FROST & SULLIVAN

TRANSFORMING CYBER DEFENSE with 360 Degree MDR Services

AUJAS CYBERSECURITY | NSE NSEIT

While enterprises have been investing in security, 73% of them still do not have complete visibility into their IT infrastructure. Managed Detection and Response (MDR) enables accurate threat detection and faster response through improved visibility beyond the network.

The Changing Threat Landscape and Emergence of Intelligent Attacks

Digital Transformation has been a key strategic objective for enterprises over the years. However, the rapid pace of technological changes and the dynamically changing threat landscape has made it imperative for organizations to relook at their transformation strategy and build more cyber resilience. Digital technologies and cyber security are inextricably intertwined and hence enterprises must put emphasis on building a pragmatic approach to cyber security.

From simple password guessing & brute force attacks in the 1980s, cyberattacks today include large scale, multi-stage, multi-vector, and multi-dimensional attacks that can easily evade traditional security defenses like firewalls, intrusion prevention systems (IPS), secure web, email gateways, and anti-virus platforms. These cyber threats are signature-less and can attack IoT devices, cloud, 5G networks, critical infrastructure, and security systems. Clearly, the rate of attack advancements have outpaced the ability of enterprises to assess, select and deploy advanced security technologies needed to combat these threats. Today, the pressing need for enterprises is to build a security posture that not just focuses on prevention but is prepared for accurate and faster threat detection and rapid response mechanism.

*Over **60%** of the global enterprises have noticed increased cyber-attacks around cloud, endpoint, social media, and IoT in the last 18 months.*

Traditional Approach hinders Security Transformation Objectives

Security Information and Event Management (SIEM) technology is the most common go-to solution for enterprises to enable comprehensive visibility into cyber threats across distributed IT infrastructure. Based on the log entries, a SIEM detects the Indicators of Compromise (IoCs) and can reconstruct the attack scenario depending on the events it collects. While SIEM has been trustworthy and a powerful security tool for most enterprises, when it comes to identifying unknown attacks, enterprises need the additional ability to capture the right security information.

Hosting a SIEM solution in an on-premise Security Operations Center (SOC) with large established team of in-house security professionals is typically capital intensive and operationally challenging. 24x7 management and monitoring of security devices is also a cumbersome task that hinders security transformation objectives. As an alternate, enterprises look towards Managed Security Service Providers (MSSPs) who offer quick deployment, affordable services, scalability and flexibility through subscription based service models. While managed firewall, intrusion prevention, DDoS (Distributed Denial of Service) mitigation, endpoint protection and vulnerability scanning are few of the most common service offering of an MSSP, most of them fall back on SIEM solution to collect logs, run analysis, perform event correlation, event alerts, reporting and incident management. However, to thwart today's cyber threats, enterprises cannot solely rely on SIEM.

Around 70% of the enterprises crumble to a modern cyberattack due to inadequate planning, strategy, and inability to respond to a threat.

TRADITIONAL APPROACH CHALLENGES THE SECURITY POSTURE OF ENTERPRISES:

- Threat Defense mechanism built on legacy architecture
- Excessive use of point security solutions
- Can stop one-dimension attacks but not multi-vector threats
- Limited visibility into the enterprise security architecture
- Unavailability of skilled security analysts
- Restricted access to latest cyber-security tools

Empowering Enterprises with Managed Detection and Response(MDR)

Managed Detection and Response or MDR, transcends the traditional MSSP model of cybersecurity by accelerating the threat detection and response time. The services not only include SIEM for security monitoring but the value proposition increases significantly with overarching security intelligence, threat hunting, endpoint threat detection, user behavior and security analytics. The contemporary approach of MDR leverages machine learning (ML) and artificial intelligence (AI) capabilities to investigate, and auto contain threats before launching an orchestrated response. In addition to 24x7 monitoring of the IT infrastructure, MDR providers offer holistic analysis, incident triaging, forensics, and response recommendations.

MDR is a process oriented cybersecurity concept that follows a 3-phased approach towards Cyber Defense through the entire life-cycle of the attack.

EXHIBIT 1: THE 3 PHASES OF THE ATTACK LIFE-CYCLE

BEFORE AN ATTACK	DURING AN ATTACK	AFTER AN ATTACK
Threat Identification: Proactively identify threats 24x7 and eliminate false positives. Aim to secure digital assets, networks, web, data, cloud, IoT devices, email, endpoints, application, platform, people and process.	**Threat Detection and Response:** Use of advanced security technologies to detect anomalies and respond to vectors by using rule based detection, threat analytics, deception technologies, incident response, EDR, UEBA and packet capture module.	**Breach Mitigation:** Quickly recover compromised devices and assets through prioritization, forensics, documentation, recovery planning, etc. and thereby improving the security posture for future threat instances.

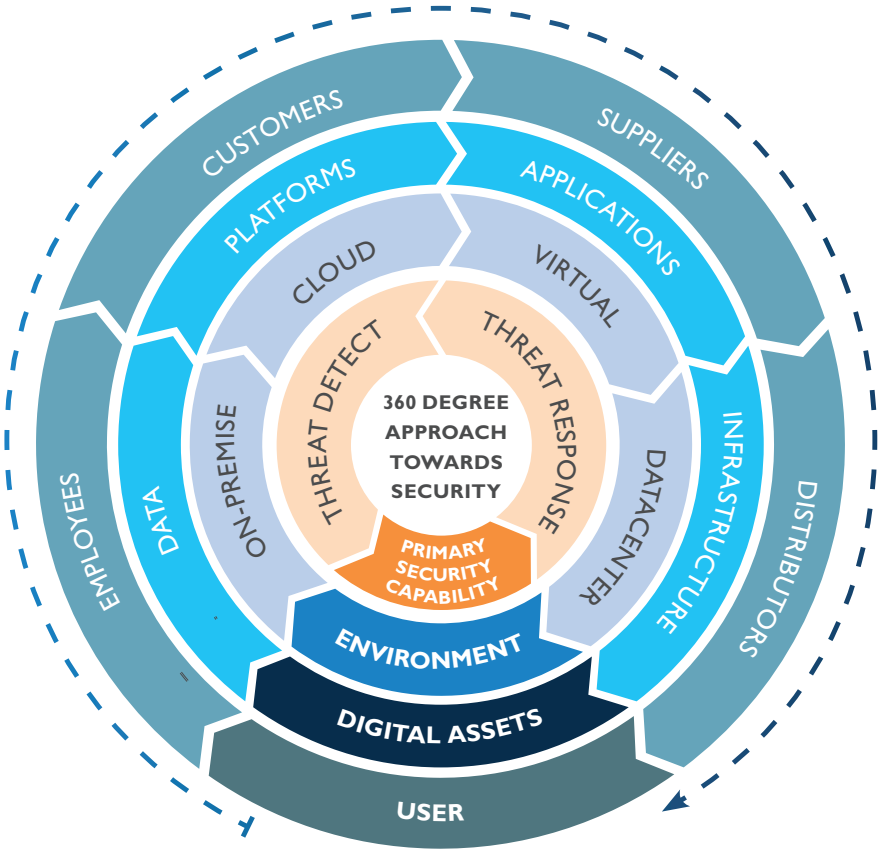
Source: Frost & Sullivan

Transforming Cyber Defense

Organizations must evaluate their cybersecurity strategy, organization structure, existing framework, technology solutions, internal processes, people competency, and other capabilities to effectively detect and respond to multi-dimensional, automated, and sophisticated attacks.

A 360-degree MDR architecture provides complete visibility into the enterprise infrastructure: be it on-premise, on the cloud or virtual environment. Any threat coming across the network, endpoint, and web or IoT devices is identified faster and a threat response plan is initiated. The response plan refers to managing risks, containing threats, and defeating attacks. It is not a reactive mechanism where damage is high; rather, it is an approach to swiftly contain and defeat attacks within the enterprise network while minimizing the effect of the breach and enable effective recovery.

EXHIBIT 2: THE 360 DEGREE SECURITY FRAMEWORK



360 Degree Approach *Source: Frost & Sullivan*

THE GOAL FOR ENTERPRISES SHOULD BE:

- Proactive and early detection of cybersecurity threats utilizing threat intelligence platforms, threat hunting solutions and techniques. Threat intelligence feeds should be analyzed for applicability, and should also be collected from non-automated sources such as from internal cross-functional departments.
- Continuous 24x7 security monitoring and operations conducted by a team of analysts as well as dedicated staff for incident investigations and forensics.
- Effective incident management and response via implementation of detailed incident handling and response process, formulation of threat specific incident response procedures, cross functional incident emergency response, and optionally rapid response contracts. A centralized inventory of all incidents related to information or cybersecurity should be maintained.

Building Next-Generation Cybersecurity Defense Center (CDC)

ALIGNING PEOPLE, PROCESS, AND TECHNOLOGY

The fundamental step towards establishing a Cybersecurity Defense Center (CDC) is to align people, process, and technology. People refer to having the right set of security analysts with the right skill sets. This includes threat hunters, product specialists, architects, and forensic experts who are responsible for 24x7 monitoring, cyber defense, and mitigation. The next step is to create the process; the typical workflow. Management systems need to be created with policy sets and procedures to fulfill the task of breach protection. Technology remains the strongest pillar in cyber defense, that binds together people and processes to deliver effective threat protection.

> *The global MDR market is expected to grow at CAGR 16.4% to reach $1.9 Bn. by end of 2024.*

EXHIBIT 3: THE 3 PILLARS OF CYBER DEFENSE CENTER

PEOPLE

- SOC Analysts, Investigators, Threat Hunters
- Forensic Experts, Incident Responders, Data Scientists
- SOC Architects
- Tool Builders, Support Teams
- Product, SIEM, Vulnerability Specialists

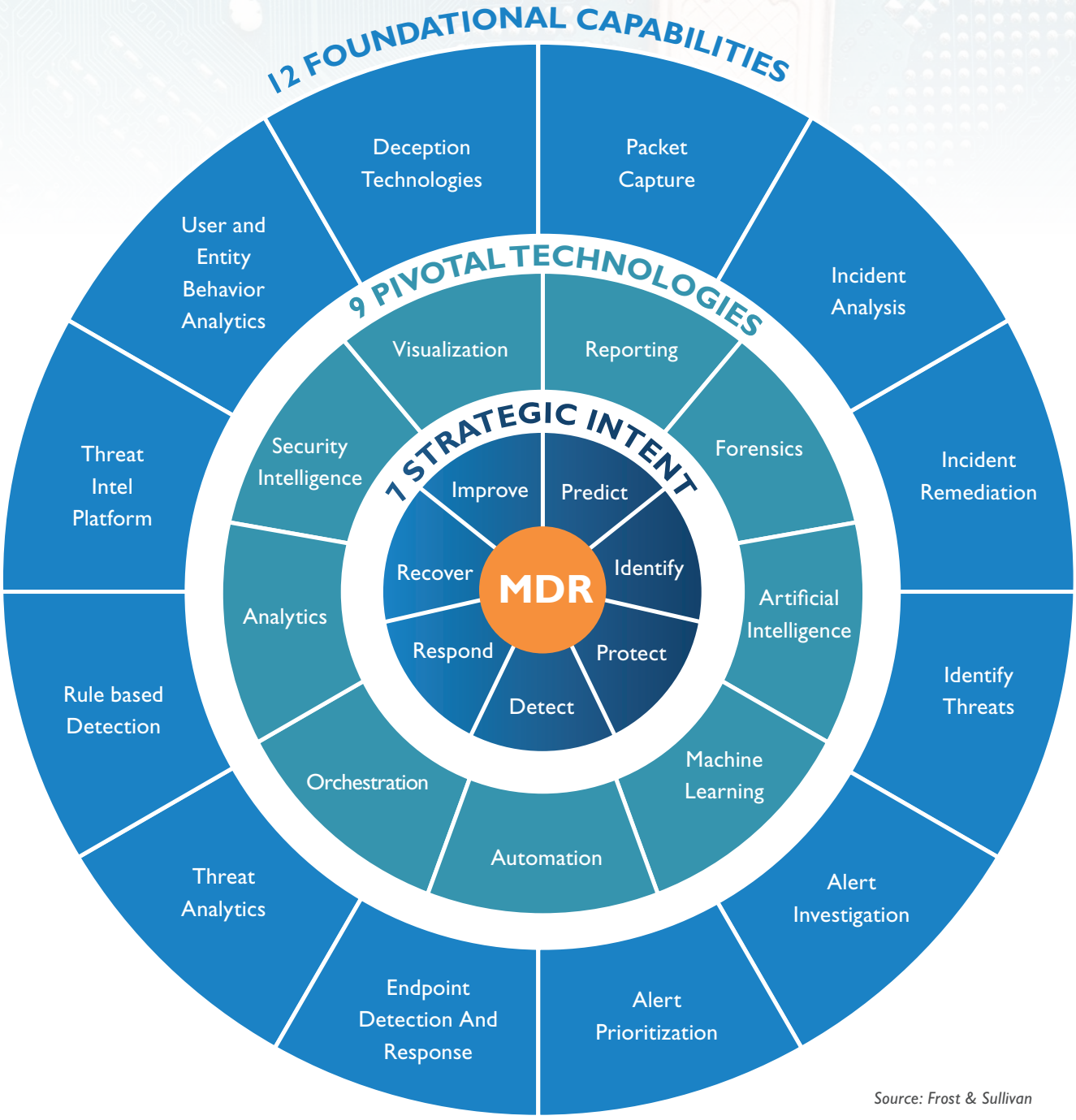
PROCESS

- Management Systems
- Governance Frameworks
- Policies and Procedures
- Vendor and 3rd party contract follow ups
- Audit Regimes

TECHNOLOGY

- Perimeter Security
- Endpoint Detection, Cloud Security, Data Security
- Threat Intelligence
- Encryption Protocols
- Monitoring and Detection

EXHIBIT 4: THE FROST & SULLIVAN MDR KALEIDOSCOPE



Source: Frost & Sullivan

The Frost & Sullivan MDR framework stands on 12 foundational elements, 9 pivotal technologies, and 7 strategic intents. Each of these parameters supports the overall structure of the framework that assesses threats from every possible perspective. It integrates human expertise with advanced technology and bridges the gap that exists between existing security capability and the ultimate need.

From a technology perspective, MDR focuses on threat intelligence to provide detection and response, which includes the capability to:

- **Identify Threats:** Focus on threat detection and elimination of false positives
- **Alert Investigation:** Ability to investigate alert volumes generated daily and find common ground between the alert, source, and destination IP
- **Alert Prioritization:** Rank alerts based on their priorities and possible impacts
- **Endpoint Detection and Response:** Record activities and events on endpoints and thus provides better visibility to security teams
- **Threat Analytics:** Addresses the drawback of rule-based detection by applying big data, analytics, and machine learning to detect advanced malware
- **Rule-based Detection:** Formulate and apply standard organizational rules on collected user activity logs to stop suspicious activity
- **Threat Intel Platform:** Aggregates, correlates, and analyzes threat data from multiple sources to create a defense mechanism by looking into IoCs like IP address, URL, domain names, email addresses, links, attachments, etc.
- **User and Entity Behavior Analytics (UEBA):** Process large datasets to identify potential threats by creating a baseline, risk scores and integrating with SIEMs
- **Deception Technologies:** Use of simulated and automated honey-nets and honey-pot concepts for easier threat detection and response
- **Packet Capture:** Focus not only to capture events but the total packet capture to understand the dynamics of an attack
- **Incident Analysis:** Automate data collection and analysis to measure the impact of an attack, find attributes of an attacker, identify assets that are compromised and finally investigate the root cause of an attack
- **Incident Remediation:** Enable faster containment, recovery, and mitigation of threats

BENEFITS OF MDR

- Early detection of threats in real-time
- Quick to assess threats and create alert prioritization
- Better response mechanism, incident response
- Faster investigation of attacks
- Predict threats based on behavioral analysis
- Access to skilled threat hunters and defenders

CHOOSING THE RIGHT MDR PROVIDER

Once enterprises have realized the need for an MDR solution, the next step is to find the right partner. Choosing the best available MDR provider may be a tough call. However, ticking the following check-boxes can help during the selection process.

The biggest success factor for MDR is its access to cutting-edge security technology.

POINTS TO CONSIDER WHILE SELECTING A MDR PROVIDER:

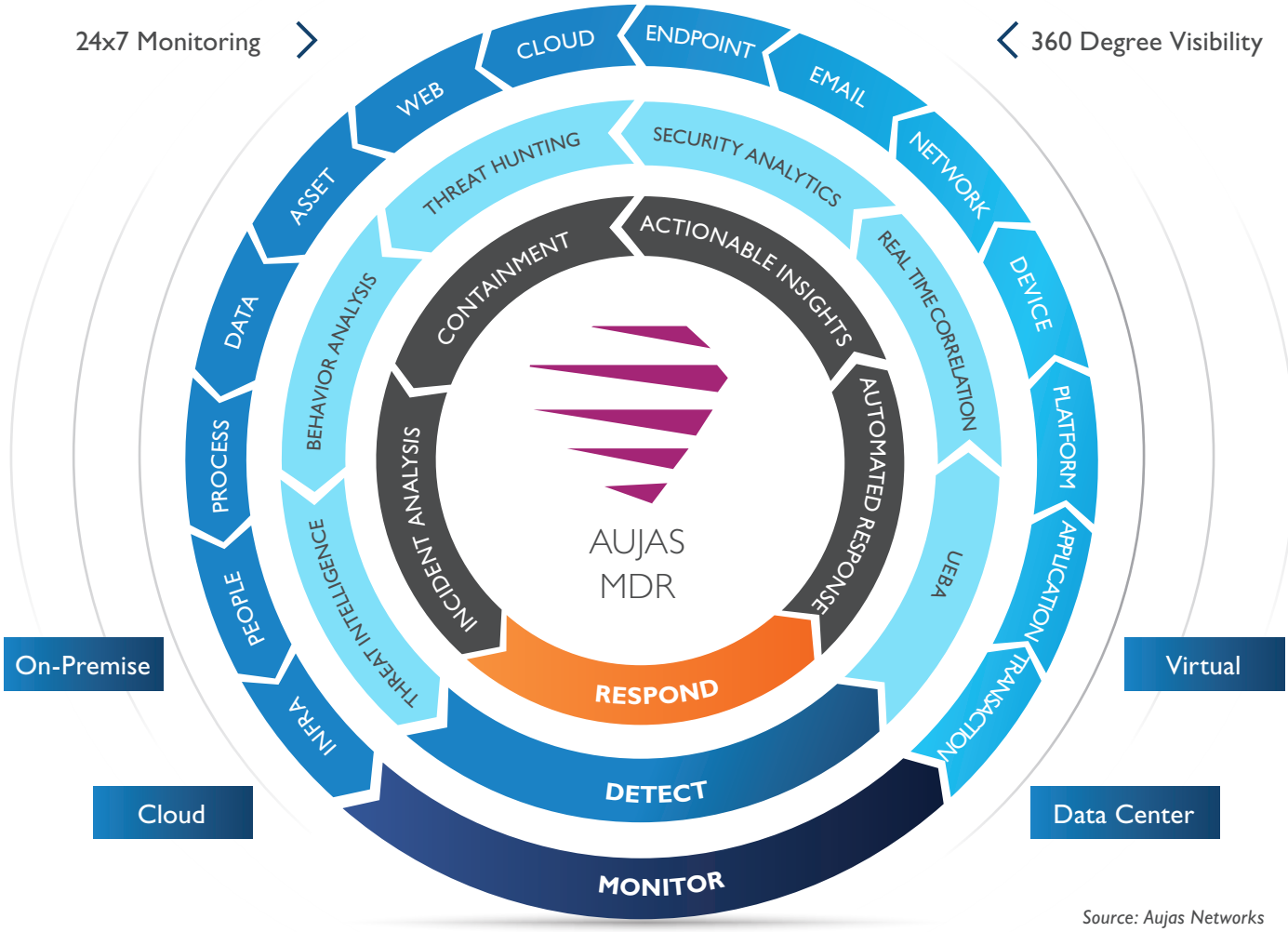
- Comprehensive MDR portfolio
- Proactive threat hunting with lesser time to detect threats in real-time
- Has structured security processes that adhere to industry mandates
- Actionable threat intelligence and reporting
- Has EDR capabilities, incident remediation, and easy threat mitigation
- Uses AI/ML, analytics, automation, and orchestration within security processes
- Hierarchy of threat hunters, defenders, investigators, architects, specialists, and forensics experts

Aujas 360 Degree MDR

Aujas is one of the emerging names in the global cybersecurity market. The company builds and transforms cybersecurity posture to enable businesses and mitigate risk. When it comes to next generation threat detection and response, Aujas offers 360 degree MDR services that are proactive, ML-driven, and offers threat detection, monitoring and response capabilities for different layers of technology infrastructure (network, web, cloud, endpoint, IoT devices, applications, and data). Enterprises get to access comprehensive and real-time visibility into the security posture by leveraging the IoCs. Breach detection time is reduced through early notification and swift contextualized remediation assistance is being provided.

360 degree reflects Aujas' ability to provide security across the entire enterprise spectrum not only for on-premise infrastructure but beyond traditional perimeter security to the data center, cloud and virtual environments.

EXHIBIT 5: AUJAS 360 DEGREE MDR FRAMEWORK



Source: Aujas Networks

Aujas 360 Degree MDR focuses strongly on the threat monitoring, detection, and response process. Irrespective of the location of the data: on-premise, data center or cloud; Aujas can monitor threats across the entire IT infrastructure. It uses advanced security technologies like threat intelligence, behavior analysis, analytics, UEBA (user and entity behavior analytics) and ML driven real-time correlation as a part of threat detection technique. The team of threat hunters, specialists, architects, investigators, and responders work closely with customers to run CDC processes by leveraging advanced technologies 24x7.

KEY ELEMENTS OF AUJAS 360 DEGREE MDR

- **PROACTIVE THREAT MANAGEMENT:** Ability to predict and neutralize threats
- **INSTANT RESPONSE:** Quick to accurately identify an attack, provide notification and activate response plan
- **REDUCED FALSE POSITIVES:** Validate, investigate, and raise alarms based on the severity of threats. Provide recommendations to minimize the impact of an attack and contain threats
- **AUTOMATED AND AI-DRIVEN BREACH PREVENTION:** Use automation to replace manual, mundane, and repetitive cyber defense processes
- **ML-DRIVEN INCIDENT RESPONSE:** Incident analysis based on Machine Learning driven techniques for faster investigation
- **SOAR:** Employ Security Orchestration and Automation (SOAR) to improve incident response and standardization of processes
- **SECURITY ANALYTICS:** Leverage security analytics across endpoints, user, network, and application behavior to provide insights on attack
- **INCIDENT REMEDIATION:** Accelerated remediation for both known and unknown threats
- **DARK WEB MONITORING:** Provide visibility into the hacker community and underground marketplaces for any stolen data
- **THREAT HUNTING:** Experienced team of threat hunters capable of blue teaming, red teaming, forensics, and investigation

EXHIBIT 6: AUJAS MDR OFFERINGS

Threat Intel Management
Consumes threat intel, supports STIX / TAXII & unstructured intel feeds, yields consumable & actionable threat intelligence

SIEM Services and Operations
Controls integration, process mapping, relevant reporting, operations & continuous improvement

Endpoint Detection and Response (EDR)
Endpoint Prevention and Quarantine

Security analytics
Big data analytics solutions with ML and AI for anomaly detection

Security Orchestration, Automation & Response (SOAR)
Continuous improvement framework, Runbook automation, incident response, visualization and orchestration

Source: Aujas Networks

The Aujas Differentiator

Over the last 12 years, Aujas has continually evolved to defend against global cyber threats. Working with a diverse range of industry verticals, Aujas has successfully developed and built a comprehensive MDR offering that enables organizations to swiftly act to cyber threats by reducing false positives and delivering services that are scalable, quick, and reliable.

> *The most important Aujas differentiator lies in its expertise and experience in defending the most critical workloads for very large scale projects.*

AUJAS VALUE PROPOSITION AND UNIQUE DIFFERENTIATION:

- **Experience in securing large scale and critical targets:** Aujas has demonstrated excellence in providing 24x7 cyber defenses for extremely large-scale environments. Be it the country's national citizen data, global banks or telecom companies, Aujas has successfully protected all these targets without any hint of a cyber breach. Customers reap benefits of this Aujas experience, which is a unique competitive advantage in terms of quality of service and ability to deal with large scale sophisticated threats.
- **Solid strength in security with complementary functions:** Managed security is an outcome of Aujas' experience and expertise across core focus areas of security. Aujas does not focus on just providing point solutions rather work continuously to create an integrated security architecture that fulfills enterprise objectives.
- **Excellence in Risk Advisory, Security Testing, Cloud Security, and Security Engineering and Technology versatility:** From helping enterprises manage compliance requirements, securing cloud applications, and integrating security diverse security products to testing the existing security posture using vulnerability assessment, penetration testing, and threat simulation, Aujas enable clients to identify vulnerabilities, security loop-holes, and attack patterns before suggesting advanced security capabilities.
- **International experience:** Aujas brings in international exposure with the team earlier worked across the world, understanding best-in-class global practices and advanced techniques.

The Future of Cybersecurity

The future of cybersecurity would be very different from what it is today. Signature based attacks would completely replace signature-less threats and legacy security infrastructure would cease to exist. Interoperability would become the hallmark of next-generation cyber defense as enterprises increase their focus towards improved threat detection, investigation, and response capability.

To stay ahead of hackers, cyber defense of the future would:

- Adopt behavioral-based analytics across users, devices, networks, applications, and cloud environments
- Need more structured and cohesive workflows with seamless integrations
- Add intelligence on top of security tools and techniques to empower security teams to implement risk and confidence based automated response actions
- Leverage AI across detection, investigation, and response processes
- Acquire solutions that treat privacy as paramount importance and consistently update Out-Of-The-Box (OOTB) playbooks with the fast-changing industry mandates
- Access real-time reports and dashboards that enable Chief Information Security Officers (CISOs) to plan, act and refine their course of action regularly
- Investigate security breaches accurately based on data analysis and machine learning
- Employ APIs to connect all security controls for improved investigation and remediation action and build a unified security posture

ABOUT FROST & SULLIVAN

For over five decades, Frost & Sullivan has become world-renowned for its role in helping investors, corporate leaders and governments navigate economic changes and identify disruptive technologies, Mega Trends, new business models and companies to action, resulting in a continuous flow of growth opportunities to drive future success.

Contact us: Start the discussion.

www.frost.com

ABOUT AUJAS CYBERSECURITY

Aujas cybersecurity is an enterprise security service provider for organizations across North America, Asia Pacific, and EMEA regions. Aujas has deep expertise and capabilities in Identity and Access Management, Risk Advisory, Security Verification, Security Engineering & Managed Detection and Response services. By leveraging innovative products and services, Aujas helps businesses build and transform security postures to mitigate risks. The service focus is to strengthen security resilience by minimizing the occurrence of sophisticated attacks and threats while offering 360-degree visibility and protection across enterprise infrastructure.

www.aujas.com

contact@aujas.com