Endpoint Agent

Contact us

Your Key Benefits

- Full coverage on-site, remote, on or off VPN
- Detailed information about endpoint activity
- Lightweight application
- Detects known and unknown threats in the earliest stage
- Self-learning AI

Detected Network Breaches Include

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

Full Movability, Full Network Security

The last years have profoundly changed our way of working and there is an increasing number of endpoints within organizations, extending beyond the conventional landscape of end-user computing devices like laptops and workstations. The rise in remote work culture has significantly amplified the demand to safeguard and supervise a wide range of endpoints, as well as the interactions among them. Given that these endpoints are prominent gateways for cyberthreats, your Network Detection and Response should move with your employee's devices.

Bring Muninn Everywhere You Go

As employees move away from traditional corporate workplaces, VPNs are not always enough to keep the network and devices safe.

With our Endpoint Agent you can bring Muninn's AI to wherever you go. Protect employees and your organization everywhere, whether they are in the office, working remotely, on or off a VPN.

Efficiency With a Lightweight Application

Muninn transmits all endpoint activities in the form of raw data packages, enhancing the system's visibility into detailed information and possible cyberthreats. This operation runs seamlessly in the background, ensuring no disruption or degradation to your network's performance.

Endpoint activities are analyzed and investigated in real time and against the entire digital enterprise for better context. Muninn will use this information to instantly determine the appropriate response to identified threats.