cryptomage®

Cryptomage Cyber Eye™

Network Detection and Response
All-seeing, full-network protection

cryptomage®

THE DIGITAL THREAT: rapidly growing, ever-evolving cyber-attacks

Just as the digital age is providing new ways for organizations to engage with the market, so too has it created opportunities for more technically sophisticated cyber-attacks. The connected, knowledge-sharing nature of digital business adds layers of structural and operational complexity that make it harder to predict and deal with any threat that may occur. Security events tend to be both frequent and sophisticated. Increasingly, we are dealing with non-signature attacks, which pose the greatest challenge for security teams.

As a result, organizations need quick protection and remediation, preferably automated, with artificial intelligence and machine learning to adapt to their business-specific needs. Only this way can they stay ahead of the threat.

THE DIGITAL ANSWER: Cryptomage's network-based Cyber Eye™ solution

Cryptomage Cyber Eye™ detects anomalies and security incidents based on the analysis of network traffic and protocols. The probe analyzes network traffic in real-time on a copy of the traffic.
It provides security teams with a high level of protection against cyberattacks, and offers the possibility of integration with SIEM, SOAR and NGFW systems.
With Cryptomage Cyber Eye™ organizations can identify, monitor, and investigate malicious events and connections - the probe is the perfect complement to automated safety systems.

All attack-ready

Cryptomage Cyber Eye can detect and predict network-based threats, such as:

- attacks on infrastructure at an early stage
- malware attacks
- indication of 0-day attacks being carried out
- suspicious network traffic
- unauthorized modification of network protocols in devices
- unauthorized connection of network devices
- personal data leaks

Sector-specific security

Cryptomage Cyber Eye is designed to meet the business challenges in a wide range of industries:

- financial services (banking, insurance)
- telecommunications (operators, providers)
- utilities (including critical infrastructure)
- government
- military & uniformed services
- manufacturing & industry 4.0
- healthcare & pharmaceutical

FEATURES: business value for your organization

Cryptomage Cyber Eye™ is a business protection approach, specifically designed to support business competitiveness and advantage, for managers, employees, and administrators alike. This is because it enables organizations to operate with greater certainty and security in a digital environment, from a number of perspectives:

Threat detection provides deep inspection of every single network packet including transported data with:

- *Network protocol discovery and validation* – easily check unknown and hidden protocols
- *Machine Learning algorithms* – proactive traffic risk-scoring

Personal data leakage detection, GDPR compliance module

- *Inspection of the network packets in order to detect transmission of personal data such as ID numbers, social security numbers, bank account numbers*
- *Generating reports for Data Protection Officers*

Network monitoring with proprietary flow metadata formats that go beyond traditional network flow analysis

- *Protocol behavior and anomaly statistics* – wider understanding of traffic flow and behavior
- *Passive mode option* – operations don't interfere directly network traffic

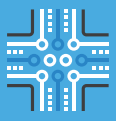
Event management with full SIEM, SOAR and NGFW integration and export thresholds

- *Risk scoring of each event and host* – effective triaging of threats
- *Built-in analytic tools and charts* – inform and guide ongoing event management
- *Configurable event triggers* – giving you control over certain packets or events when needed

Forensics to better measure the ratio of security events against source of traffic

- *Extraction of high-risk network traffic* – easy to analyze and focus on specific threat levels
- *Storage of processed traffic metadata in extended format* – faster trend analysis

Configuration of traffic rules to focus on high-risk subnetwork traffic



- *Separate configuration for each subnetwork* – keep key areas of threat in focus
- *Manual edit of high-risk hosts* – define specific requirements for specific areas of risk

Administration that responds quickly and logical to issues

- *Web administration interface* – flexible, anytime-anywhere, easy-to-use
- *User management and accountability* – creating dedicated user accounts and monitoring account usage

Cryptomage Cyber Eye™ and Gartner's SOC Visibility Triad

The Gartner's SOC Visibility Triad increases the visibility of every aspect of the network environment and consists of three main pillars that allow a comprehensive look at the organization's cybersecurity:

- SIEM or UEBA – gives a unified view of the organization's IT infrastructure security
- EDR – provides endpoint detection and response.
- NDR or Cryptomage Cyber Eye™ adds a network perspective and thus completes the SOC Visibility Triad.

DIFFERENCE: Cryptomage Cyber Eye™ provides network security like no other

Cryptomage Cyber Eye™ offers a unique approach to network traffic analysis, with a combination of protocol behavior, packet analysis, and host communications behavior analysis powered by AI and ML. While the majority of security solutions focus only on user and host behavior, Cryptomage Cyber Eye™ also incorporates unusual low-level network behavior.

The Cryptomage Cyber Eye ™ is integrated with Recorded Future's platform. All metadata in our probe are enriched with the information provided by Recorded Future, which enables even more accurate detection of security events, more effective validation and analysis of detected events and false-positive reduction.

While Cryptomage Cyber Eye™ is always evolving, armed with AI and machine learning capabilities, it is also designed to integrate and interact with other security solutions to increase threat detection. This means you can combine our unique network analysis capabilities with other security tools to achieve even greater levels of threat detection.

Integrated with:

Recorded Future®

TECHNOLOGY: the key components of our security solution

Cryptomage Cyber Eye™ is custom network equipment comprising proprietary artificial intelligence and machine learning algorithms, analyzing your network traffic in real time.

The solution can be deployed with sensor parameter configuration, algorithm block addition, and incident prioritization:

Cryptomage Cyber Eye™ works out of the box and does not require time-consuming configuration to be fully functional.
Detected anomalies and security incidents are available in the management panel and provided to other devices for further analysis by security teams.

Parameter	Cryptomage Cyber Eye
Maximum throughput	1 Gbps - 5 Gbps
Maximum monitored hosts	5 000 - 50 000
Maximum sessions	50 000 - 300 000
Network interfaces	2x GbE, optionally 2x QSFP
Management interface	RJ-45
PCAP Storage	4 TB SATA
Maximum power consumption	600W
Weight	26.5 lbs (12.0 kg)
Dimensions	1U
Operating temperature	50-95 °F (10-35 °C)

GET IN TOUCH

If you would like to get new levels of business network security with improved ROI, get in touch with us now, by email (info@cryptomage.com) or phone (+48 71 757 55 69). Alternatively, just visit our website at www.cryptomage.com.

ABOUT US

Cryptomage LLC is a dynamic hi-tech ICT company offering hardware and software solutions and services in the cybersecurity domain across North America and Europe.

We provide cybersecurity advisory services and solutions to blue-chip IT integrators and government agencies. These are delivered by our team of cybersecurity experts, professor-level scientists, hardware engineers, software developers and analysts.

cryptomage®