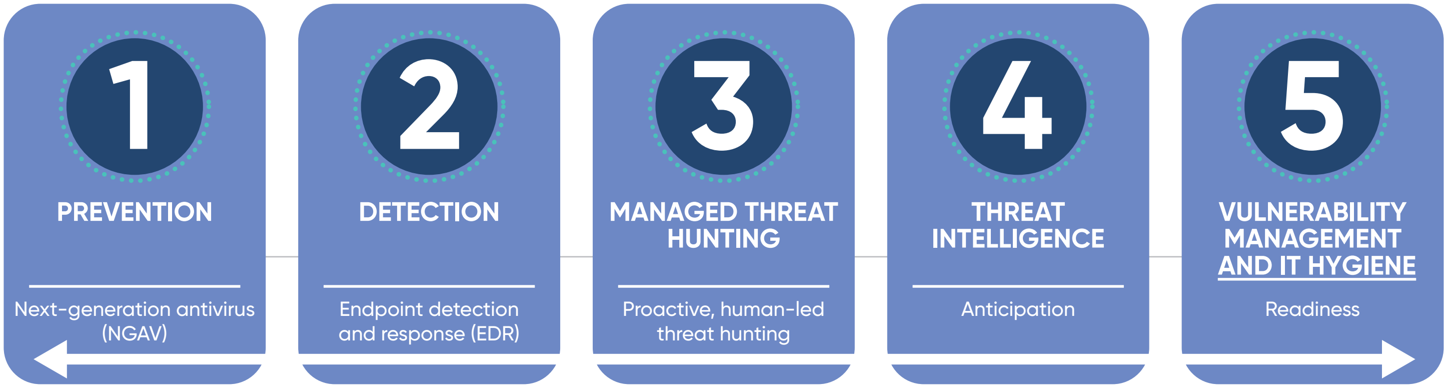
Endpoint Detection and Response (EDR)

Attackers move so quickly and stealthily that it's challenging for both protection technologies and security professionals to keep up with the latest threats and proactively defend against them.

To respond just as quickly as the attackers, modern endpoint protection requires full visibility:


1
PREVENTION
Next-generation antivirus (NGAV)
2
DETECTION
Endpoint detection and response (EDR)
3
MANAGED THREAT HUNTING
Proactive, human-led threat hunting
4
THREAT INTELLIGENCE
Anticipation
5
VULNERABILITY MANAGEMENT AND IT HYGIENE
Readiness

These five capabilities can only be fully enabled, integrated, and delivered through a fully managed, cloud-native platform that simplifies security operations and meets the speed, flexibility, and scalability required to defend against today's most sophisticated threats.

Prevention – Deny entry to bad actors

Unlike legacy security solutions requiring daily updates that leave endpoints temporarily unprotected, next-generation antivirus solutions can leverage machine learning to keep security current without burdening security and IT teams.

Detection – Find and remove attackers who slip through

An EDR solution should record all activities of interest on an endpoint for deeper inspection, both in real time and after the fact, and enrich this data with threat intelligence.

Managed threat hunting — Elevate detection beyond automated defenses

Managed threat hunting teams analyze threats and work closely with in-house teams, guiding them from detection through response. This interaction with experts raises the maturity level of in-house security and IT teams.

Threat intelligence – Understand and anticipate attacks

To respond just as quickly as attackers, endpoint security solutions should always incorporate threat intelligence and/or have the ability to integrate third-party intelligence.

Vulnerability management and IT hygiene – Fortify your environment against attacks

Provide the visibility and actionable information that security and IT teams need to understand which systems and applications are at risk, as well as who and what are active in the environment.

Managed Endpoint Detection and Response—managed by the CBTS security operations center and powered by the CrowdStrike platform—leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft, and enriched telemetry from across the enterprise. Together, we deliver hyper-accurate detections, elite threat hunting, and automated protection and remediation.

Configuration

- Ensure proper configuration of the Prevent and Insight products.
- Incidents managed through CBTS ITSM system.

24x7 Monitoring & Alerting

- Always on SOC
- On-staff level 3 and 4 security technicians.
- Exceptions management

Threat Hunting

- Monthly
- Searches for threats not caught by existing signals/analysis, based on latest threat intelligence.

Reporting

- Monthly/quarterly reporting of alarms, incidents, and threats.

70% of successful breaches begin on endpoint devices.

Purplesec – cybersecurity statistics – data and trends for 2022

About CBTS

From developing and deploying modern apps and the secure, scalable platforms on which they run, to managing, monitoring, and optimizing their operations, CBTS is the trusted partner businesses need to thrive in the application era. For more information, please visit **www.cbts.com**