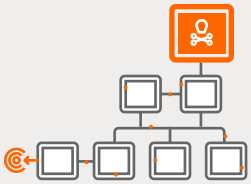
Intrusion Detection Systems (IDS)

Intrusion Detection Systems represent a critical security control to monitor your environment for potential threats that get past traditional firewall solutions. However, IDS systems can generate a significant and at times, overwhelming number of alerts for smaller security teams, making it difficult to keep up. In addition, event data from stand-alone IDS products may not be correlated with other security infrastructure present in the environment to reveal a broader pattern of indicators or behavior that may suggest a potential threat.

Armor provides these Intrusion Detection security management solutions



NETWORK-BASED INTRUSION DETECTION

Available through Armor's secure hosting solutions, the Armor Network-based Intrusion Detection System service provides 24/7/365 management and monitoring of your network traffic to identify potential malicious and anomalous behavior such as buffer overflows, stealth port scans, CGI attacks, SMB probes and OS fingerprinting.

HOST-BASED INTRUSION DETECTION

Available for on-premise and cloud environments, Armor's Host-based Intrusion Detection System service is managed and monitored 24/7/365 to provide security protections where they are needed most – on your servers and instances. With visibility to inbound and outbound activity at the host as well as activities taking place on the host, Armor's IDS service provides versatile and robust protection for your servers, Virtual Machines and cloud workloads.

1 Advanced Threat Detection

Armor IDS services provide advanced detection capabilities to analyze traffic across your network and hosts, monitor resident applications for unusual activity, identify installations of unwanted applications, and look for rogue processes taking place that indicate the presence of a threat.

2 Advanced Analysis and Correlation

IDS events are analyzed and correlated with event data from your other devices under management by our Spartan threat prevention and response platform, delivering enhanced detection of potential threats across your cloud, on-premise, hosted and hybrid environments.

3 Audit-ready Compliance

Network-based and Host-based IDS capabilities help you meet key controls for major compliance mandates such as PCI DSS, GDPR, HIPAA, and HITRUST.

4 Response that Goes Beyond Alerting

Unlike traditional MSSPs, Armor goes beyond simple IDS alerting and helps you identify when a single intrusion event could be part of a broader security incident. Our SOC analysts monitor your environment 24/7/365 while they also work closely with your team to investigate and respond to potential incidents.

Intrusion Detection System (IDS) - How It Works

NETWORK-BASED IDS

Catch threats targeting your systems through signature-based threat detection. Network intrusion detection provides real-time inspection of HTTP (port 80) network traffic that has passed through the Armor Complete perimeter for malicious and anomalous behavior. Armor uses custom signature-based policies to monitor network traffic. All traffic is subject to packet logging and traffic analysis. Through protocol analysis, content searching and matching, Armor can detect a variety of attacks and probes such as buffer overflows, stealth port scans, CGI attacks, SMB probes and OS fingerprinting.

HOST-BASED IDS

With visibility to inbound and outbound activity at the host, Armor inspects anomalous traffic against predefined policies – detecting attacks like generic SQL injections, generic XSS attacks, DoS and generic web app effects. This service provides an agent-based Intrusion Detection System on the installed host for network traffic analysis and reporting on activities taking place on the host based around policies defined by Armor.

ARMOR INTRUSION DETECTION DELIVERS TRUSTED SECURITY:

- Unify protection across your cloud, on-premise, hybrid and hosted environments through correlation of IDS events with other security controls under management
- Go beyond simple alerting to also get help responding to potential incidents
- Get access to battle-tested security and compliance experts monitoring your environment

TURN UP ARMOR INTRUSION DETECTION FOR PROTECTION OF YOUR ON-PREMISE, CLOUD AND HOSTED WORKLOADS.

POWERED BY SPARTAN

Armor Intrusion Detection (IDS) services are powered by Spartan, the industry's leading threat prevention and response platform that outthinks and outpaces threats at the speed of cloud. 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. Customers can tap into the power and value of Spartan through the Armor Management Portal.

GET CRITICAL PROTECTION ACROSS YOUR HOSTS IN ANY ENVIRONMENT

Armor Intrusion Detection services inspect traffic across your network (network-based), and to and from your hosts (host-based) while validating that activities taking place on your hosts are within acceptable norms. All security events are analyzed and correlated through Spartan, and alerts further investigated by our Security Operations Center.

ARMOR™