secureCENTRX

mBRANE

Security Operations Center

Unifying Security Dimensions in the Information Space

SOC+XDR+NDR+SIEM

Introducing mBRANE, a cutting-edge cybersecurity solution designed to safeguard your organization's digital assets with unparalleled efficiency and precision. Drawing inspiration from the protective qualities of a membrane, mBRANE encompasses all aspects of network traffic, ensuring comprehensive protection in every direction. Our innovative service diligently monitors north-south and east-west traffic, forming a robust shield that defends against even the most sophisticated cyber threats.

At the core of mBRANE's effectiveness lies our advanced artificial intelligence technology, complemented by a team of highly trained human analysts. Working collaboratively, our AI and expert analysts continuously analyze network traffic to identify potential anomalies and malicious activities. This powerful combination of cutting-edge technology and human expertise ensures that your organization stays one step ahead of attackers. Experience peace of mind with mBRANE's intelligent, adaptive, and proactive approach to safeguarding your valuable digital assets, as we strive to achieve the highest degree of threat detection and mitigation.

ENHANCED INFORMATION SECURITY OPERATIONS

GLOBAL THREAT PROTECTION

- ❑ Award-winning Security Operation Center
- ❑ Cloud hosted SOC platform customized to Customer’s requirements
- ❑ 24/365 Eyes-on-Glass Monitoring & Active Threat Hunting
- ❑ Threat Intelligence Service from multiple reputed sources
- ❑ Implementation of common policies and correlation rules
- ❑ Continuous security monitoring
- ❑ Alerting and weekly/monthly reporting
- ❑ Log management platform

- ❑ Event Management
- ❑ Customized and Personalized Reporting
- ❑ Production support
- ❑ Forensic Investigations
- ❑ Endpoint detection and response
- ❑ Development of custom parsers to extract event info from unsupported infrastructure devices.
- ❑ Proactive threat hunting including low severity alerts
- ❑ Powered by combined Stellar Cyber & ArmorPoint SOC platforms

SECURITY OPERATIONS CENTER

24/365 Eyes-on-Glass Monitoring

Highly trained security analysts
Proactive monitoring for potential threats
Rapid response to security incidents
Minimizing downtime and financial impact

Active Threat Hunting

Continuous investigation
Identify previously undetected threats
Proactive defense
Strengthening overall security posture

Long Game

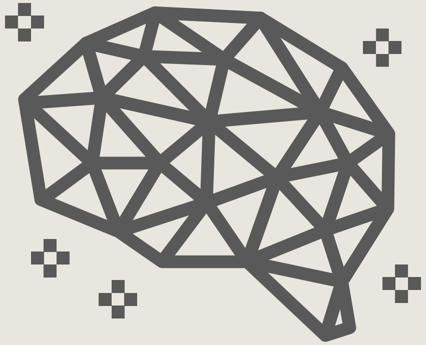
Reduced risk of security breaches
Increased operational efficiency
Compliance with regulatory requirements
Peace of mind with expert support

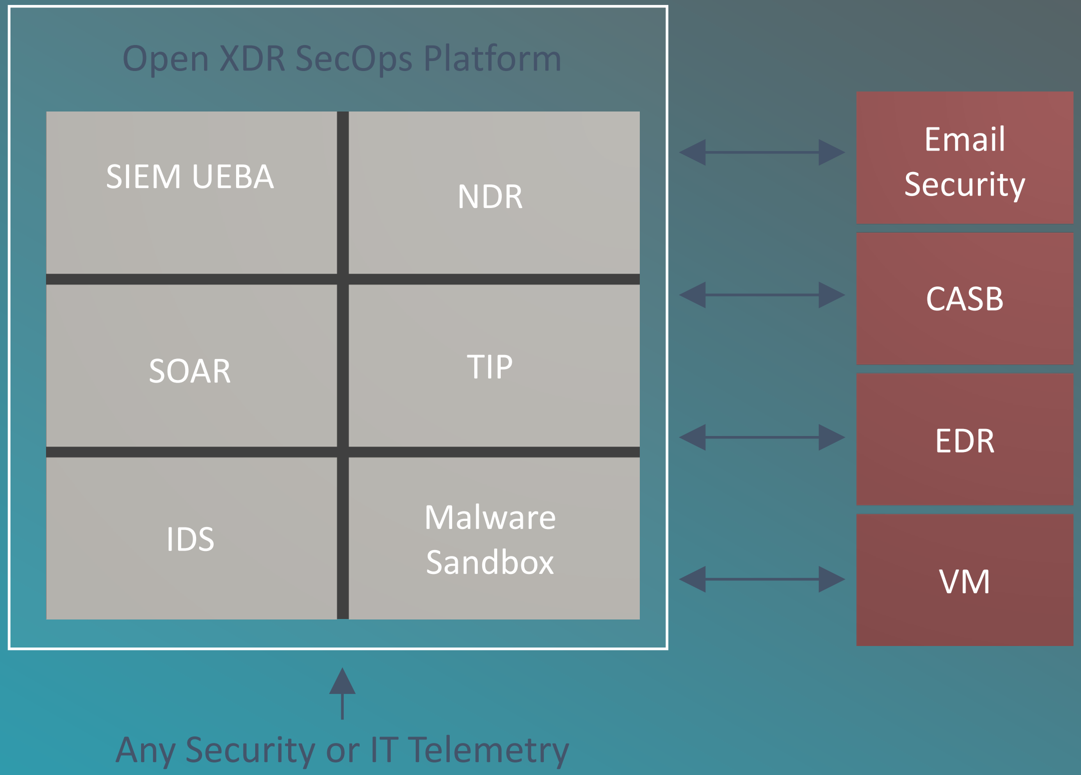
mBRANE
Security Operations Center

Unified Security Operation Center

SIEM Security Information Event Management	NDR	CASB
SOAR	TIP	EDR
IDS	Email Security	VM

Unified Intelligent Platform Integrated with Environment





Open XDR SecOps Platform

SIEM UEBA

NDR

SOAR

TIP

IDS

Malware Sandbox

Email Security

CASB

EDR

VM

Any Security or IT Telemetry

| Importance of MITRE ATT&CK framework to security operations.

97% of security professionals

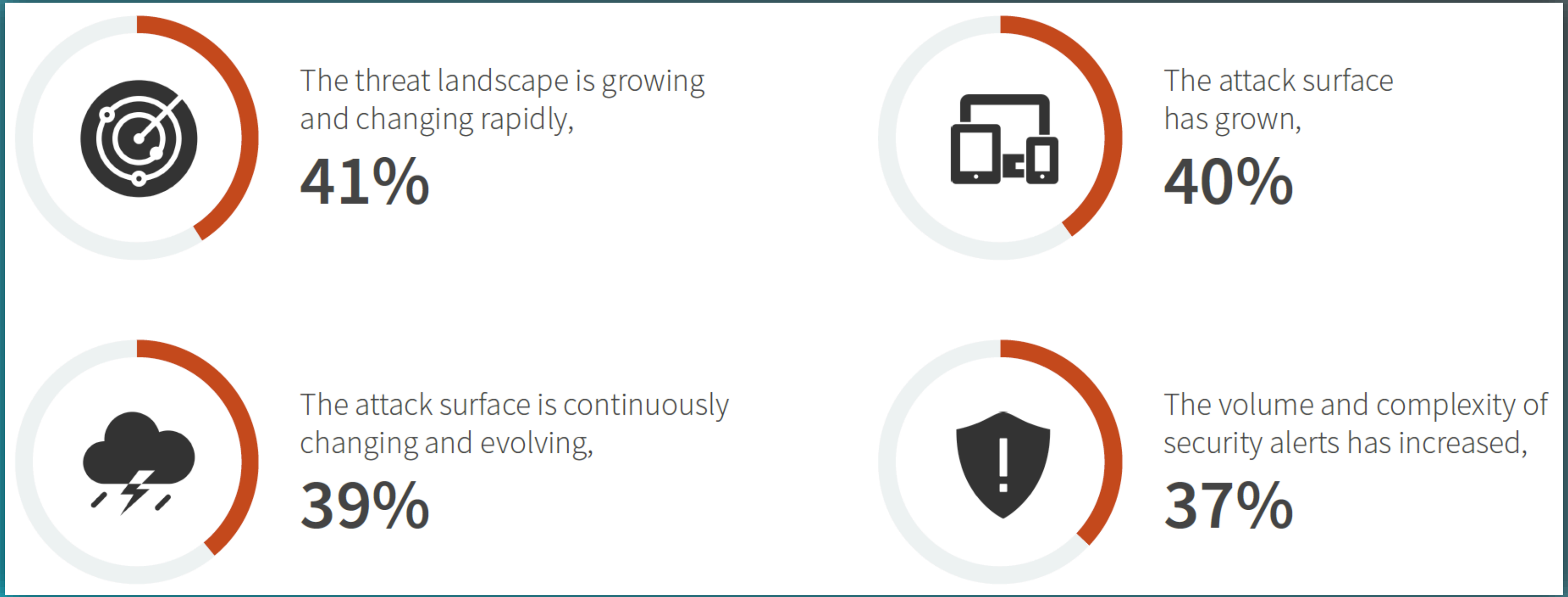
believe that MITRE ATT&CK (and derivative projects) will be critical, very important, or important to their organization’s security operations strategy

Most Organizations Use and See Value in the MITRE ATT&CK Framework for Security Operations

The MITRE ATT&CK framework has grown in popularity to the point that nearly nine in ten organizations use it to some extent today. As SOC managers look into the future, they see even greater MITRE utilization. In fact, 97% of security professionals believe that MITRE ATT&CK (and derivative projects) will be critical, very important, or important to their organization’s security operations strategy.

Information Security Operations Outcomes

Reasons for increased difficulty, per surveyed organizations



The threat landscape is growing and changing rapidly, **41%**

The attack surface has grown, **40%**

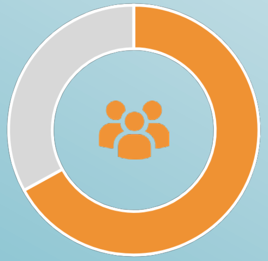
The attack surface is continuously changing and evolving, **39%**

The volume and complexity of security alerts has increased, **37%**

Improved SecOps efficiency, skills gap addressed, reduced MTTD/MTTR, and improved economics *

HALF OF ORGANIZATIONS BELIEVE SECOPS IS GETTING MORE DIFFICULT? **

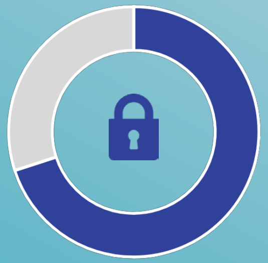
* Outcome modified from Gartner's XDR market guide
** From 2022 ESG Study "SOC Modernization and the Role of XDR"



67% of security professionals say that a cybersecurity “platform” is offered as an agreed-upon, standard architecture provided as an OPEN suite of products integrated through standard APIs and development tools.

PLATFORM PROLIFERATION IS ALREADY HAPPENING.

Enterprise Strategy Group by TechTarget



70% of organizations have deployed, are planning to deploy, or are considering deploying an extended detection and response (XDR) platform for threat management.

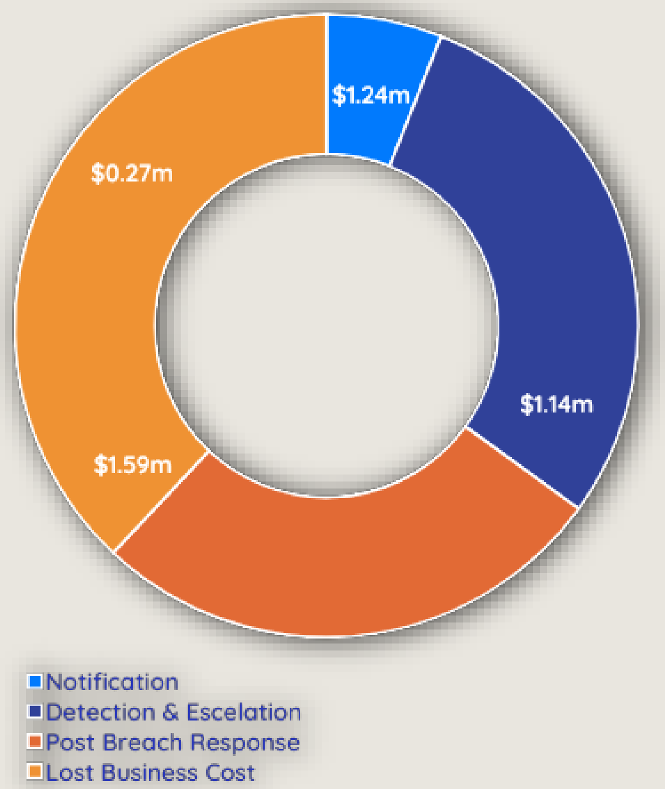
Cost of a Data Breach

$4.62m

Average total cost of a **ransomware breach**

Ransomware and destructive attacks were costlier than other types of breaches

Enterprise Strategy Group by TechTarget



The Case for SOC Modernization

Security Operations remain challenging

Increasing difficulty is due to the growing attack surface, dangerous threat landscape, and increasing use of cloud computing

Security professionals want more data and better detection rules

Despite the massive amount of security data in use, more is desired, as are better detection rules

SecOps process automation investments are proving valuable

While implementation strategies vary, automation investments are paying off for most

MITRE ATT&CK framework is proving valuable for most

However, many are still figuring out how and where to apply it to gain value

XDR momentum continues to build

While there is confusion about what XDR is, investment in support of advanced threat detection is significant.

MDR is mainstream and expanding

While use cases vary, MDR services are widely adopted across organizations of all sizes and maturity

SOC Modernization

SOC-as-a-Service

Next-Generation SIEM (NG-SIEM)

Stellar Cyber NG SIEM enables security teams to collect and automatically normalize log data from any data source making data audit ready for compliance needs. Once collected, threat intelligence and other contextual information enrich the data to optimize search and threat hunting functions. Additionally, user entity behavior analysis (UEBA) automatically identifies anomalous and suspicious behaviors to eliminate potential security threats missed by other security controls.

Network Detection and Response (NDR)

Stellar Cyber NDR combines raw packet collection with NGFW logs, NetFlow, and IPFix from physical or virtual switches, containers, servers, and public clouds, enabling deep packet analysis for over 4,000 applications and L2-L7 metadata and files from network traffic. In addition, with IDS and malware sandbox included, suspicious files will be automatically detonated safely to determine if they have malicious intent.

Security Orchestration and Automated Response (SOAR)

Stellar Cyber SOAR allows security teams to respond to cyber threats using pre-defined playbooks, ensuring consistent security outcomes. With hundreds of pre-built integrations to security, IT, and productivity products, users can create virtually any workflow required to mitigate identified cyber threats appropriately.

Open Extended Detection and Response (Open XDR)

Stellar Cyber Open XDR enables organizations to collect log and alert data from any security control, from the endpoint to the cloud and anywhere between. Then, using advanced machine learning techniques and threat detection rules to identify, correlate, and respond to advanced cyber-attacks in real-time. Unlike “closed” XDR solutions that only work with the vendor’s specific EDR data, Stellar Cyber’s “Bring your Own EDR” approach means organizations can use any EDR product they want with Stellar Cyber. Currently, Stellar Cyber supports all major EDR vendors.

XDR is designed for the outcome of detection and response.
It can still meet compliance requirements.

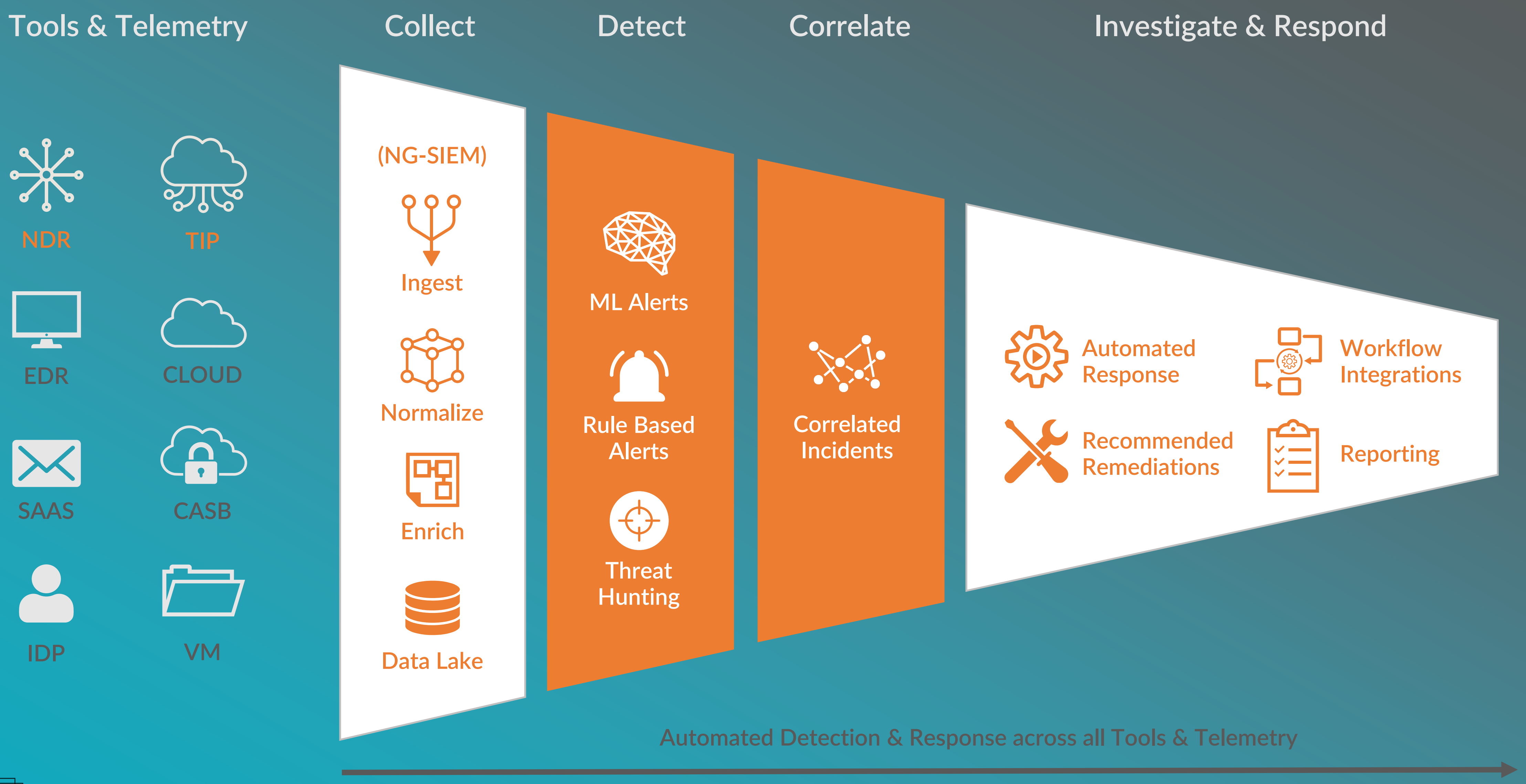
Deployability Cloud-native microservice architecture for scalability, availability and deployment flexibility

Data Fusion Centralize, normalize and enrich data across the entire attack surface, including network, cloud, endpoints, applications and identity

Detection
Built-in automated detections and Machine Learning

Correlation
High-fidelity correlated detections across multiple security tools

Intelligent Response
One-click or automated response from the same platform



Tools & Telemetry

- NDR
- TIP
- EDR
- CLOUD
- SAAS
- CASB
- IDP
- VM

Collect

(NG-SIEM)

- Ingest
- Normalize
- Enrich
- Data Lake

Detect

- ML Alerts
- Rule Based Alerts
- Threat Hunting

Correlate

- Correlated Incidents

Investigate & Respond

- Automated Response
- Workflow Integrations
- Recommended Remediations
- Reporting

Automated Detection & Response across all Tools & Telemetry

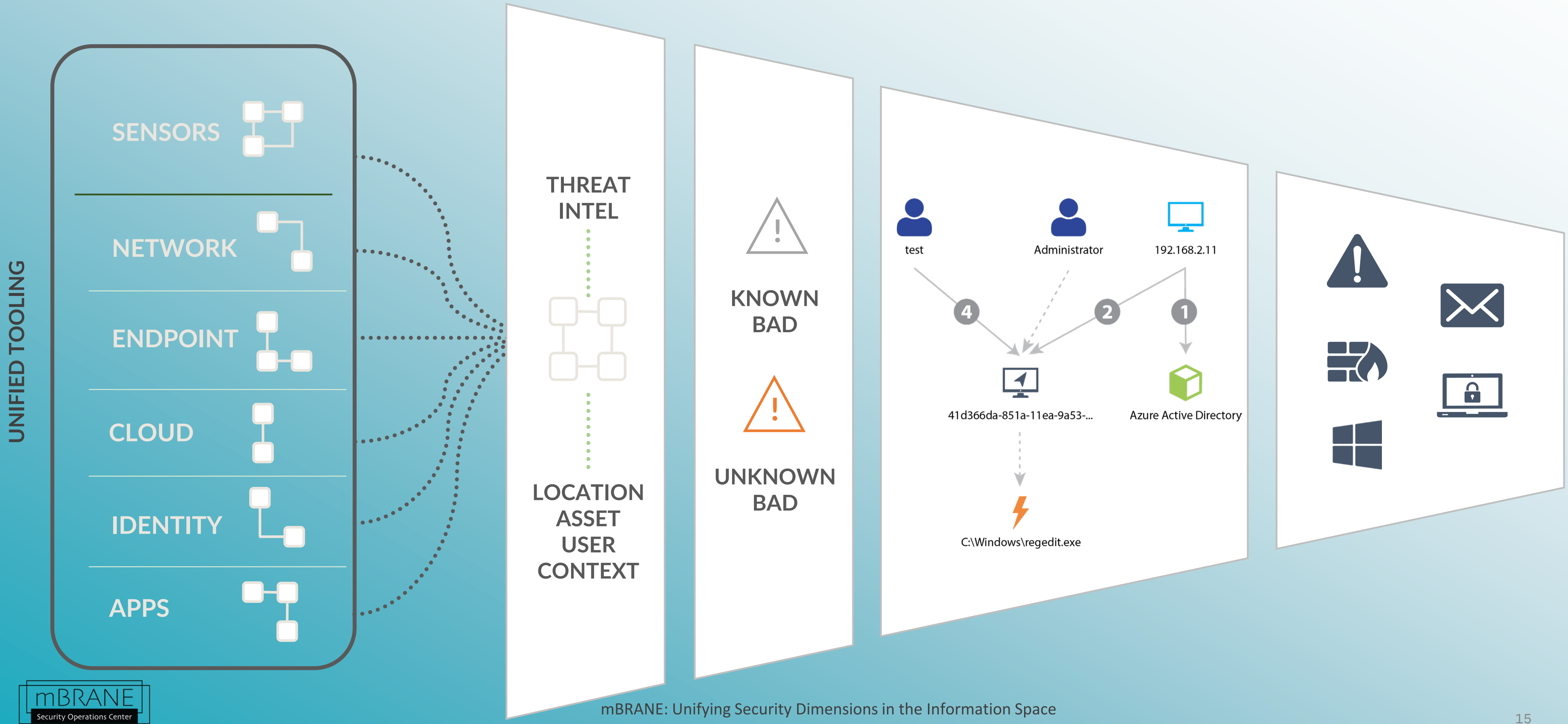
Entire Enterprise Attack Surface Collection

Normalized, Enriched Data

Multi Method Detections

ML-Based Incident Correlation

Automated Investigation, Intelligent Response



UNIFIED TOOLING

SENSORS

NETWORK

ENDPOINT

CLOUD

IDENTITY

APPS

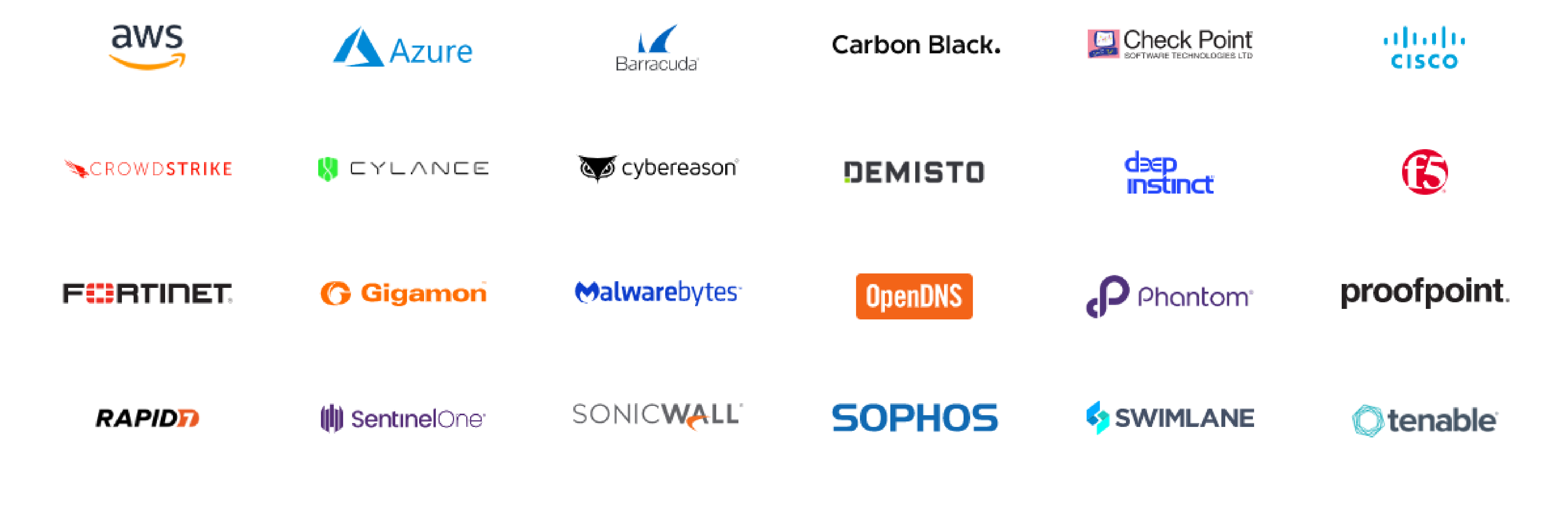
THREAT INTEL

LOCATION ASSET USER CONTEXT

KNOWN BAD

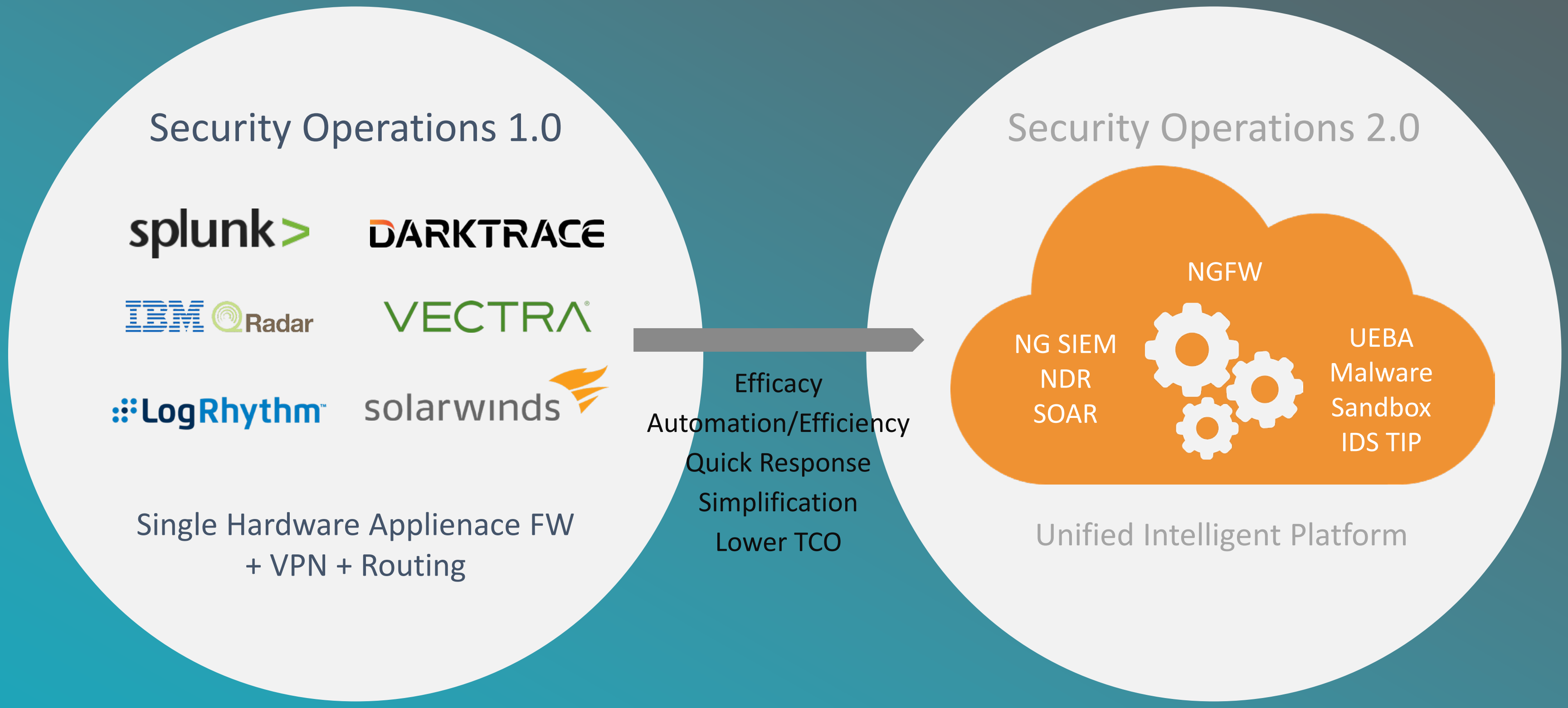
UNKNOWN BAD

SPOTLIGHT INTEGRATIONS



ADDITIONAL & CUSTOM INTEGRATIONS AVAILABLE

UNIFIED INTELLIGENCE



Security Operations 1.0

Single Hardware Applienace FW
+ VPN + Routing

Efficacy
Automation/Efficiency
Quick Response
Simplification
Lower TCO

Security Operations 2.0

Unified Intelligent Platform

Monthly Pricing

Unlimited devices

Cost Per Gb Daily Data Ingestion

$39.95/Gb/mo

Cloud Data Lake Managed Instance

$299/mo

Cost Per TB 30-Day Log Retention

$40/Tb/mo

secureEVERYTHING

UNIFYING SECURITY DIMENSIONS
INFO@SECURECENTRX.COM