



## YOU ARE A TARGET

People, organisations and governments see an increasing threat from cyber-attacks every year. Organisations are recognising that it is no longer a question of whether a cyber-attack will be successful, but when. In fact, many organisations may already be breached and not know it.

Without a sophisticated method for detecting and responding to advanced attacks, businesses will stay unknowingly infected and the criminals will continue to operate under the radar. Undetected attacks can lead to business disruption, information theft and reputation loss.

### HOW YOU ARE TARGETED

Your business depends on IT services and the Internet. The legitimate use of the web, email and apps are all necessary parts of modern business and critical to day-to-day operations.

Using these services increases your threat exposure. Throughout their normal daily tasks, your users will be exposed to threats that may install malicious code on a company computer that not only disrupts normal workflow, but also connects your company to a botnet infrastructure operated by criminals. Aside from the cost of remediating this malware, businesses and their customers are exposed to data breaches and service disruption.

We experience that cyber-attacks change constantly. The targets change and methods evolve, improving their efficiency and impact. Businesses must keep pace with cyber criminals to protect themselves and stay secure – managing IT security in this landscape is becoming increasingly difficult.

### HOW ARGUS MANAGED DEFENCE CAN HELP

We are proud of being in the forefront of detecting, responding to, and preventing cyber threats. Through monitoring activity, collecting data and producing intelligence on the known and unknown, we discover the attacks and defend our customers against the attackers. Our aim is to neutralise the risk and protect your assets so that you can carry on with your business.

Argus Managed Defence provides our customers with protection against known and unknown threats 24/7/365 and we deliver alerts and incident reports that are factual, correct and actionable, based on the customers' business processes and risks.

Our threat intelligence network keeps us continuously updated, and in case of an incident you will expand your security staff with close to 100 highly trained experts. We have helped our customers respond to incidents for more than a decade, and are uniquely qualified to provide on-site assistance to stop, remediate and investigate cyber-attacks.

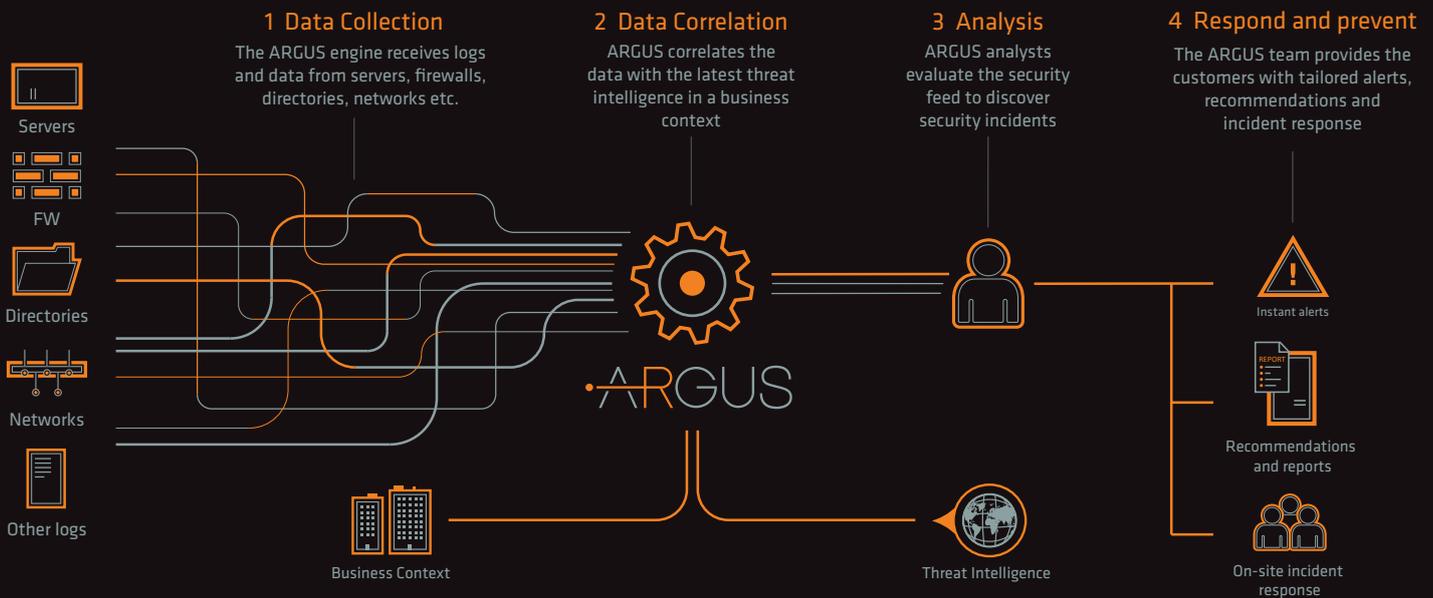
The Argus Managed Defence team works closely with our customers in their daily business.

*Our goal is to keep your business  
and information safe.*

We **detect** and intercept threats.

We **respond** and intervene when incidents occur.

We **prevent** threats from causing serious impact.



**CONTACT US:**

**Erik Wold**  
Sales

+47 994 91 879  
erikw@mnemonic.no

**THE BENEFITS**

**24/7 Attack Detection**

Our analysts use specialised solutions to discover attacks against your IT infrastructure. We watch the stream of traffic going in and out of your organisation 24/7. As we find threats, our analysts customise alerts to tell you what is happening, what the consequence is to your business, and what you should do about it.

**Applied Threat Intelligence**

Our intelligence network observes billions of online events every day. We detect anomalies, analyse suspicious files, examine Internet hosts and investigate hacker groups. We feed all our information through our Threat Intelligence systems to identify patterns of misuse, discover new threats and gain new insights into cybercrime. We correlate all patterns and events from your systems with our database to discover potential attacks.

**Business Integration**

Every business is different, and the risk scenario varies from organisation to organisation. We analyse your business and tailor a service policy that fits you. As we learn about your processes and setup, we shape our incident response to fit with your organisation. We fine-tune the solution to emphasise alerts where the target asset is vulnerable, and to ignore events that do not represent a threat to you. Information and alert overload is in itself a threat, and we make sure you only receive relevant information.

**Best of Breed Technologies**

Our goal is to detect every single security threat, using a range of tools to meet the exact requirements of our customers. Partnering with recognised industry leaders we can offer advanced malware detection, SSL inspection, intrusion detection or prevention, log analysis, data leakage prevention, anomaly detection and more cutting edge detection technologies such as use of passive DNS, flow analysis and reputation based detection.

**Argus Managed Defence Sensor**

Our appliance Argus Managed Defence Sensor provides a small footprint solution (1U) that is installed in a matter of hours, providing a full suite of tools to quickly implement a high quality security monitoring solution. Built to be flexible, the sensor provides intrusion detection, log analysis and supplementary tools. Supporting logs from any security device you already have, it correlates this log data with network traffic and our own threat intelligence.

**Incident Response Team**

Our Incident Response Team is called on several times each year to provide our customers with on-site assistance. From incidents involving smaller malware infections or data recovery, to engagements with advanced and persistent attackers that last for months, the mnemonic IRT is trained to respond correctly and timely.

**Compliance**

We support your compliance initiative. Regardless of whether the requirement is regulatory, based on a standard or from an internal policy, we will help you deliver exactly what you require.