Digital Security
Progress. Protected.

CYBER**RESILIENCE**  DETECT + RESPOND

Achieving cyber resilience: ESET's four-step approach to business continuity.

Step 3: Detect and respond

Business networks typically face an endless stream of chatter as hackers probe systems. This activity is analogous to a knock on the door, not an intrusion. Detecting real threats, and prioritizing and responding to them, demands human oversight—strongly supported by the right technologies.

Primary among these is **endpoint detection and response** (EDR). Gartner defines EDR as "solutions that record and store endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems."

Many insurance companies now require an EDR solution as well as endpoint security as a condition for cybersecurity coverage.

Cloud sandbox analysis executes and analyzes potentially malicious files in an isolated environment to identify their true purpose and block them before they can spread. It has the ability to protect against previously unknown threats, including zero-day malware and ransomware.

Data leak prevention (DLP) defends against planned or accidental data leaks, malicious insider actions, productivity issues, BYOD risks and more.

A threat intelligence service provides data feeds that can be used to configure network protection devices to be on the lookout for new threats. It can offer global knowledge on targeted attacks, advanced persistent threats, zero-days, botnets and more.

ESET Solutions

- **ESET Inspect**—Comprehensive EDR solution
- **ESET LiveGuard Advanced**—Cloud sandbox analysis
- **ESET Threat Intelligence**
- **Safetica**—Data leak prevention

Checklist: A closer look at ESET Inspect, ESET's EDR solution

- By monitoring and evaluating all activities happening in the network (for example, user, file, process, registry, memory and network events), ESET Inspect enables traceability of threats—allowing you to see the chain of events that led to a threat appearing on your network.
- Provides the ability to identify and take action against anomalous and suspicious behaviors that expose the network to vulnerabilities.
- Delivers real-time monitoring, rapid risk assessment, incident response, investigations and remediation—all of which reduce the possibility of data breaches, successful ransomware attacks and undetected threats.
- Implementing ESET Inspect meets the cybersecurity insurance requirements for EDR.