



# **EDR vs MDR vs XDR**

Out of Many Acronyms, One Sure Choice

---

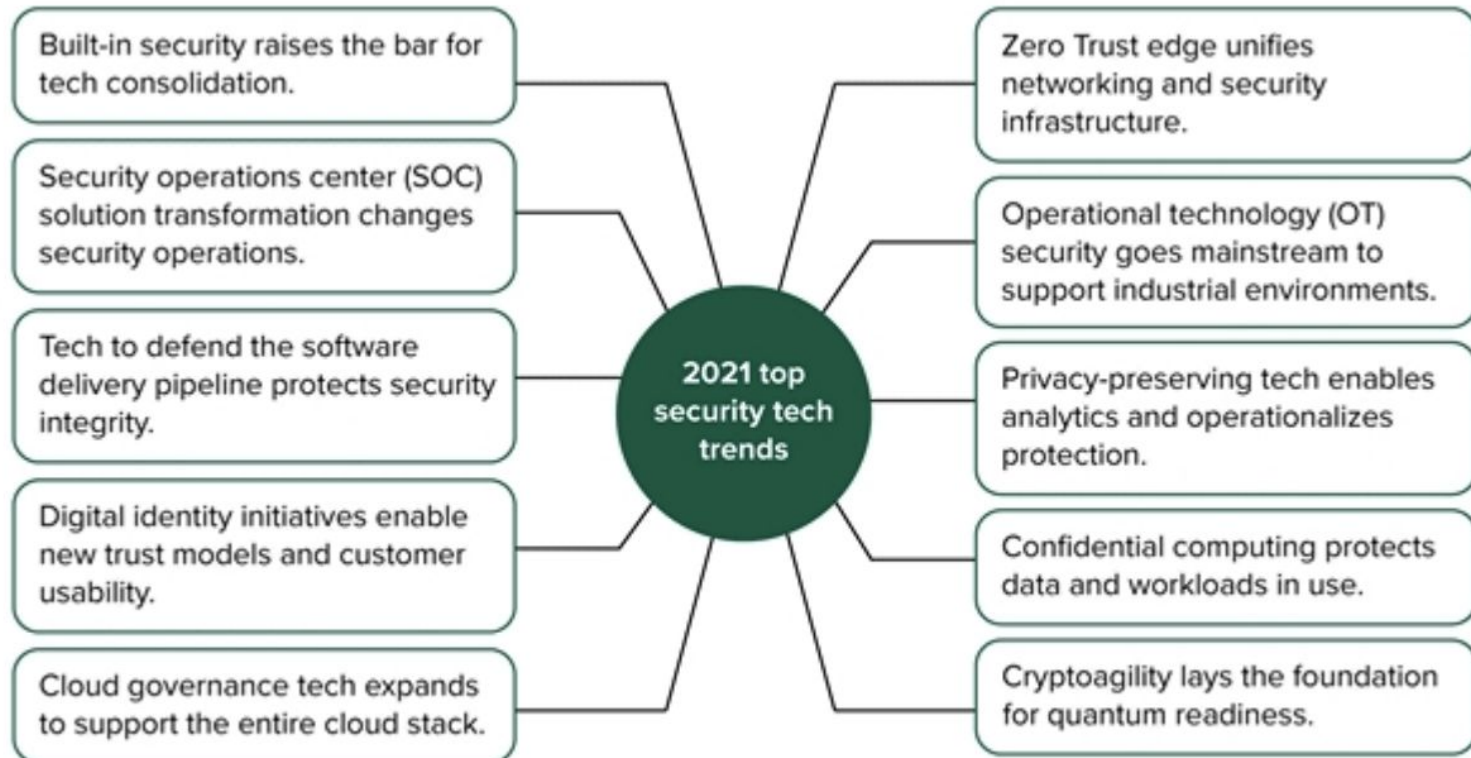
# What is EDR, MDR, and XDR?



Why do organizations  
NEED  
XDR?



Figure 1: 2021 Top Security Tech Trends



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.



**Which solution is ideal for my organization?**

# Elastic Wins XDR!



**Provides native prevention on critical assets:  
endpoint and cloud**



**Correlates telemetry across data sources into a single  
alert/incident**



**Uses security analytics to automate root cause analysis**



**Automates native response actions into workflows**



**Enables tool, workflow, and vendor consolidation**



**Simplifies purchasing and pricing**



## Innovation & Validation

### Gartner

Elastic named a Challenger 2021 Gartner Magic Quadrant™  
for Insight Engines, 2021

Elastic named a Visionary 2021 Gartner Magic Quadrant™  
for Application Performance Monitoring, 2021

Elastic named a Niche Player 2021 Gartner Magic Quadrant™  
for Security Information and Event Management, 2021

### FORRESTER®

Elastic named a Leader  
The Forrester Wave™: Cognitive Search, Q3 2021

Elastic named a Contender  
The Forrester New Wave™: XDR, Q3 2021

Elastic named a Strong Performer  
The Forrester Wave™: EDR, Q2 2022



elastic

**CYBERSECURITY  
BREAKTHROUGH  
AWARD  
2022**

**THREAT INTELLIGENCE  
PLATFORM OF THE YEAR**



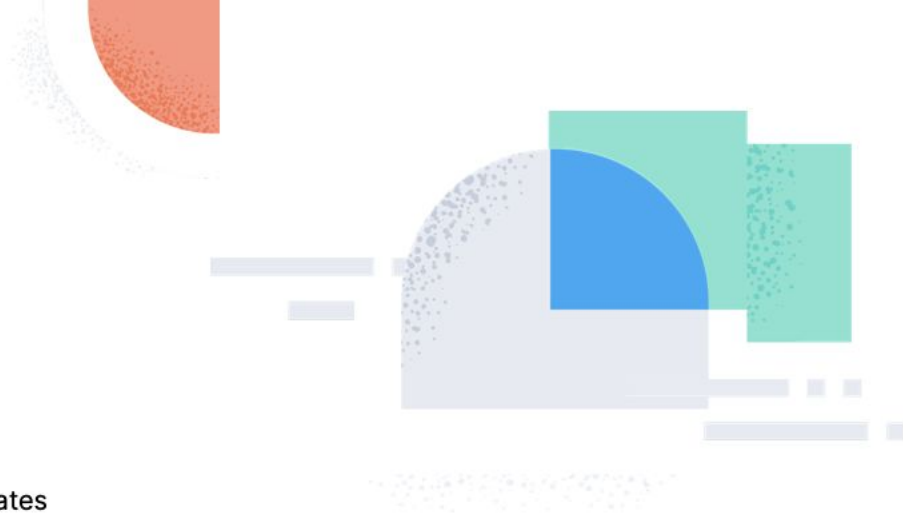


U.S. AIR FORCE

Hill Air Force Base

# Hill Air Force Base monitors and secures a geo-dispersed data center

Hill Air Force Base improves compliance practices that translates into superior security and more efficient secOPS processes with Elastic



## PROFILE

**About:** The Hill Enterprise Data Center (HEDC) provides a hosting service within Hill Air Force Base

**Industry:** Public Sector

**Location:** USA

## GOALS

- Collect, monitor, and analyze the logs from more than 100 information systems and its supporting infrastructure
- Provide near real-time continuous RMF compliance monitoring at the scale of a multi-tenant hosting platform

## SOLUTIONS

- **Elastic Cloud Enterprise** delivers logging and DoD compliance monitoring for the life-cycle of hosted information systems as an integrated service within the HEDC PaaS

## RESULTS

- Provides a scalable enrichment layer using **Logstash**
- Able to gather and aggregate logs for each unique hosted information system without inappropriately exposing information

[Watch customer video](#)



# Solving Cybersecurity Issues and Increasing Diversity in Security

“Elastic and MISI together are helping the manufacturing industrial base become cyber resilient.”

– Armando Seay, Cofounder

## PROFILE

**About:** A nonprofit that helps organizations accelerate the discovery of viable cybersecurity and related technologies

**Industry:** Public Sector

**Location:** USA

[Read customer story](#)

## GOALS

- Rapid fire capability
- Finding a configurable platform that is always innovating
- Extend stability

## SOLUTIONS

- Utilized **Elastic Stack** and **Elastic Security** to build out their MSSP offerings, accelerating the detection and mitigation of threats and increasing the stability, efficiency, and resiliency of mission-critical services for their agency partners

## RESULTS

- Matured their ability to accelerate Department of Defense suppliers to comply with regulations
- Network reconnaissance in a cost effective and efficient way
- Accelerated the process of becoming cyber resilient



**Thank You**  
**Search. Observe. Protect.**

---