PRODUCT SHEET

Managed Security

Unified Enterprise Security

Advanced Managed Cyber Security Powered by Patented Technology

Masergy's patented technology and continuous expert monitoring protects global enterprises from advanced cyber threats. Our Unified Enterprise Security (UES) technology leverages sophisticated machine learning and big data analytics. UES can be deployed standalone, or integrated with existing security systems, to deliver continuous prediction, protection, and detection of advanced cyber threats.

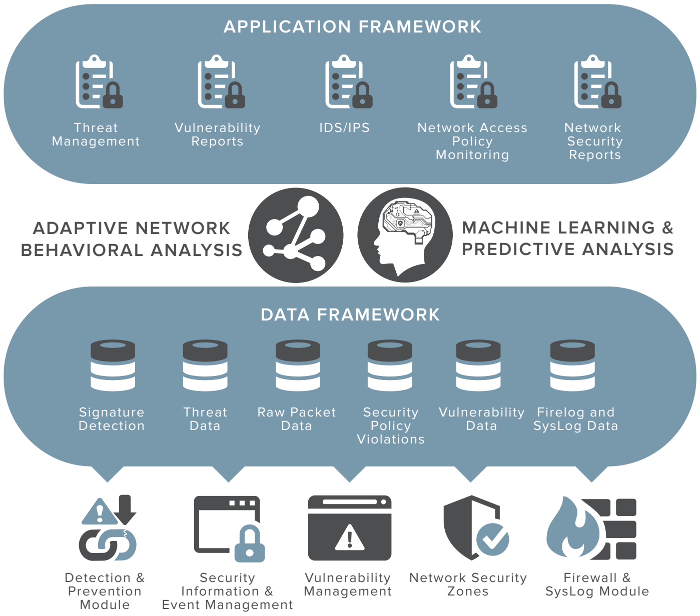
Discrete Point Solutions Alone are Not Enough

Advanced threats from criminal and state-sponsored hackers are increasing in frequency and severity. All corporate networks are targets. Enterprises have invested in discrete point solutions such as firewalls, IDS/IPS systems, SIEMs, and sandboxes for years. Unfortunately, hackers are skilled at avoiding detection. Even when a discrete point solution detects a threat, it is often overlooked due to the sheer volume of alerts being generated.

Superior Prediction, Protection, and Detection

Masergy's UES patented technology continuously and automatically learns the unique normal behaviors of each client network. By comparing actual behavior to predicted behavior, we detect even the most subtle anomalies. Our team of security experts continuously monitor and investigate all suspicious behaviors and threat alerts. When a threat is confirmed, we block the malicious traffic and initiate an incident response with actionable remediation steps.

Masergy UES Technology Architecture



MASERGY
Performance Beyond Expectations

FEATURES

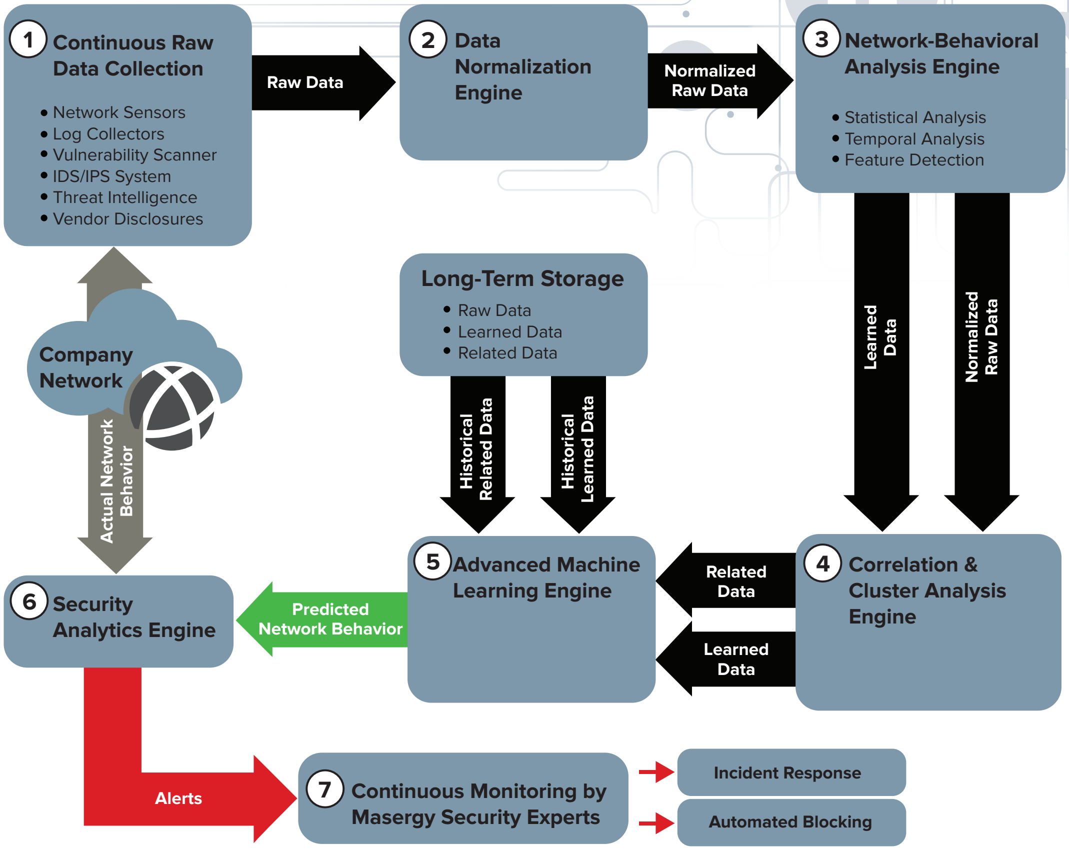
- Designed for premise, cloud, and hybrid networks
- Integrated architecture with sharing of data between subsystems
- Patented network behavioral analysis and correlation
- Automated correlation between vulnerability scanner and IDS/IPS subsystems
- Technology delivered as a 24/7 managed security service

BENEFITS

- Access to real-time, actionable root-cause information to prevent sophisticated threats both outside and inside an organization
- Works with existing security investments; no additional equipment or host agent software required
- Customizable security alert response procedures
- Unified administration, monitoring and reporting on any Internet-enabled device
- Supports all industry-standard regulatory compliance standards (e.g. HIPAA, PCI, SOX)
- Continuous monitoring, ticketing and reporting by certified security analysts 24/7

Learn how UES works on page 2

UES - How It Works



1 Continuous Raw Data Collection
- Network Sensors
- Log Collectors
- Vulnerability Scanner
- IDS/IPS System
- Threat Intelligence
- Vendor Disclosures

Raw Data

2 Data Normalization Engine

Normalized Raw Data

3 Network-Behavioral Analysis Engine
- Statistical Analysis
- Temporal Analysis
- Feature Detection

Learned Data

Normalized Raw Data

Long-Term Storage
- Raw Data
- Learned Data
- Related Data

Historical Related Data

Historical Learned Data

Company Network

Actual Network Behavior

4 Correlation & Cluster Analysis Engine

Related Data

Learned Data

5 Advanced Machine Learning Engine

Predicted Network Behavior

6 Security Analytics Engine

Alerts

7 Continuous Monitoring by Masergy Security Experts

Incident Response

Automated Blocking

1. Our fully integrated system includes all required subsystems that collect and generate vast amounts of raw data.
   - Network Sensors capture and forward 100% of all raw packet data for both North-South and East-West traffic.
   - Log Collectors gather logs for all log-producing devices including firewalls, routers, switches, servers, and applications.
   - The integrated vulnerability scanner identifies all known vulnerabilities.
   - The integrated IDS/IPS system automatically aligns signatures with vulnerability scan results and global threat intelligence, and generates signature-based alerts.
   - Threat intelligence from internal threat intel teams and the community are aggregated into the system.
   - Vendor disclosures on vulnerabilities are incorporated into the system.
2. All Raw Data is processed through the Data Normalization Engine to convert all raw data into a common consumable format.
3. Normalized Raw Data is processed by the Adaptive Network Behavioral Analysis Engine where a series of multi-dimensional analyses are performed to generate Learned Data.
4. Learned Data and Normalized Raw Data are processed by the Correlation Engine which conducts a series of cluster analyses to generate Related Data.
5. Both current and historical Learned Data and Related Data sets are processed by the Advanced Machine Learning Engine to generate a current prediction of normal network behavior.
6. The Security Analytics Engine compares the current prediction of normal network behavior to actual network behavior, identifying and alerting on subtle anomalies and suspicious traffic.
7. Our security experts analyze and dissect every alert.
   - If an alert is determined to be a false positive, we apply customized learning sets that accelerate the machine learning to avoid future false positives.
   - If an alert is determined to be a threat, we initiate incident response with detailed actionable remediation steps, and automatically block traffic to stop the attack in its tracks.

Rev. 102915

MASERGY
Performance Beyond Expectations

www.masergy.com US +1 (866) MASERGY (627-3749)
EMEA +44 (0) 207 173 6900