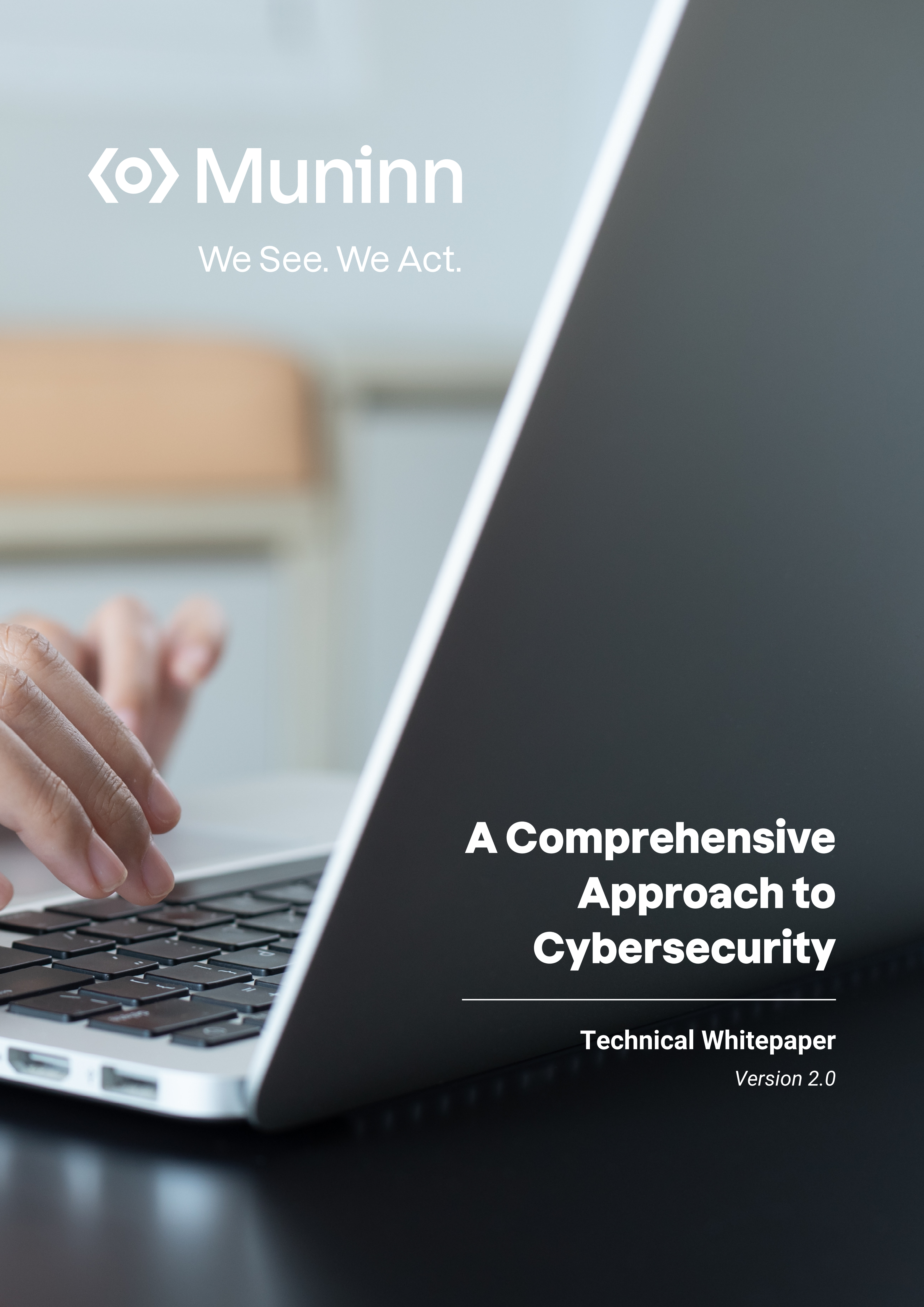


Muninn

We See. We Act.

A Comprehensive Approach to Cybersecurity

Technical Whitepaper

Version 2.0

TABLE OF CONTENTS

1. What is Muninn AI Prevent and Muninn AI Detect

In today's fast-paced digital world, cyber-criminals 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.

A Comprehensive Approach to Cybersecurity

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. Muninn' machine learning involves training algorithms using data, allowing our AI 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 Muninn does so 24/7.

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

Isolating and Blocking Threats

Muninn's autonomous response technology, Muninn AI Prevent, uses AI to instantly mount the most effective response to cyber-threats.

Muninn AI Prevent works both as a stand-alone blocking mechanism using TCP / IP reset commands sent to the device causing the critical high alert. It can also be integrated into certain 3rd party network types with an open REST API or into endpoint software with an OPEN REST API that has an "isolate" capability. Muninn AI Prevent also integrates into SIEM systems such as IBM QRadar (Forwarding notification information using syslog and flow data) and others.

A partner operating a SOC / SAC / NOC / MSS service can then aggregate all alerts from all systems in one place and provide 24/7 monitoring, security advice on best practice, network hardening etc..

2. Introduction to Network Detection and Response

Gartner defines Network Detection and Response (NDR) as follows; "NDR solutions primarily use non-signature-based techniques (for example, machine learning or other analytical techniques) to detect suspicious traffic on enterprise networks. NDR tools continuously analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior. When the NDR tools detect suspicious traffic patterns, they raise alerts. In addition to monitoring north/south traffic that crosses the enterprise perimeter, NDR solutions can also monitor east/west communications by analyzing traffic from strategically placed network sensors."

NDR is a cutting-edge cybersecurity technology that has emerged in recent years as a tool for organizations to combat the growing sophistication of cyberthreats. This technology provides real-time monitoring and analysis of network traffic, enabling organizations to quickly identify and respond to potential threats. Using advanced machine learning algorithms, behavioral analysis, and threat intelligence, NDR solutions provide comprehensive visibility into network activity, detecting and alerting security teams to suspicious behavior.

NDR's proactive approach helps organizations to stay ahead of the ever-changing threat landscape and protect their valuable assets. By leveraging NDR technology, businesses can detect and respond to cyberthreats quickly, minimizing the impact of an attack and reducing the risk of data breaches, financial losses, and reputational damage.

This makes Muninn a prime example of an NDR. Muninn AI Prevent working as an active blocking system, operating in real-time against threats like malware attacks, can even be considered an IPS (intrusion prevention system).

In general, there are two types of NDR's: Those that work on raw network traffic, which is received via a span/mirror port or, And others based on simple flow data generated from network switching equipment, e.g. NetFlow. Both types have their own advantages and disadvantages.

TYPE	ADVANTAGES	DISADVANTAGES
Raw data capture	Full data stream to perform analysis on. Can extract metadata which contains the same but often much more data than NetFlow	In general, more costly to deploy, due to higher CPU, memory and storage need.
NetFlow	Easier to fully deploy across a large enterprise.	A lot less information to base anomaly detection on.

2.1. EDR vs. NDR

Endpoint Detection and Response (EDR), another cybersecurity solution, has gained significant attention in recent years. One noteworthy similarity between EDR and NDR is their shared emphasis on detecting advanced threats in an organization's IT infrastructure

EDR vs. NDR Comparison Table

TYPE	ADVANTAGES	DISADVANTAGES
NDR	Automatically covers all devices in the network.	Only covers devices while inside the perimeter.

EDR	Gives in-depth information about a single infection on a managed device.	A lot less information to base anomaly detection on. Almost impossible to make sure that all devices are covered. IoT devices are not covered. Focuses on individual devices instead of an entire network.

Muninn recommends a complementary approach to utilizing both technologies, whereby NDR is employed for anomaly detection throughout the network, and EDR is utilized for conducting comprehensive endpoint investigations. It is advisable to have specialized capabilities in-house to handle the EDR platform effectively.

2.2. NDR Capabilities

Depending on the specific NDR technology being used, it's findings can vary based on the focus it has. We will describe some of the most common examples in the following list:

Command and Control (C2 / C&C) Activity

Once a machine is infected with malware, it typically establishes communication with a command and control server to receive further instructions. Muninn AI Detect identifies this type of activity by scrutinizing connections for known IOCs (indicators of compromise) within the available Threat Intelligence. It also utilizes a sophisticated dyadic Machine Learning engine to determine if a connection deviates from the automatically established baseline, and therefore, is abnormal.

Lateral Movement and Execution

Once an attacker has gained access to your network, their next goal is to locate and obtain the appropriate credentials and access to sensitive information. This is accomplished by moving from one machine to another, a process commonly referred to as lateral movement. Muninn is capable of detecting this type of activity by examining standard attack indicators, such as files written to administrative shares and remote execution over WMI. Additionally, Muninn utilizes its AI to identify these types of attacks by monitoring activity that occurs outside of normal business hours or unusual interactions between machines that typically do not communicate with each other.

Ransomware

Muninn has the ability to identify ransomware that spreads throughout the internal network, infecting other devices. By utilizing both ML and AI, Muninn can detect anomalous activity within the network. This is achieved by analyzing interactions between devices that typically do not communicate using specific protocols and services.

Exfiltration of Data

No company today has only non-sensitive data, exemplified with GDPR. Exfiltration of data, caused by e.g. insider threats and espionage, is now more severe and costly than ever. In the case where an attacker has gained access to the network, they will try and gain as much value as possible from the hack. One of these actions is exfiltration of all kinds of data, which can be anything from customer information, HR data and confidential corporate documents. Using AI & Machine Learning, Muninn already has a baseline of how every single machine on the network normally behaves. So, if an employee starts to extract more data than is normally required by their job, Muninn will create a notification about this.

Today, every company and organization keep sensitive data to some kind of extend, hence why the European Union established GDPR regulations. The exfiltration of these data resulting from insider threats or espionage has become increasingly severe and expensive. If a hacker successfully breaches a network, they typically attempt to extract as much valuable information as possible. This includes customer information, HR data, and confidential corporate documents.

Muninn AI Detect establishes a baseline of normal behavior for every machine on the network. If an employee extracts more data than is necessary for their job, Muninn will notify and alert your cybersecurity team.

Malicious Insider Threats

The insider threat is notoriously challenging to detect, as perpetrators often carry out their nefarious activities while maintaining their usual work patterns. Nonetheless, Muninn is continually learning and adapting to the network, enabling it to identify even minor deviations from the norm. For instance, it can detect when an employee is active outside of their typical work hours or when a system administrator goes rogue.

2.3. NDR Areas

Network Detection and Response (NDR) has emerged as a crucial component of companies' cybersecurity strategy, as the insights it provides can be leveraged for security, compliance, and GDPR compliance purposes. NDR is particularly effective in mitigating the following risks:

- Data breaches
- Hacking
- Insider threats being malicious or unintentional
- Ransomware
- Bitcoin-mining
- llegal botnet activity
- Detection of anomalous network behavior e.g., unusual hours of communication, large file size transfers, changes of user privileges and others

3. Muninn Overview

Muninn AI Detect and AI Prevent have been developed to increase cybersecurity for organizations in many different areas and in scenarios. This section describes the most important and will describe some of the details regarding the machine learning engines

3.1. Feature Overview for Direct Customers

FEATURE	CHECK
Detect unknown threats and zero days in your network using advanced AI and Machine Learning.	✓
Full, in-depth interaction analysis using Machine Learning to reveal insider threats and espionage.	✓
Muninn AI Prevent isolates infected hosts immediately and in real-time.	✓
Full packet capture of Ethernet frames, protocol analysis, raw data analysis & forensics	✓
Monitor in cloud, on-premise devices or hybrid.	✓

Detect commodity threat using known blacklist and indicators of compromise (IOC).	✓
Detection of suspect behavioral traffic patterns.	✓
Full integration to SIEM / Log management tools, including generated network flows.	✓
Full-service solution possible including hardware and alert monitoring.	✓
Advanced searching capabilities which enable easy threat hunting.	✓

3.2. Feature Overview for Partners

Muninn AI Detect and AI Prevent have been developed with some distinct and unique features for partners, which are listed below.

FEATURE	DESCRIPTION	CHECK
Multi-tenancy for data centers, based on VLAN id and subnet grouping.	Muninn supports hosting providers, which segment customer by VLANs, by natively integrating this into all aspects of the user interface.	✓
Cloud based control system for easy monitoring of customer Muninn sensors, that are managed bypartners.	By design Muninn is built to support partners in Cloud based environments.	✓
Administration of user privileges for Muninn AI sensors.	Management is easily and quickly available for partners across their entire customer base.	✓

3.3. Compliance Feature Overview

Given the broad scope of cybersecurity, Muninn not only addresses immediate security concerns but also emphasizes critical compliance issues that can be effectively tackled with an NDR solution.

FEATURE	DESCRIPTION	CHECK
Get an overview of all network-based assets in the company	Using passive asset discovery, Muninn provides an overview of all devices connected to the network.	✓

Monitor Windows administrator login activity	Muninn monitors all network traffic in the network, this includes standard windows authentication protocols such as Kerberos and NTLM and will give notification based on anomalous connections.	✓
Verify software installation based on passive network monitoring	Muninn's comprehensive traffic monitoring and recording capabilities enable organizations to gain an overview of the software that traverses their network.	✓
Monitoring of common cloud filesharing services, including Dropbox, Google Drive, Azure & Office 365.	Muninn can detect connections to common file-sharing sites and issue notifications for any relevant sites.	✓
Monitoring of common configuration errors, such as external DNS and email servers.	Muninn will monitor for connections on common ports and services.	✓
Possibility for forensic analysis, discovery of real-time threats and related documentation according to requirements specific to CIS20/NIST/GDPR/CMMC and Danish Legislation on IT preparedness for the electricity and natural gas sectors (BEK 820).	Muninn will perform full packet capture and register and safeguard all traffic on the network. Muninn also has the capability to compile advanced reporting on specific events and timeframes.	✓

3.4. Detailed Feature Set

The table presented below provides a comprehensive list of Muninn's relevant features, which can be used for comparison with other security solutions, including NDR.

DETECTION

FEATURE	DESCRIPTION	CHECK
Supervised machine learning detections	See Machine Learning (ML) in-depth Section 3.5.1	✓
Unsupervised machine learning detections	See Machine Learning (ML) in-depth Section 3.5.1	✓
Track individual events/incidents, converting them into incidents with full PCAP ondemand for forensic investigation	Muninn keeps track of suspicious patterns, triggered by network events (IoCs, signatures, anomalies etc.), over time.	✓

Enterprise Application Protocols	Muninn supports OSI layer 1-7 and common enterprise protocols such as Kerberos, SMB and HTTP.	✓
Decryption	Muninn records a large amount of meta data for all connections, incl. details of SSL handshakes in encrypted connections. ** This meta data enables Muninn to also model anomalous behavior for these encrypted connections.*	✗
Behavioral Analytics (Data Science)	See Machine Learning (ML) in-depth Section 3.5.1	✓
Training Period (Data Science)	Muninn will start giving relevant notifications from day one, and the ML will continue to learn over the following weeks.	✓
Threat Intelligence Integration (Deployment & Extensibility)	Muninn has native integration of several threat intel feeds, which are automatically updated.	✓

INTERFACE

FEATURE	DESCRIPTION	CHECK
Critical Asset Prioritization	In Muninn you can raise the severity for specific devices in one or more notifications categories, thereby making sure that high risk or VIP users are always at the top of analysts' workflows.	✓
Forensics	See "Full Digital Forensics"	✓
User Experience & Workflows (Use Cases)	Muninn has been designed with a focus on security for both detection and response purposes, as well as with the proper workflow in mind for SOC analysts.	✓
Detect Known Attacker TTPs (Use Cases)	Muninn can detect attacks using various features, including Threat Intelligence (TI) and Machine Learning (ML). In case these features are not sufficient, SOC analysts can manually review metadata to search for new Tactics, Techniques, and Procedures (TTPs).	✓

Retrospective Detection (Use Cases)	Only manual investigation in metadata.	✓
Query Language & Threat Hunting (Use Cases)	Based on Muninn's meta data store, and custom query language it is possible for further analysis of data and finding new threats if you have the right skillset. The team behind Muninn continuously improve the detection of the system, which means you don't have to do deep threat hunts.	✓
Free Text Search (Use Cases)	By using Muninn's built-in search feature, it is possible to quickly and easily search through all the relevant data, without any limitations.	✓
Full Digital Forensics (Use Cases)	Since Muninn stores all raw and meta data, it is possible to perform full digital network forensics in the system.	✓
Traffic statistics	Muninn will report on network traffic statistics, based on all the collected meta data.	✓
Reporting and email notifications	Muninn supports sending email on high notifications, and will provide detailed reports on network usage, such as DNS requests.	✓

BACKEND

FEATURE	DESCRIPTION	CHECK
Integrates with firewall, NAC, endpoint, SIEM and SOAR products to streamline incident response	See "Integrations with other Security Tools"	✓
Cloud Integrations	Supports common cloud services such Azure and Amazon AWS.	✓
Integrations with other Security Tools (Deployment & Extensibility)	Muninn is native built upon a rest API, which means you can easily integrate to other in-house system and tools. Muninn already has native integration with IBM QRadar and other SIEM systems, using syslog and flow forwarding.	✓

OTHER

FEATURE	DESCRIPTION	CHECK
Delivers a complete solution for network detection and response	Muninn delivers an all in one solution for your current cybersecurity needs, without the use of other external tools. Muninn AI Prevent prevents threats in real-time and can be used independently without integrations, using TCP reset to effectively block devices generating malicious traffic. It can also be integrated to external 3rd party systems.	✓
Throughput	Muninn supports networks from 100mbit/s till 40Gb/s.	✓
Organizational Data Privacy (Data)	Muninn will help companies to manage privacy related items, including GDPR*. All customer data including ML data is only saved on the sensor.	✓
Expertise & Security DNA (Corporate Background)	Muninn's sole focus is on cybersecurity, which means that the tool is designed to specifically address the security challenges that companies face on a daily basis, not only in terms of detection but also in terms of workflow.	✓

*) *To learn more about how Muninn can support you with GDPR, please contact us and read our GDPR brochure.*

3.5. Unique Features

When compared to other products, whether they're NDR solutions or something else, Muninn stands out thanks to its unique features:

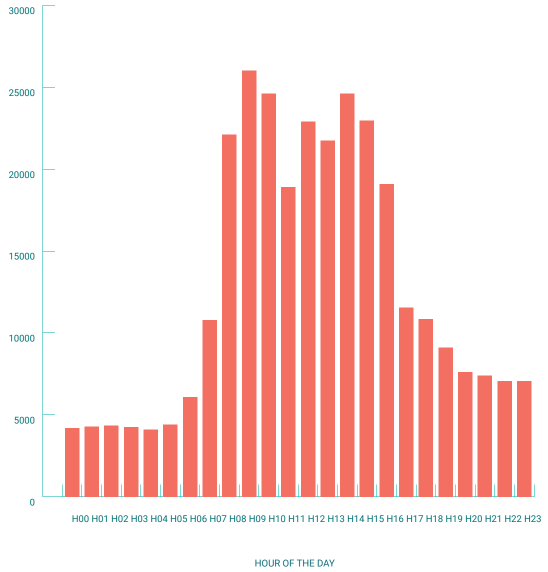
- **Advanced machine learning reducing the amount of false positives.**
- **Ability to identify out of hours anomalies.**
- **Easy set up of Muninn Central where all alerts and notifications of all sub-networks can be monitored.**
- **Deep inspection of traffic from unmanaged devices IoT**
- **Full packet capture**
- **Multi-tenant (where a managed hosted service provider partner can host multiple customers on one box)**

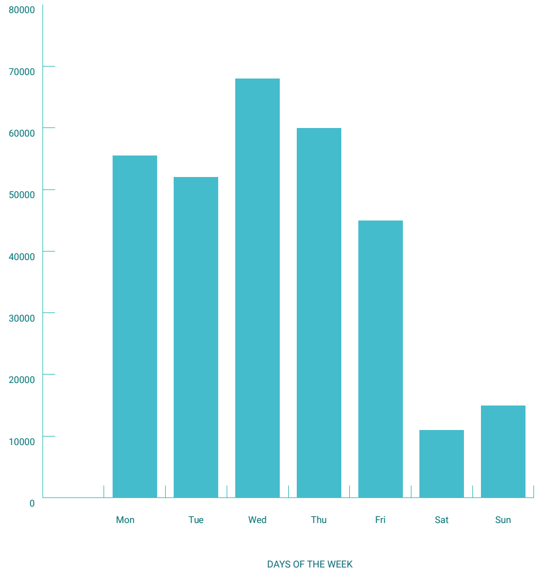
3.6. Machine Learning (ML) in-depth

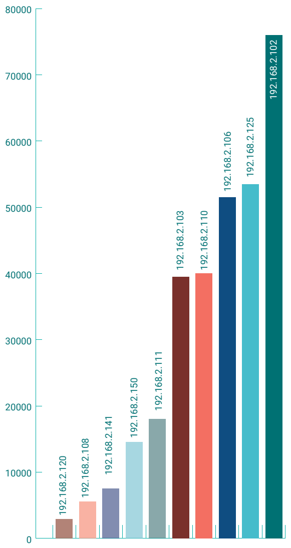
Muninn's embedded machine learning engine is a unique and crucial feature that employs two distinct ML engines to detect network anomalies. The first engine, ML1, utilizes probabilistic clustering to automatically determine normal data transfer volumes in the monitored network. With its probabilistic nature, Muninn can precisely describe the probability of data sent or received within a given time window. Whenever a host transmits or receives more data than the network's normal volume, Muninn generates a notification categorized as a Point Anomaly, specifying the event's unlikelihood.

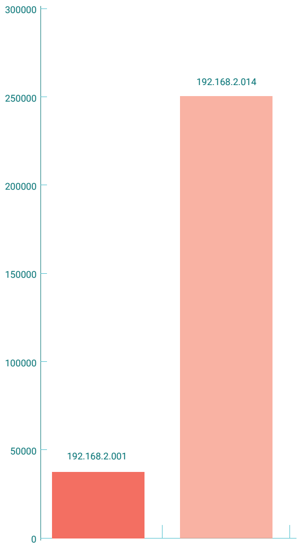
Muninn's AI also includes a Dyadic ML Engine (ML2), which introduces a novel approach to data representation and processing by emphasizing the importance of interactions. The engine is named after the concept of dyadic data, which refers to the context of two specific machines communicating under specific circumstances. In contrast to ML1, which treats data as monadic, ML2 recognizes that interactions in a network are inextricably linked to the context in which they occur.

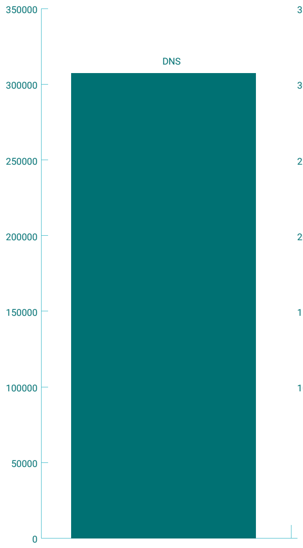
The Muninn Dyadic engine takes a unique approach to analyzing network traffic by representing it as counts of interactions in an 8-dimensional tensor with 10^{20} possible communication circumstances between machines. With a specially optimized algorithm, this tensor is factorized into traffic patterns that accurately depict all types of network interactions. The algorithm considers various contextual factors, such as the time and day of the interaction, the port and protocol used, and the amount of data sent and received.

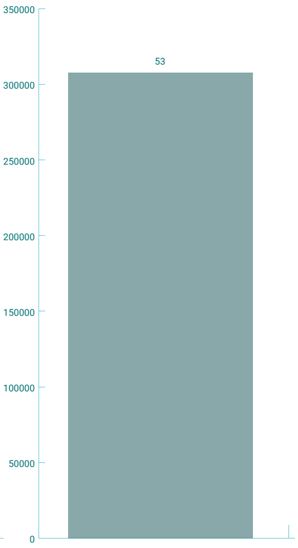












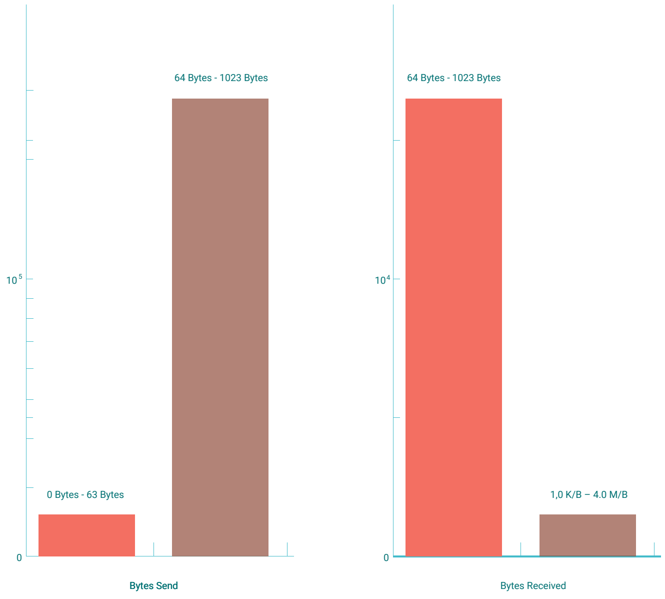


Figure 1 Example of a traffic pattern describing DNS traffic in a typical office

The traffic patterns produced by Muninn's machine learning engine can provide a remarkably detailed and precise description of network activity. This analysis is performed entirely on the Muninn specific sensor, with no data being transmitted to the cloud. Advanced mathematical software and carefully constructed code allow for high speed and memory efficiency.

The Dyadic ML Engine employs the traffic patterns to achieve a straightforward yet ambitious objective: scrutinizing each network interaction to identify whether it's normal and in real-time. Additionally, Muninn uses the traffic patterns to ascertain which hosts display comparable behavior and applies that knowledge to allow interactions that may not be typically normal for a single host but are typical for hosts of similar nature. This strategy significantly reduces false positives, particularly for new users and devices on the network

Example: *For instance, a new HR employee joins the company and starts accessing various HR-related services. Within a short period, Muninn associates this employee with some of the traffic patterns of the HR team but not all of them. Based on the assigned traffic patterns, Muninn concludes that the employee is similar to other HR team members and permits the employee to engage in behavior similar to that of other HR employees, thereby reducing false positives.*

The Dyadic ML Engine places significant emphasis on reducing False Positives (FP), and Muninn employs various strategies to achieve this goal. Our first step is to ensure that only high-quality data is used for modeling by thoroughly vetting all traffic based on extensive domain knowledge. Additionally, we carefully tune the granularity and resolution of the extracted traffic patterns to balance generalization with nuance, ensuring that new behaviors are recognized while avoiding overgeneralization that would result in lost information. An apt analogy is compressing a grainy image. Compress the original enough and the graininess will smooth out and the image becomes clearer but compress too much and the image becomes an unfocused blob.

Finally, we leverage host-to-host similarity derived from traffic pattern memberships to enhance our ability to identify expected behavior.

4. Deployment

Muninn supports different types of deployment, for different scenarios and companies.

- On Premise sensor which can be either physical or virtual or a mix of both.
- Cloud service installations, currently Amazon and Azure.
- Multi-tenant for hosting partners, which segments their userbase based on VLAN id.
- Scalability: customer installations ranging from one sensor, and no upper limit for large enterprises.

5. 3rd Party Product Integrations

Muninn understands and wants to support the current cybersecurity product landscape, by providing an open platform which customers can easily adapt to their needs.

Muninn AI Prevent works and blocks independently, but also integrates with the following systems:

- SIEM / SOAR systems such as IBM QRadar (Forwarding notification information using syslog and flow data in the LEAF format)
- Muninn AI Prevent: o TCP reset (independent from any integrations) o Software Defined Networks (SDN) using OpenFlow 1.3 and up o Other REST based SDN controllers
- Ubiquiti Unifi series controller (block a device from accessing the network)

Muninn is an agile company and we design our products in a modular way, which enables us to quickly create new integrations for any relevant 3rd party system integration which currently isn't natively supported by Muninn.

6. Muninn Sensor Internal Security

For the customer, Muninn AI Detect and AI Prevent are an appliance black box. All security updates, hardening, health monitoring etc. are handled by Muninn. Some hardening measures taken are:

- **The only allowed traffic to sensor, is to TCP port 443.**
- **All communication to and from the cloud platform is protected with username/password, and certificates.**
- **Coding is done according to best practice.**

Muninn is solely responsible for monitoring the network traffic and detecting anomalies. However, it is important to note that the customer or partner is responsible for monitoring the sensor for potential attacks. This is in line with industry standards and best practices for any security solution. It is expected that the customer or partner will actively monitor the sensor, not only through Muninn notifications but also through other relevant security products installed in their infrastructure.

6.1. Communication and Data Flow

This section briefly describes the dataflow between Muninn and the cloud system, including which types of data are being sent.

Muninn is monitoring all installations from an operational and performance perspective through its Muninn sensor and service. To achieve this, the sensor sends certain data to our cloud services, which are hosted on Amazon within the EU.

Monitoring data sent to the cloud:

- CPU usage
- Memory usage
- Disk usage
- Network statistics

Besides the above data, the sensor also sends information about notifications created. However, by default, no metadata or raw data is included in the transmission.

Notification data includes:

Monitoring data sent to the cloud:

- Timestamp
- Source and destination IP-address
- Category
- Description
- Severity
- Score

A. Appendix A - NDR Compared to Other Solutions

This appendix compares NDR to other commonly used IT security technologies. It is worth noting that it is not a matter of choosing between these solutions and NDR, as each has its own advantages and disadvantages.

A.1. Antivirus

Antivirus is widely used as a protection mechanism in companies organizations, although it does not provide comprehensive coverage, it does offer a basic level of protection. Here are some common characteristics:

- **Limited to protection of managed endpoints and does not cover IoT devices nor the full scope of the network.**
- **Dependence on the operating system**
- **Cannot capture raw data.**
- **Protection is only at the application level.**
- **Limited threat detection as it is based on known threats such as signatures and blacklists.**
- **Monitors physical media such as CDs and USBs inserted into the computer.**

GENERAL FEATURES	ANTIVIRUS	NDR e.g. Muninn
Management Dashboard	Yes	Yes
Scope	Clients only	Full
Inventory	No	All devices within the network, including detection of new devices which were not previously known
Client Requirements	Some requirements in form of CPU and memory usage. Operating system needs to be supported.	Full
Deployment	Days	Hours
Network Usage Statistics	No	Yes
Log Concentrator	No	No
Software Updates	Frequently	Frequently
Availability	N/A	24/7
Maintenance Costs	Medium	Low
Implementation Costs	Medium	Medium
Raw Traffic Capture for Forensics and GDPR compliance	No	Yes
SIEM feeder of notifications, alerts, flows	Yes	Yes
DNS Protection	Depending on product	Yes

THREAT DETECTION	ANTIVIRUS	NDR e.g. Muninn
Protocol Behavior Analyzer	No	Yes
Traffic Signatures	Yes	Yes
Blacklists	Yes	Yes
Based on ML	No/Limited	Yes
Log Analysis	No	Yes
Sending notifications to syslog server in LEEF format	Depending on productv	Yes

PROTECTION	ANTIVIRUS	NDR e.g. Muninn
Packet Filter	No	N/A
DoS filter	No	N/A
Application filter	Yes	Yes

A.2. Firewall

Companies and organizations commonly use firewalls as network protection mechanisms, which offer a good basic level of protection despite not being comprehensive. It monitors and controls incoming and outgoing network traffic based on predetermined security rules and acts as a barrier between a trusted internal network and an untrusted external network, such as the internet. However, unlike firewalls, Muninn is a dedicated sensor that boasts significant processing power and is capable of processing raw packet network traffic in real-time and leveraging artificial intelligence to identify potential threats that already past the firewall and anti-virus software.

Muninn, unlike firewalls that analyze traffic and discard the information immediately after, is a state-of-the-art system that can analyze network traffic patterns over an extended period. This unique feature enables Muninn to identify and prevent security breaches more effectively.

Next-generation firewalls (NGFW) are primarily designed to protect the network perimeter against external attacks, while Muninn acts as a network sensor that monitors and analyzes all network traffic, including internal traffic between devices. Therefore, these products complement each other and serve different purposes.

By leveraging artificial intelligence, Muninn drastically reduces false positives as compared to relying solely on lengthy signature lists. This feature saves user time by reducing the need for reviewing and analyzing alerts.

Moreover, Muninn is designed to be a plug-and-play system that requires minimal configuration before it can start functioning. Its built-in machine learning and AI algorithms understand normal network behavior, enabling it to quickly detect any abnormal activity. In contrast, setting up and maintaining a next-generation firewall can be time-consuming. With Muninn, users can swiftly gain an overview of their network’s security status immediately after installation.

To achieve best-in-class IT security, a network sensor like Muninn is critical as it provides extensive coverage of all network activities. Muninn is tailored to protect companies from industrial espionage and data breaches by utilizing artificial intelligence to detect and mitigate potential threats efficiently after they pasted the standard network protection mechanisms.

GENERAL FEATURES	NETWORK FIREWALL	NDR e.g. Muninn
Management Dashboard	Yes	Yes
Network Scope	FULL at perimeter	Full
Inventory Overview	No	All devices within the network, including detection of new devices which were not previously known
Client Requirements	No	No
Network Usage Statistics	Limited to Perimeter	Yes
Log Concentrator	No	No
Software Updates	Rarely	Frequently
Availability	24/7	24/7
Maintenance Costs	Low	Low
Implementation Costs	Low	Medium
Raw Traffic Capture	No	Yes
SIEM feeder of notifications, alerts, flows	Yes	Yes
DNS Protection	No	Yes

THREAT DETECTION	NETWORK FIREWALL	NDR e.g. Muninn
Protocol Behavior Analyzer	No	Yes
Traffic Signatures	No	Yes
Blacklists	No	Yes
Based on ML	No	Yes
Log Analysis	No	Yes

PROTECTION	NETWORK FIREWALL	NDR e.g. Muninn
Packet Filter	Yes	N/A
DoS filter	Yes	N/A
Application filter	No	Yes

A.3. DNS protection devices

Due to the prevalence of malware using DNS to communicate with their command and control servers, having a dedicated DNS protection service to filter potential malicious DNS requests has become increasingly common.

Here are some characteristics of DNS protection devices:

- **Relying solely on the DNS protocol**
- **Based only on blacklists, contrary to behavioral intelligence**
- **Protection limited to the DNS queries**
- **No package capture (analysis and forensics)**
- **DNS protection benefits from filtering of DNS queries**

GENERAL FEATURES	DNS PROTECTION SERVICE	NDR e.g. Muninn
Management Dashboard	Yes	Yes
Scope	Full DNS	Full Network Traffic
Inventory	No	All devices within the network, including detection of new devices which were not previously known
Client Requirements	Depends on Solution	None
Deployment	1 Hour	1 Hour
Network Usage Statistics	Limited	Yes
Log Concentrator	No	No
Software Updates	Frequently	Frequently
Availability	24/7	24/7
Maintenance Costs	Low	Low
Implementation Costs	Low	Medium
Raw Traffic Capture	No	Yes
SIEM feeder of notifications, alerts, flows	Limited	Yes
DNS Protection	Yes	Yes

THREAT DETECTION	DNS PROTECTION SERVICE	NDR e.g. Muninn
Protocol Behavior Analyzer	No	Yes
Traffic Signatures	No	Yes

Traffic Signatures	No	Yes
Blacklists	Yes	Yes
Based on ML	No	Yes
Log Analysis	No	Yes

PROTECTION	NETWORK FIREWALL	NDR e.g. Muninn
Packet Filter	No	N/A
DoS filter	No	N/A
Application filter	No	Yes
Threat Auto filter	No	Yes

A.4. SIEM

SIEM, and consequently central logging, are integral components of advanced protection strategies. However, to reap the full benefits of these systems, significant manual effort is required, as elaborated below.

Muninn enables real-time automated threat detection and monitoring, unlike a typical SIEM that consists of searchable logs from the past. By scanning all network traffic and utilizing advanced machine learning, Muninn can detect anomalies effectively. Additionally, Muninn's protocol analysis extracts up to 300 types of meta data from network traffic.

Muninn is a plug-and-play solution that requires minimal configuration, unlike SIEM, which requires creating and identifying rules from the beginning. With Muninn, users are constantly updated with the current threat picture, which is continually evolving.

It is possible to integrate Muninn with an existing SIEM solution, enabling correlation of notifications and alerts across different technology stacks.

GENERAL FEATURES	SIEM	NDR e.g. Muninn
Management Dashboard	Yes	Yes
Scope	Full	Full
Inventory	Yes	All devices within the network, including detection of new devices which were not previously known
Client Requirements	Yes	None
Deployment	Weeks	Hours
Network Usage Statistics	Depends on Solution	Yes

Log Concentrator	Yes	No
Software Updates	Rarely	Frequently
Availability	24/7	24/7
Maintenance Costs	High	Low
Implementation Costs	High	Medium
Raw Traffic Capture	No	Yes
SIEM Feeder	N/A	Yes
DNS Protection	Yes	Yes

THREAT DETECTION	**SIEM**	**NDR e.g. Muninn**
Protocol Behavior Analyzer	No	Yes
Traffic Signatures	No	Yes
Blacklists	Yes	Yes
Based on ML	No	Yes
Log Analysis	Yes	Yes

PROTECTION	**NETWORK FIREWALL**	**NDR e.g. Muninn**
Packet Filter	Yes	N/A
Application filter	No	Yes

Muninn

About us

Founded in 2016 by engineers and computer scientists from the prestigious Massachusetts Institute of Technology (M.I.T), Muninn has been changing the way companies approach cybersecurity.

With our advanced AI technology and reliable security solutions, Muninn AI Detect and AI Prevent empower organizations to protect their critical digital assets and infrastructures from cybercriminals.

Located in the heart of Denmark, Copenhagen, our team is comprised of inspiring colleagues with multiple nationalities and backgrounds. Each commitment to professional development and growth ensures that Muninn will continue to be a game-changer in the field of cybersecurity.

www.muninn.ai

info@muninn.ai

+45 70 60 59 08