Muninn

We See. We Act.

Proof of Value Process

What is Proof of Value?

Proof of Value (PoV) is a unique opportunity for companies and organizations to experience the effectiveness of a Muninn AI Detect and Muninn AI Prevent within their own computer networks. With our intelligent network sensor, complete with built-in machine learning, you can protect your network from emerging threats and ensure the safety and security of all your company's data.

Our experienced technicians will install the sensor and provide access to the highly intuitive Muninn Dashboard. Our dashboard will give you a complete overview of all network activity. Throughout the PoV our specialized support team will update you on all findings, in order for you to gain a deeper understanding of your network's behavior and potential security vulnerabilities.

Why Proof of Value?

Gain total overview

Today's digital networks are often busy and highly complex, which makes it very hard for companies and organizations to know exactly what is happening when and where within their network. Muninn models, maps out and learns every device's behavior in real time to visualize all network traffic, which allows your cybersecurity team to gain the full overview.

- Discover all network activities
- Gain the ability to accurately identify specific parts of your network's infrastructure down to device level
- Discover possible cybersecurity vulnerabilities

Always one step ahead

Muninn discovers the cyber threats of tomorrow using automatic Machine Learning and probabilistic mathematics. Our system stays informed and learns the normal behavior patterns of your network traffic. That's how Muninn discovers threats from the outset of the attack.

- Muninn's AI engine begins baselining the network from day one
- Be aware of threats before actual damage is done
- Be able to take precautionary measures in time to minimize risks for your organization

Muninn threat report

During the PoV period, our support team at Muninn will introduce you to our Dashboard, continuously keep you updated on all findings and help you calibrate the sensor. The PoV process is concluded with a detailed report on vulnerabilities and anomalies within your organization's network, detected by Muninn. With experience from the Danish Defense Intelligence Service and universities such as M.I.T. and DTU, our analysts have a deep understanding of which steps must be taken to secure your networks in the best possible way.

The PoV process

1. Installation of Muninn AI Detect and Prevent

A Muninn sensor will be set up by one of our technicians in 1-2 hours depending on the company's network structure.

2. Data collection
Immediately after installation, Muninn will begin capturing raw packet data and extract metadata to obtain the maximum overview of the company's network. All data will be collected passively without any negative impact on the network's performance. In practice, packet capture is done in one of the following ways:

- Muninn is connected to a SPAN on the "Main Switch" of the network, from which it receives copies of raw data directly.
- Muninn is connected through a Test Access Point (TAP).
- A virtual Muninn sensor is connected using a virtual switch / VDS (VMware or HyperV)

3. Data analysis and modeling
Muninn utilizes advanced Machine Learning algorithms to process the data as it is being gathered. This leads to the creation of a model for the company's digital network and establishes a baseline for regular traffic. With the help of Muninn's anomaly detection module, any actual anomalies can then be identified.

PoV timetable – Over 4 weeks

Levels	Timetable	Steps
1	Pre-PoV	• Arrange dates for the installation of Muninn. When Muninn runs satisfactorily – the 3 PoV meetings will be set.
	Day 1	• Installation (1-2 hours) • Validation of system compatibility • Activation of Machine Learning • Cyber Threat Detection is activated
	Week 1	• Muninn maps out the company's network and establishes a baseline image of the network traffic • MEETING 1 – ONLINE (or onsite) 1 hour • Discover your network – see what's happening and who makes it happen, while it's happening • Get a demo walkthrough of the Muninn dashboard • Begin using the Muninn dashboard • First notifications are appearing
2	Week 2	• After 2 weeks: MEETING 2 – ONLINE 30 min. • Observed user behavior outside of the norm – anomalies (if any yet) – and further questions and answers
3	Week 3	• The initial learning phase of the Machine Learning engine is complete • Discover and assess real time notifications for true anomalies, which have compromised network security
4	Week 4	• MEETING 3 – ONSITE (if possible) 1-1,5 hours • Detailed report on relevant network activity for the entire POV period is presented • The PoV expires
	Post-POV	• Discuss which subscription deal and service package could suit your needs best

Try Muninn AI Detect and AI Prevent

Book an online demo, a meeting or order your Muninn sensor already today by writing us an email at sales@muninn.ai or give us a call +45 70 60 59 08.