Indian Health Service

KOWAINE BAKER
A&E FEDERAL LEAD
DATE

EndPoint Detection and Response (EDR)

- THE VALUE AND IMPACT PROVIDED

What is Endpoint Detection and Response?

- EDR provides enterprise security professionals with enhanced capabilities to analyze and search detailed endpoint data for traces of malicious activity, and bring high-risk data to the attention of analysts
- gathers and analyzes information related to security threats on computer workstations and other endpoints, making it possible to identify security breaches as they happen and facilitate a quick response
- cybersecurity technology that continuously monitors devices to detect and respond to cyber threats like ransomware and malware

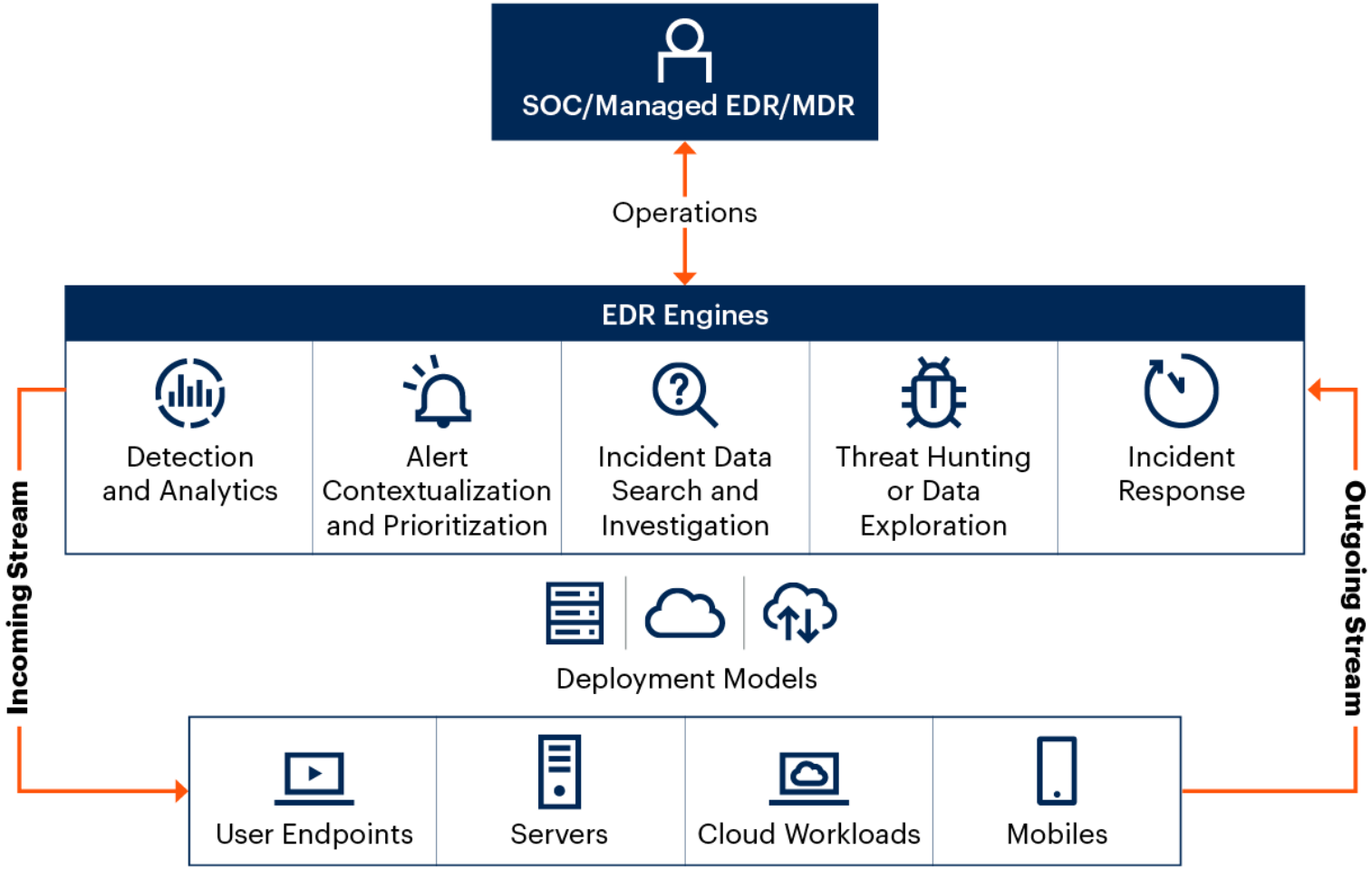
EDR Value

- Reduced Incident Response (IR) costs
- Remediation functionality in case of ransomware attacks
- Achieve deeper endpoint activity visibility
- Alleviate response fatigue

Misinterpreted characteristics of EDR

- EDR does not replace forensics tools, which tend to focus on collecting full disk captures with an emphasis on ascertaining legal truth
- EDR does not conduct endpoint log analysis
- EDR is not a user and entity behavior analytics (UEBA) technology that establishes a baseline of user behavior and triggers alerts when anomalous behaviors are seen
- EDR is not a host-based intrusion prevention system (HIPS)

EDR Design Diagram



Source: Gartner
750046_C

Gartner

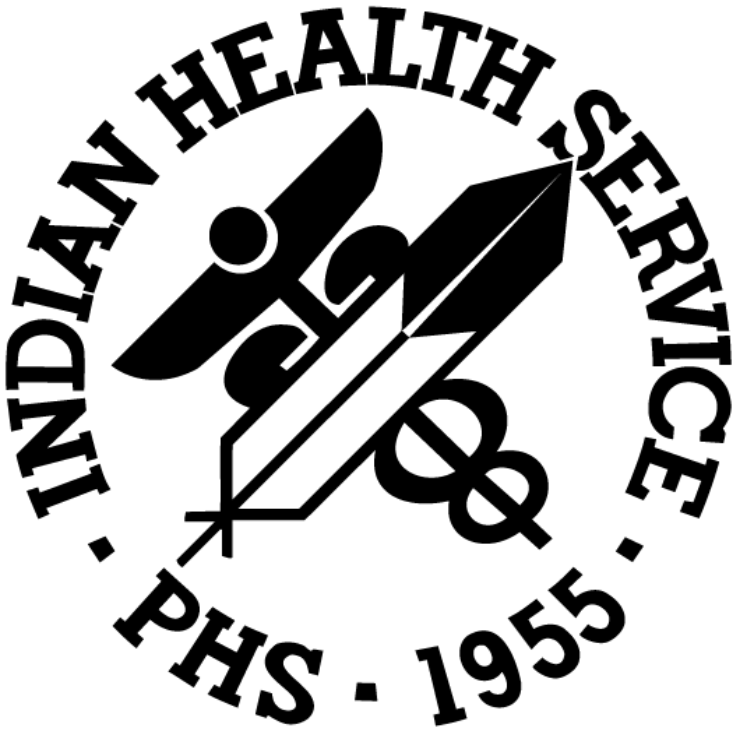
Implementing EDR effectively

- choose solutions with a single unified agent and fast remote deployment
- prioritize technologies with ease of use and prebuilt automated playbooks
- favor cloud-hosted solutions with flexible deployment options
- integrate with existing security infrastructure and operations tools is as important as specific EDR features
- requires more skill to deploy, manage and operate than traditional endpoint protection platforms (EPP) solutions
- assess the organization's ability to monitor and manage detection and response services to identify gaps and determine if a managed service is required

Best Practices for EDR Operations

- Do not turn on automated blocking until confident in detection accuracy
- The shift from monitoring to block mode should be made in phases
- When planning operational practices around EDR, avoid “malware-centricity.”
- Institute a root-cause analysis process aimed at figuring out how an attacker got in and then making technology and policy changes to prevent similar occurrences in future
- Integration with overall threat detection and response program

EDR Demo


INDIAN HEALTH SERVICE
PHS · 1955 ·