



# Managed Detection and Response (MDR)

Monitor, Detect, and Resolve security issues across multiple endpoints with Managed Detection and Response. US Signal's next generation Managed Detection and Response (MDR) is an endpoint security solution that deploys software-based tools to gather data from endpoints and utilizes that data to analyze suspicious system activities. US Signal leverages a third-party software platform to monitor, collect, and analyze data from endpoints that could indicate a threat. Additionally, rules can be configured to automatically respond to identified threats to remove or contain them.

Let US Signal's security experts monitor, detect, and resolve security issues across your multiple endpoints with Managed Detection and Response (MDR), a Managed Endpoint Detection and Response service. US Signal's Security Operations Center ("SOC") team receives and responds to all security alerts, freeing up your internal resources and enabling you to leverage the SOC team's extensive security experience and expertise.

## TECHNICAL OVERVIEW

US Signal's Security Operations Center ("SOC") team will work with your team to manage the deployment and setup of the MDR service. This product utilizes a cloud-based deployment model, which means that the agents communicate directly with a central management platform in the cloud, as well as light weight agents, or endpoint installations that usually have much less performance impact on systems.

Software agents conduct endpoint monitoring and collect data—such as processes, connections, volume of activity, and data transfers—into a central database. From there, pre-configured rules in an MDR solution can recognize when incoming data indicates a known type of security breach and triggers an automatic response, such as to log off the end user or send an alert to a staff member. Lastly, Forensics tools can enable IT security professionals to investigate past breaches to better understand how an exploit works and how it penetrated security. IT security professionals also use forensics tools to hunt for threats in the system, such as malware or other exploits that might lurk undetected on an endpoint.

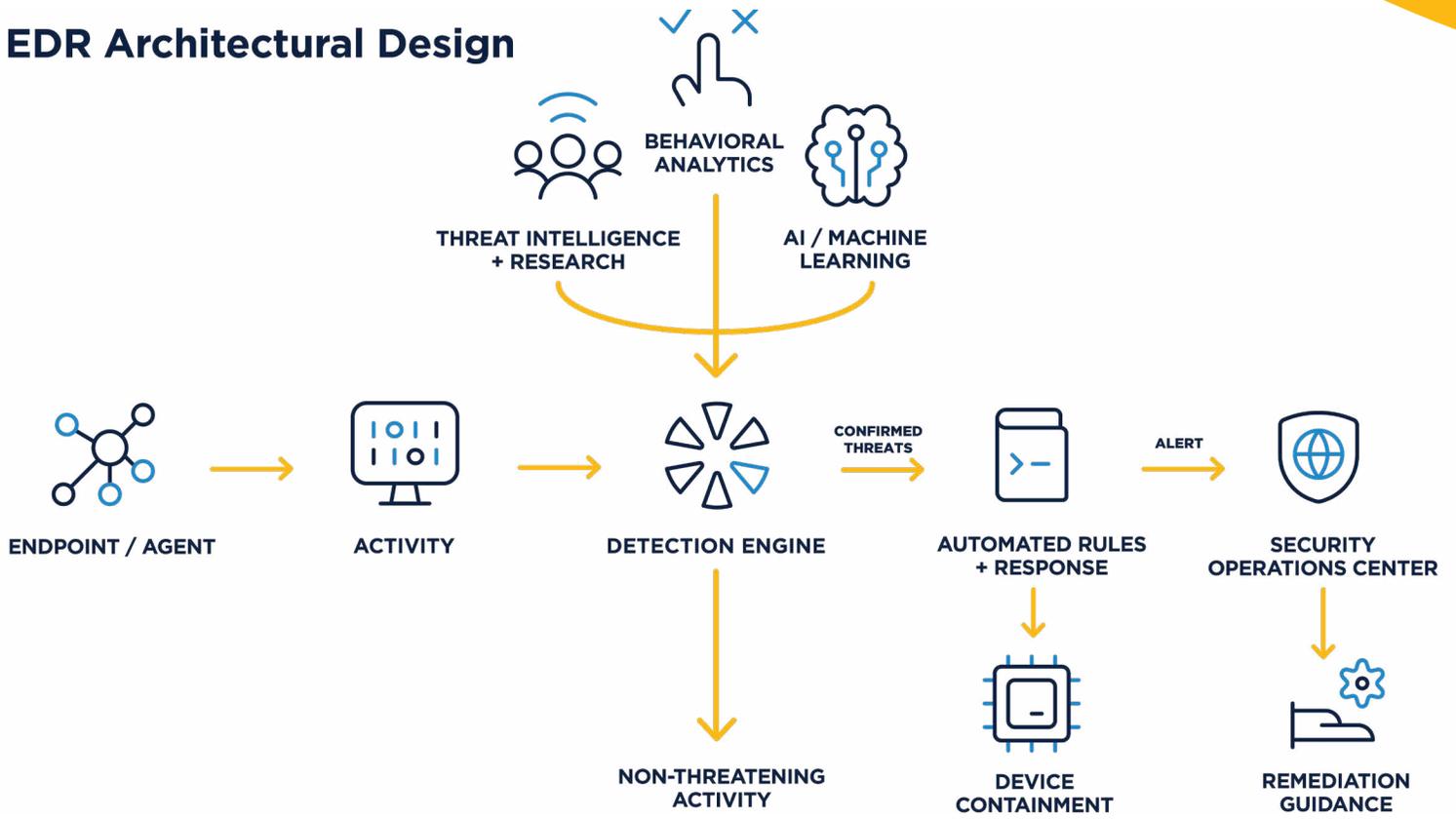
## AT-A-GLANCE

- + Monitor and collect activity data from endpoints that could indicate a threat
- + Analyze this data to identify threat patterns
- + Responds automatically to identified threat to remove or contain, and notify security personnel
- + Research identified threats and search for suspicious activities with forensics and analysis tools

## KEY FEATURES

- + Real-time continuous monitoring and collection of endpoint data
- + Rules based automated response and analysis capabilities
- + AI behavioral based detection
- + Cloud based deployment model
- + Light weight agents

# EDR Architectural Design



## SERVICE LEVEL AGREEMENT

For MDR customers, Response SLA is 1 hour for Customer alert notifications from the receipt of alert within US Signal’s Alert Management System. Service Portal availability guarantee of 99.95%, excluding planned and emergency maintenance. US Signal will use commercially reasonable efforts to notify customers of any scheduled maintenance that may affect the availability of the Services.

## SERVICEABILITY

This product is available on an annual term basis with a minimum of a one-year term agreement. It can be bundled with other US Signal services or be purchased independent of other US Signal services.

## PRICING

Pricing will be comprised of a monthly fee per endpoint as well as a non-recurring implementation and setup charge. The customer may add or remove endpoints throughout the billing period but will be billed for the highest number of agents deployed at one time throughout the billing period.

## FEATURES OF MANAGED DETECTION RESPONSE

✓ Global Platform Management	✓ Visual Killchain Representation
✓ Remote Worker Protection	✓ Secure Remote Shell
✓ AI Behavioral Based Detection	✓ Custom Detection Rules
✓ Machine Learning Based Detection	✓ Automated Quarantine
✓ Malware Rollback	✓ Advanced Technical Support
✓ Firewall Control	✓ Alert Response
✓ Device Control for USB, Bluetooth	✓ Agent Lifecycle Management
✓ Device Containment	✓ Remediation Guidance
✓ Complete Endpoint Visibility	✓ Quarterly Account Review
✓ 24x7x365 US Signal SOC Monitoring	

## RESPONSIBILITIES

### DEPLOYMENT

US Signal will provide virtual guidance during the deployment process to ensure proper deployment is achieved, however the customer is ultimately responsible for the execution of the deployment. US Signal can offer physical assistance for deployment if desired, this will result in an additional cost to the customer.

### ALERTS & RESPONSE

Alerts will be sent to the US Signal SOC who will handle the response measures and notify the customer accordingly.

### TECHNICAL SUPPORT

Full technical support will be provided by US Signal. Any support that requires escalation will be coordinated by US Signal on behalf of the customer.