ARMOR DYNAMIC THREAT BLOCKING (DTB)

Armor dynamic threat blocking enhances our Armor Anywhere managed security-as-a-service (SECaaS) to block communication with malicious IP addresses at any layer of your security stack.

Organizations are under constant threat from a barrage of scans and attacks delivered across IP traffic, ranging from botnet attacks to phishing to crypto-jacking attempts. As if that were not enough, systems inside the environment may already be communicating with a suspect IP address. Without access to IP blacklists that capture critical information on suspected malicious IP addresses, prevention becomes a daunting challenge.

IT security teams need access to threat intelligence on known and suspected malicious IP addresses that can enhance their efforts at preventing many of the threats hitting their network defenses every day. Further, the ability to integrate threat intelligence on malicious IP addresses into existing workflows and orchestrate automated response actions will help organizations reduce the burdens associated with maintaining white- and blacklists, while heightening security.

STOP ATTACKS BEFORE THEY HAVE AN IMPACT

DTB is a cloud-based IP reputation management (IPRM) service designed to allow security teams to assess and automatically block both incoming and outgoing malicious IP traffic at any layer of their security stack. Through the service, customers get access to Armor threat intelligence available on suspect IP addresses to expand and streamline their blacklisting and whitelisting efforts.

API-DRIVEN, MULTI-LAYER CONNECTIVITY

Armor DTB makes automating your whitelisting and blacklisting efforts easy through our available API. Unlike other IPRM services, you can use the API to provide enhanced and automated protection against malicious IP addresses by connecting Armor's DTB service to your other security appliances, such as network and web application firewalls (WAF), or connecting directly to your hosts and applications. Integrate the service with any security operations center (SOC) workflow and tools to quickly validate threats as a dynamic part of your security stack.

PAY ONLY FOR WHAT YOU USE

Instead of paying for expensive threat services that have high integration costs with drawn out timelines and an annual contract, DTB allows you to pay only for what you use.

DYNAMIC THREAT BLOCKING IN ANY ENVIRONMENT

Armor's DTB service allows you to identify and actively block threats—even in the cloud—before they can enter your environment, saving your team valuable time when investigating and responding to each potential threat.

AUTOMATED BLOCKING OF THREATS

Armor DTB provides enhanced threat detection to automatically stop inbound and outbound communications to suspect IP addresses for your on-premise, cloud, and hybrid IT environments.

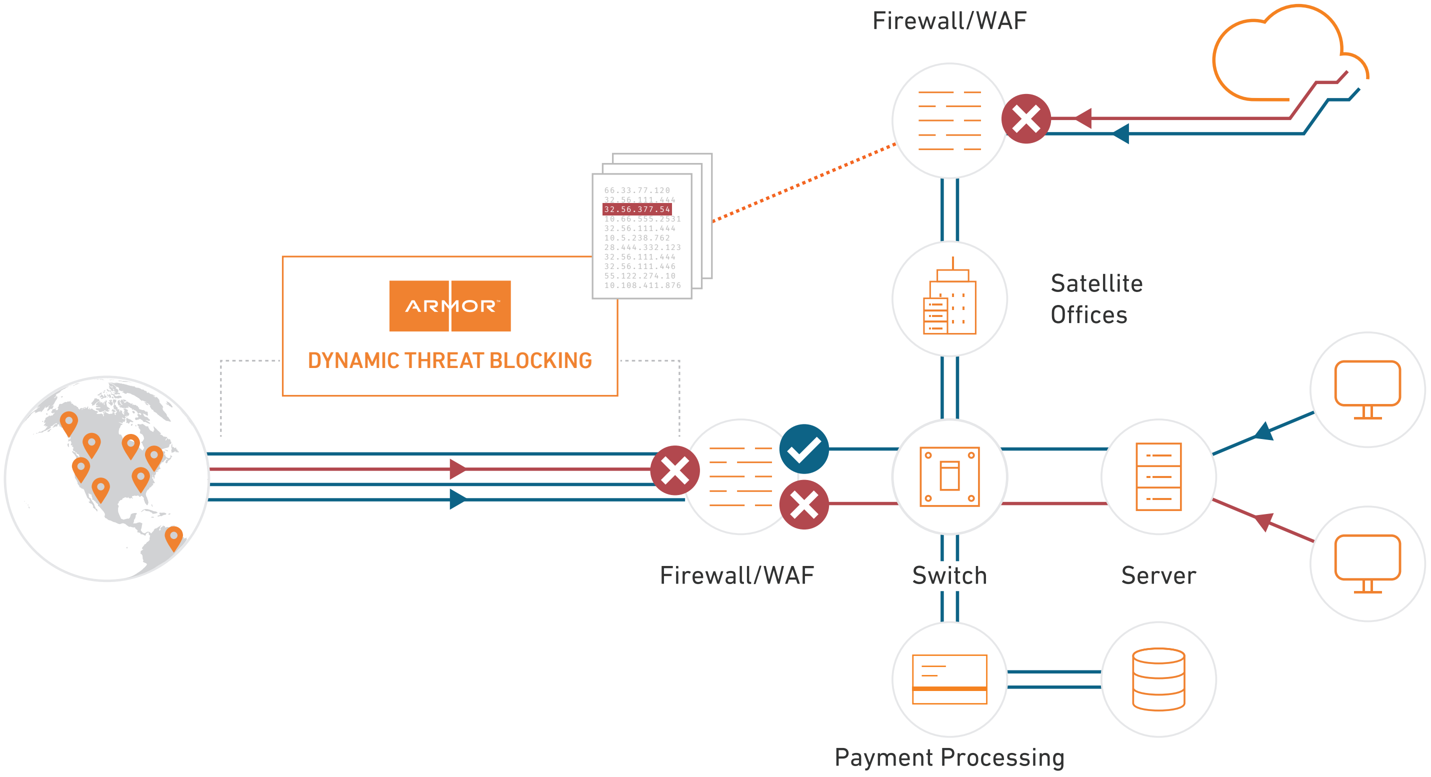
ACCESS TO ARMOR THREAT INTELLIGENCE

Get access to ongoing threat intelligence on suspect IP addresses—amassed and curated by the Armor Threat Resistance Unit (TRU)—to aid in your blacklisting and whitelisting efforts.

SIMPLE INTEGRATION, EXTENSIVE INTEROPERABILITY

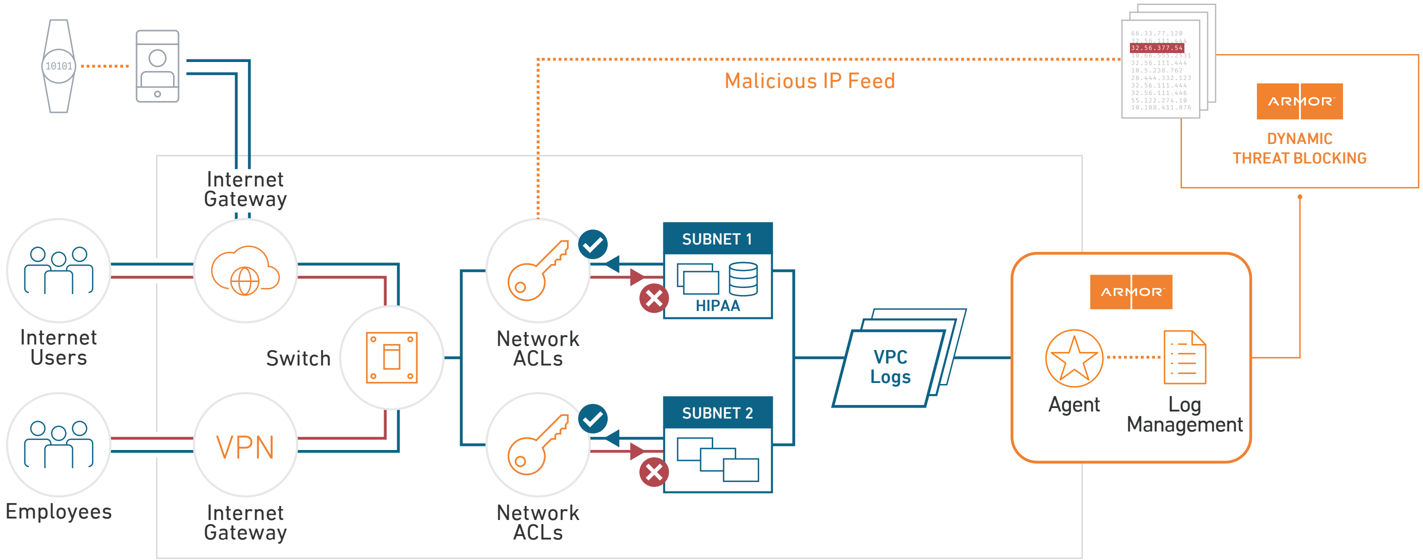
Using Armor's API, you can easily integrate Armor DTB to enhance protections for your WAFs, firewalls, applications, and hosts, among others.

DYNAMIC THREAT BLOCKING FOR YOUR ON-PREMISE ENVIRONMENT



A financial services firm needs to protect cardholder and financial asset information for its customers. With Armor DTB, the firm gets an additional layer of protection against incoming and outgoing traffic tied to malicious IP addresses. This protection works to identify cardholder transaction attempts tied to a suspect IP address and blocks their connection, stops suspect communications to the firm's other business entities and satellite offices, and monitors for outgoing communications to malicious IP addresses from systems within the environment.

DYNAMIC THREAT BLOCKING FOR YOUR CLOUD WORKLOADS



A software-as-a-service (SaaS) technology provider to the healthcare industry needs to protect its core application offering deployed in AWS from attacks. The application includes a transaction engine that touches patient data for a wide base of customer organizations. With DTB in place via Armor API, the SaaS provider can dynamically identify incoming suspect IP addresses and block them before they can have any impact on the application. The provider gets enhanced protection from threats, beyond its own capabilities at its edge, to block malicious IP addresses with no manual intervention required by staff resources.

ARMOR DYNAMIC THREAT BLOCKING DELIVERS TRUSTED, COST-EFFECTIVE SECURITY:

- Enhance protection against malicious IP addresses powered by Armor threat intelligence
- Unify protection through correlation of event information with other security controls under management by Armor
- Pay only for what you use
- Get access to time-tested security and compliance experts monitoring your environment 24/7/365

HOW IT WORKS

The Armor DTB service applies Armor's threat intelligence and an extensive database of malicious IP addresses to strengthen your security defenses. Using Armor's API, integrate protection from malicious IP addresses at the network, host, or application layer to enhance your whitelisting/blacklisting efforts while reducing the burden on your team to collect and investigate suspicious IP addresses.

POWERED BY SPARTAN

Armor DTB is powered by Spartan, the industry's leading threat prevention and response platform. Spartan integrates advanced analytics, global threat intelligence, and continuous response capabilities into a single solution that bolsters your defenses, uncovers hidden threats, and prevents security breaches.

aws

Google Cloud

PRIVATE CLOUD

HYBRID CLOUD

OTHER CLOUDS

ON-PREMISE INFRASTRUCTURE

PROTECT YOUR NETWORK, HOSTS, AND APPLICATIONS FROM MALICIOUS IP ADDRESSES, ANYTIME, ANYWHERE.

Armor DTB is designed to allow security teams to access, investigate, and automatically block both incoming and outgoing malicious IP traffic at any layer of their IT ecosystem.