SOLUTION BRIEF

Armor XDR

Detect, respond and correlate across your environment to identify threats

Managed detection and incident response

XDR, or extended detection and response, extends endpoint and network detection and response to correlate log event and telemetry data from across your environment to deliver comprehensive security insights to detect even the most advanced threats.

Integrate custom log events and telemetry

Armor XDR includes deployment and configuration of a cloud-native security information and event management (SIEM) solution. Integrations can include ingesting the logs and telemetry data as well as integrating with a system's API to perform automated tasks.

Detect malicious behavior with continuous updates

Armor provides a library of advanced detection and correlation rules that are designed to run on your SIEM platform. These rules can detect:

- Basic indicators
- Behavioral anomalies
- Advanced Persistant Threats (APTs)

Prioritise with threat intelligence and data enrichment

XDR subscribers receive curated feeds of threat intelligence data that integrate into their SIEM platform using the standard STIX/TAXII protocol. Armor also utilizes multiple data sources including static databases and on-demand datasets.

Save time with unparalleled automation

Armor includes standard SOAR automations and integrations such as notifications and ChatOps, and can work with you to build custom automations that will address security workflow bottlenecks.

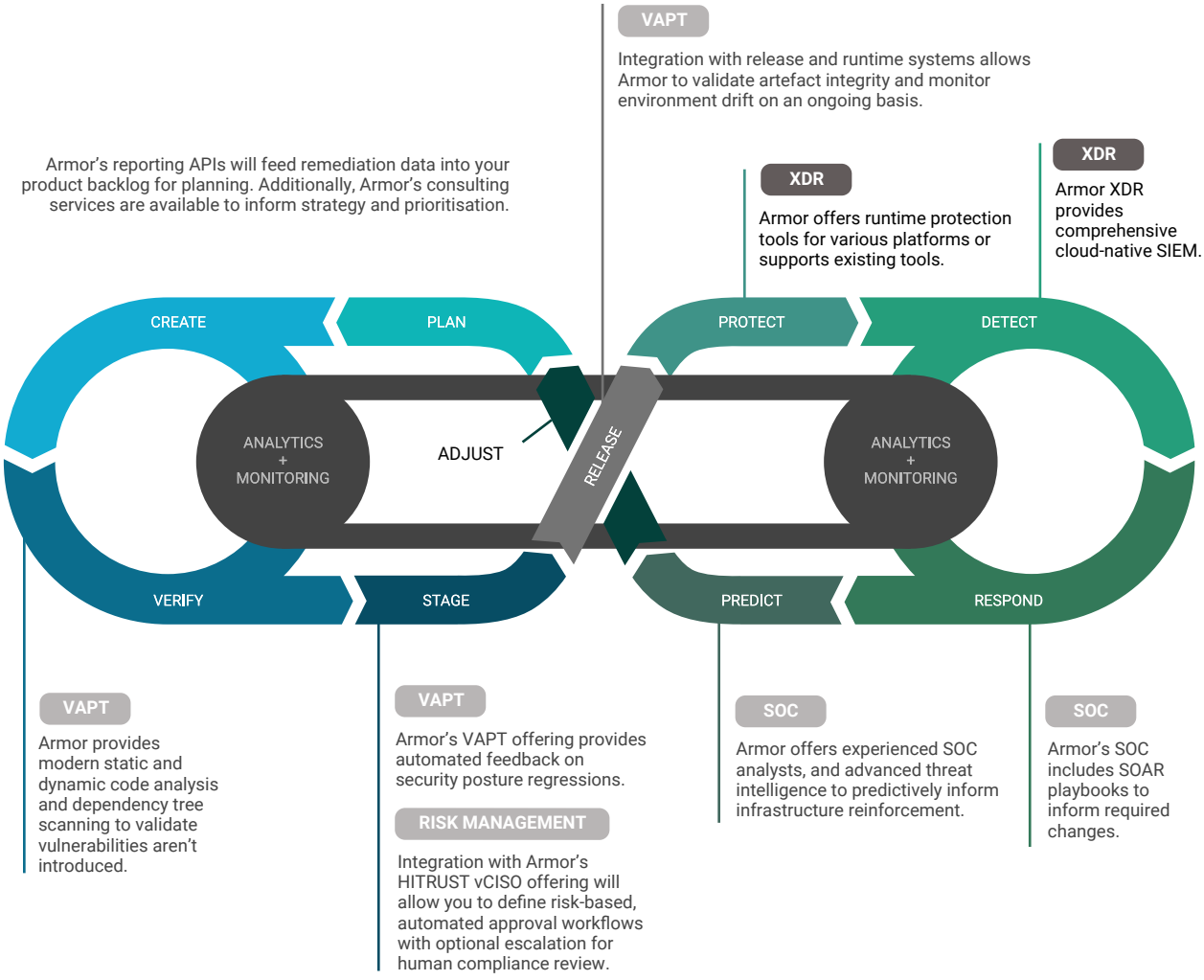
Why Armor XDR?

- Realize performance and cost savings with cloud-enabled security
- Eliminate vendor lock-in if you decide to cancel after your initial term
- Utilize a single platform to reduce complexity and increase visibility to investigate threats
- Respond faster by tracking activities and detecting attacks at any layer
- Future-proof your DevOps workflows by integrating security with our reference architecture and infrastructure code
- Navigate any environment complexity with flexible and customizable platform

Standalone and full-service options

Our XDR solution is available as a standalone subscription, but is typically combined with our SOC solution (collectively XDR+SOC) to ensure that incidents generated by the XDR solution are properly investigated and remediated.

Armor XDR is a key component of Armor's overall security portfolio



Armor XDR features

ARMOR RULE LIBRARY

Subscribers get access to Armor's library of correlation, alerting, and threat-hunting rules.

ARMOR DASHBOARD LIBRARY

Includes Armor's default security dashboards and widgets that you can customize.

CUSTOM RULES AND TUNING

For Professional and Enterprise subscribers, in addition to our default library, Armor will work with you to build custom rules to meet your specific requirements.

CUSTOM MANAGED DASHBOARDS

For Professional and Enterprise subscribers, Armor will align with your teams to determine the critical security KPIs for your organization and create dashboards to highlight these insights.

SOAR INTEGRATION

Leverage out-of-the-box integrations with popular SOAR platforms.

OPEN SOURCE FEEDS

Integrates a list of open sources threat intelligence feeds curated by Armor.

CUSTOM THREAT INTELLIGENCE

For Enterprise subscribers, bespoke threat intelligence program with analysts dedicated to monitoring trends and activities directly related to your organization.

COMMERCIAL FEEDS

For Professional and Enterprise subscribers, along with open source feeds, your logs will be enriched and correlated using a list of commercial threat intelligence feeds.

About Armor

Armor is a global leader in cloud-native managed detection and response. As a trusted partner to more than 1,500 firms in over 40 countries, Armor offers cybersecurity and compliance consulting, professional services, and managed services. Armor's industry-leading experts leverage non-proprietary frameworks and a 24/7/365 SOC to be the de facto standard that cloud-centric customers trust with their risk.

Contact us

https://www.armor.com/company/contact

For a free cyber health check

https://www.armor.com/forms/cyber-health-check

For more information

(US) +1 877 262 3473 **(UK)** +44 800 500 3167

