employees
	Number of datacenters	4	6	8	12	30

Fenror7 stand-alone on premises solutions

Fenror7 W-series is our stand-alone lateral movement detection product, providing single-site organizations with the same detection capabilities of Fenror7's enterprise solutions.

Model	W-50V	W-200	W-500	W-1000
Maximum effective throughput	500Mbps	1Gbps	3Gbps	5Gbps
Typical organization size[3]	500 employees	2,500 employees	5,000 employees	10,000 employees
Capturing Interfaces	Dedicated physical port	2 x 1Gbps (copper)	1 x 10Gbps (fiber) 2 x 1Gbps (copper)	2 x 10Gbps (fiber) 4 x 1Gbps (copper)
Form Factor	Virtual Machine	1U	2U	2U

[1] Additional scalability is possible by adding detection servers in addition to the detection servers provided in the base configuration shown here.
[2] Represents the total number of detection servers supported by this series.
[3] Represents typical organization size. Requirements may vary depending on actual utilization of organization network bandwidth.

FAQ

What makes Fenror7 better than my existing detection solutions?

Using existing detection solutions, internal attacks go undetected for many months. Fenror7's engines provide near immediate detection giving your organization time to defend itself at the early stages of an attack.

How is lateral movement detection different than other detection methods?

Other detection methods often rely heavily on detecting exploitations of specific vulnerabilities or analyzing user behavior. While these detection methods can detect attacks, using them is in many ways similar to glancing through a key hole, and missing the bigger picture. This is due to the fact that they require constant updates and can be bypassed easily by introducing slight variations to known attack methods.

While exploits and payloads can be changed easily by attackers, they will not be able to avoid moving laterally within the enterprise as they move towards their ultimate goals.

Can Fenror7 integrate with my SIEM?

Fenror7's enterprise and stand-alone products are able to fully integrate with any standard SIEM system. Our products are also capable of integrating with Active Directory as well as Network Access Control systems and Firewalls, allowing you to get more out of these systems.

How do you prevent Fenror7's products from becoming an attack platform?

All of our products run on fully patched and hardened Linux servers, and are designed as out-of-band solutions connected to a network tap.

FENROR7
LATERAL MOVEMENT CYBER SOLUTIONS

REVEAL UNDETECTED CYBER THREATS AS THEY MOVE

FENROR7 REDUCES THE AVERAGE THREAT DETECTION TIME FROM MONTHS, TO HOURS, PROVIDING NEAR IMMEDIATE DETECTION OF INTERNAL CYBER ATTACKS

www.fenror7.com
info@fenror7.com

Global HQ
Galgalei ha-Plada St 16
Herzliya, Israel

US Office
Fenror7
PO Box 1167
Northbrook, IL 60065
USA

Frankfurt Office
Fenror7
Platz der Einheit 2
60327 Frankfurt am Main
Germany