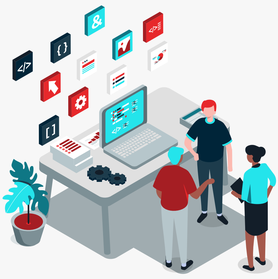
EASM vs DRP vs TI: What's the Difference?

EASM, DRP, and TI are separate, but complementary, elements of a comprehensive external cybersecurity program. When combined, they form a powerful, practical framework for external cybersecurity.





External Attack Surface Management

External Attack Surface Management (EASM): Identifies and mitigates risks associated with external digital assets and presence, such as public-facing websites and online platforms.

> **Key Benefit:** Understands and manages risks presented by digital assets visible from outside an organization's network, providing insights into external threats from the eyes of an adversary.

Digital Risk Protection

Digital Risk Protection (DRP): Encompasses proactive strategies and practices to secure digital assets against a myriad of risks that can emerge in the digital domain.

> **Key Benefit:** Plays a crucial role in safeguarding an organization's digital assets and reputation, especially during periods of extensive digital transformation.





Threat Intelligence

Threat Intelligence (TI): Collects, analyzes, and disseminates information from a variety of sources about current and potential threats.

> **Key Benefit:** Allows organizations to stay ahead of emerging threats, enabling them to update their security strategies in real time.

How EASM, DRP, and TI Work Together

1. EASM provides a clear picture of an organization's external exposure, identifying everything from publicly accessible systems to online brand presence.
2. Next, DRP applies proactive measures to safeguard assets from emerging digital risks. This includes monitoring for data leaks or breaches and ensuring compliance with data protection regulations.
3. TI then complements these efforts by offering real-time intelligence about potential and active threats, informing an organization about the methods and targets of cyber attackers.



Learn more about building an all-in-one framework for external cybersecurity at zerofox.com/easm-resources.