Products Solutions

Muninn

Version 2.0

Muninn

We See. We Act.

AI Detect

Contact us

Your Key Benefits

- ✓ Full visibility of all activity within your network.
- ✓ Including on-premises, multi-cloud and IoT infrastructure
- ✓ Detects known and unknow threats in the earliest stage
- ✓ Reduces time spent on threat investigation
- ✓ Minimizing the alerts for false positives

Detected Network Breaches include

- ✓ Malware, ransomware, botnets and worms
- ✓ 0-day attacks and other unknown threats
- ✓ Suspicious traffic using Tor, Darknet, BitTorrent or tunneling
- ✓ Newly introduced services in the network e.g. SMTP or FTP file server
- ✓ Brute-force attempts

See all Network Activity

In today's fast-paced digital world, cybercriminals are constantly evolving and adapting their tactics to bypass traditional signature-based security solutions. Unfortunately, basic security tools like firewalls, endpoint security agents, and other legacy technologies are no longer sufficient to detect and neutralize these sophisticated attacks.

The consequences of a cyberattack can be devastating for any business and organization - not only can it cause a loss of revenue, but it can also damage your reputation and erode customer trust. That's why it's essential to have a close eye on all your network activity and establish a comprehensive approach to cybersecurity that considers the latest threats as well as grows with your network, whether this includes home office or different production sites.

Detect Known and Unknown Threats

Designed to think and act like a human, **Muninn AI Detect** uses Artificial Intelligence alongside signature and script models to identify and respond to novel as well as known common threats. Our Machine Learning involves training algorithms using data, allowing **Muninn AI Detect** to learn and improve over time without being explicitly programmed. Muninn is able to process vast amounts of data, recognizing network patterns and making decisions based on those patterns, and unlike humans our AI does so 24/7.

Protect Your entire Organization

Muninn AI Detect allows your cybersecurity team to maintain a real time overview of the entire digital estate through a single interface. By continuously learning your network behavior it reduces false positives and lets your team focus on the real threats, enabling them to rapidly neutralize these threats regardless of where they enter your organization.

Muninn

We See. We Act.

AI Prevent

Contact us

Your Key Benefits

- ✓ Blocks attacks immediately within seconds
- ✓ Email and dashboard alerts when Muninn identifies and stops an attack
- ✓ Isolating the attacker without interrupting business operations
- ✓ Easy set up and configuration

Detected Network Breaches include

- ✓ Compromised IoT devices
- ✓ 0-day attacks
- ✓ Ransomware attacks
- ✓ Data Exfiltration attempts
- ✓ Brute-force attempts

Time-Saving Response

Due to the lack of cybersecurity staff and the growing complexity of digital networks, security teams are working harder than ever to monitor and control their digital estate. Today's cyberthreats are sophisticated, fast-moving, and often devastating. Cybersecurity teams do not have the resources to stay alert around the clock and to act fast enough. **Muninn AI Prevent**, uses artificial technology to instantly mount the most effective response to cyberthreats.

Because the **Muninn AI Detect** autonomously learns normal network behaviors and has a highly developed understanding of your organization's legitimate traffic patterns, **Muninn AI Prevent** can respond to novel threats that have never been seen before – buying your security teams the time they need to catch up.

Strategic Defense Mechanism

Leveraging strategic defense mechanisms, **Muninn AI Prevent** acts as the AI-hub of the entire security stack. Through integrations, this technology can seamlessly add AI power to your existing defense infrastructure.

Our self-learning AI responds through firewalls, software defined networks, and network devices such as switches or routers.

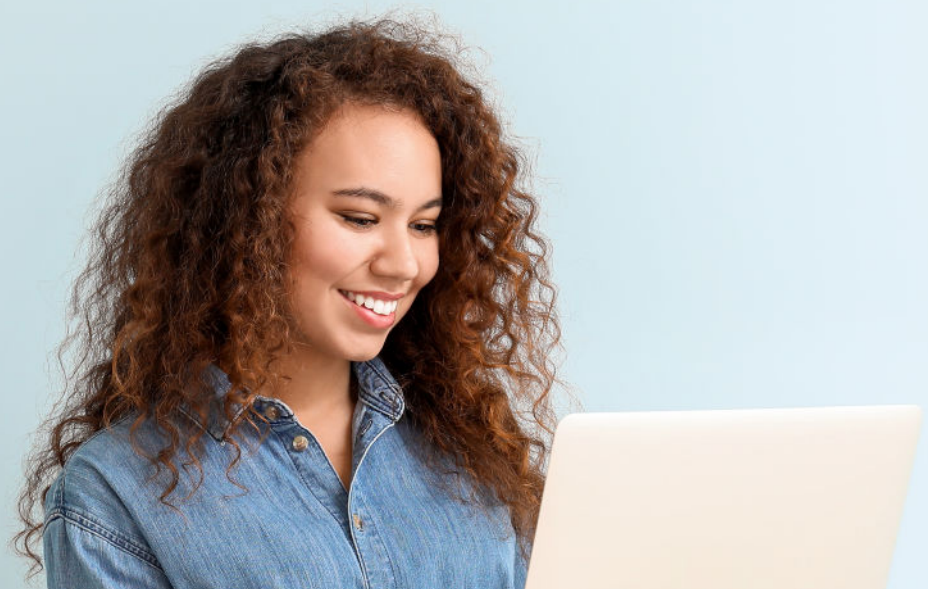
Through Tactical Defense Mechanisms

Through tactical defense mechanisms, **Muninn AI Prevent** autonomously neutralizes attacks immediately, without relying on third-party security tools or network devices.

Each action **Muninn AI Prevent** takes leverages a highly developed understanding of the organization's normal network behaviors, ensuring that daily business operations continue uninterrupted, while preventing further harm.

Muninn

We See. We Act.



Muninn & GDPR

Contact us

Data breach, malware and hacker groups are words you hear in the news each day. Due to the vast amount of sensitive data, we store online, every company and every person are being targeted. This has led to the introduction of the GDPR, an effort of the European Union to hold businesses accountable for data privacy and data protection.

All companies that hold EU personal data, regardless of the nation of origin, must disclose breaches. Failure to comply with these rules will result in a fine of up to 4% global turnover (or 20 million Euros). These fines may seem severe, but they help businesses understand the data they collect and the severity of data protection more. Complying with these rules creates much needed trust between customers, employees, and businesses.

State of the art cybersecurity

Utilizing advanced Machine Learning and AI technologies, Muninn is able to detect, report, and prevent a wide range of anomalies, security incidents, and compliance breaches, ensuring the implementation of best practices for your network security.

GDPR Requirement	How Muninn helps fulfill this
Article 25 Data protection by design and by default … "the state of the art"…	Muninn is specifically designed to ensure data security through its advanced threat detection and immediate response mechanism. Today leading security analysts strongly recommend state-of-the-art protection tools like Muninn AI Detect and Muninn AI Prevent. Our cutting-edge technology enables continuous, autonomous, and intelligent monitoring and protection around the clock.
Article 321 …the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk…	Through constant monitoring for abnormalities, detection of non-compliance and sub-standard connections, Muninn empowers you to maintain the highest security standards. Moreover, when combined with a strong security partner, Muninn functions as a continuous pen-testing tool in specific areas of your IT infrastructure, helping you to enhance the security of your network consistently.
Article 33 Notification of a personal data breach to the supervisory authority	To report incidents within 72 hours of detecting a breach, Muninn: • Stores searchable logs of all data events, increasing the speedof reporting incidents. • Immediately stops data breaches and prevents further harm. • Unlike many other solutions, such as SIEM and Log Management, it includes actual raw data, not just metadata. • Enhances the speed of identifying advanced persistent threats, preventing breaches from occurring. • Reduces the need to spend money on incident recovery, thereby helping to save costs.
Also see Recitals 85, 87 & 88 Dealing with the forensics and whether adequate tooling was in place	Muninn provides continuous monitoring for anomalies, breaches, and suspicious activities on a network, including IoT devices. Our features to ensure GDPR compliance include: • Detecting, logging, and blocking file-sharing activities. • BitTorrent logging and blocking. • Logging and blocking of IoT activities. • Reporting on SSL, TLS, and certificate non-compliance, and best practices to follow in case of breaches.