VULNERABILITY SCANNING

The pressure is on. Businesses must embrace digital change to remain relevant and to set the stage for future growth. Meanwhile, cybercriminals continue to up their game and create risk to businesses and their digital efforts. From personal health records to intellectual property and credit card numbers, they're stealing valuable data, leaving the breached organization facing extreme consequences.

While regulatory compliance doesn't guarantee security, it's a critical step in reducing the risk of cyberattacks. Vulnerability scanning makes the often complex and daunting process of compliance easier.

Armor partners with approved scanning vendor (ASV), Rapid7, to deliver a vulnerability scanning service. This service helps customers navigate the complexities of compliance, bolster security, and reduce risk. Developed and used by auditors, the vulnerability scanning service can help you achieve PCI DSS and HIPAA compliance.

DEFENSE-IN-DEPTH & PROACTIVE SCANNING

Integrated with Armor Anywhere and Armor Complete solutions, Armor vulnerability scanning scans for application vulnerabilities that may introduce the risk of a breach.

GAIN FULL VISIBILITY OF YOUR ECOSYSTEM

Continuously identify and assess risk across your cloud, on-premise and hybrid IT infrastructure. Armor provides visibility through the Armor Management Portal (AMP), helping you confidently understand and prioritize the risks that affect your entire ecosystem.

BREAK DOWN THE SILOS OF IT, SECURITY & DEVOPS

Enable collaboration with IT operations and developers so that vulnerabilities of all kinds are identified and patched quickly and seamlessly.

DON'T BE BLINDSIDED

Take command of your risk assessments and secure your applications.

Customers have the option to assess technical vulnerabilities of external and internal networks to mitigate risk and meet compliance requirements. The Armor management portal (AMP) scanning console allows our customers to manage their scans and vulnerability reports.

BENEFITS INCLUDE:

- Identify potential vulnerabilities both inside and outside of your devices
- Search networks and applications for vulnerabilities that could result in identity theft, credit card fraud, spam, and malware
- Quickly and easily comply with industry-specific requirements and internal compliance processes

ARMOR

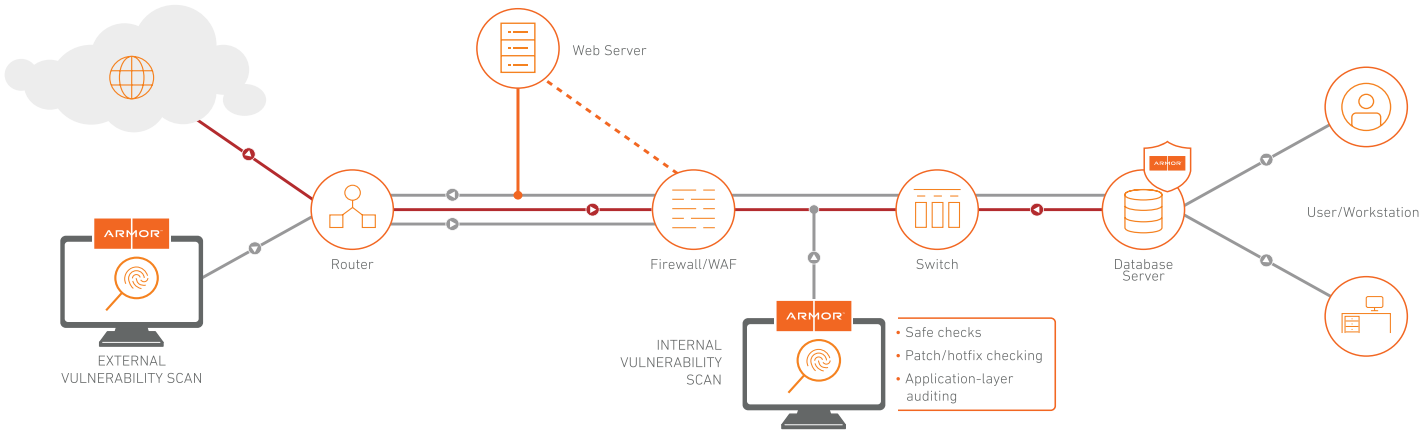
COMPLIANCE & SECURE CONFIGURATIONS, WITHOUT THE HEADACHES

Show auditors how your environment has changed over time, demonstrating how you're compliant with PCI DSS, HIPAA/ HITECH, and CIS standards for risk and vulnerability management.

HOW DOES IT WORK?

An external vulnerability scan looks for gaps in your network firewalls, where malicious threat actors can infiltrate and attack your network. In contrast, an internal vulnerability scan operates inside your organization's environment to identify real and potential vulnerabilities.

Armor provides these security management solutions:



Armor Vulnerability Scanning service delivered via the Armor Anywhere agent, automatically assesses risk across your entire infrastructure and includes:

- Live Dashboards
- Real Risk Prioritization
- IT-Integrated Remediation Projects
- Cloud, Virtual, and Container Assessment
- Integrated Threat Feeds
- Easy-to-Use RESTful API

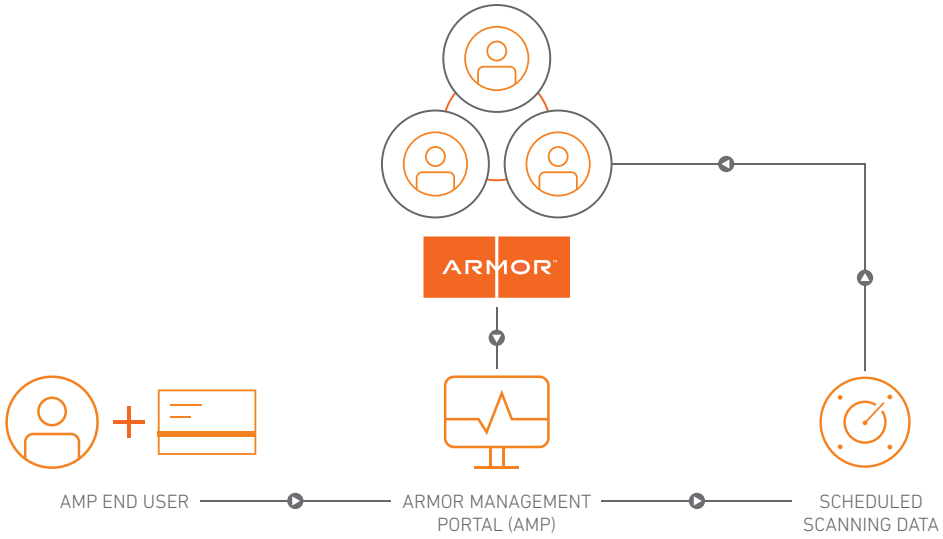
Vulnerability Scanning is provided as part of Armor's Armor Anywhere security-as-a-service solution and integrated into the Anywhere agent. Local scans are performed on the installed asset that report vulnerability, patching, and compliance results. You can review the scan results through the Armor Management Portal (AMP). The External Vulnerability Scanning service is available for Armor Anywhere protected instances that are publicly available on an individual request basis via the Armor Ticketing System offered with the AMP. You can schedule scanning times and view the schedules as well as view the output from scans through the Armor Security Dashboard. The agent collects the following types of data, compresses it, and submits it back to its cloud:

- Basic asset identification information
- Windows registry information
- File version and package information

The agent performs a "Full audit without Web Spider" scan. This full network audit uses only safe checks, including network-based vulnerabilities, patch/hotfix checking, and application-layer auditing.

MAINTAIN SECURITY POSTURE & COMPLIANCE

Armor does more than secure the network. Our experts monitor and secure your hosts, providing a defense in-depth solution that secures your operating system up to the application layer.



VULNERABILITY SCANNING

Vulnerability Scanning service enhances Armor's Armor Anywhere Managed security-as-a-service and Armor Complete Secure Hosting (Optional) solutions to provide complete security protection for your cloud, on-premise and hybrid workloads.

Click to learn more about Armor Anywhere or Armor Complete.

SHARED RESPONSIBILITY

Installation and management is a collaboration between the customer, Armor, and Rapid7. We have outlined the responsibilities for each party.

Responsibility Breakdown	Armor	Customer
Provisioning and Management of Vulnerability Scanning Service	X	
Availability of Vulnerability Scanning Service Portal	X	
Initial Configuration of Customer Account Details	X	
Subsequent Configuration of Environment Scan: Scope & Scheduling	X	X
Ongoing Scan Modification	X	X
Remediation of Detected Vulnerabilities	Upon Request	
Remediation of Detected Vulnerabilities & Disputes in Application	X	X
Review of Reports by Armor's Security Operations Team	Upon Request	
Application of Scan Reports to Customer Audit	X	X

POWERED BY SPARTAN.

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

Whether your sensitive data and workloads are stored in a private, public, or hybrid cloud—or in an on-premise IT environment—Spartan provides a proactive approach to cyberthreats. Customers can tap into the power and value of Spartan through the Armor Management Portal (AMP).

INSTALLATION

Armor is responsible for creating your organization's portal account and for providing credentials. Armor will also input all subscribed IP addresses into the portal. During installation, your team is responsible for completing their enrollment in the portal and for ensuring the accuracy of the configured IP addresses.

CONFIGURATION

Armor will update the list of IP addresses in the customer portal based on additions and subtractions to the list of IP addresses that are initiated by your team's actions (ordering new servers or decommissioning servers). Your team is responsible for configuring all scans, including the IP addresses to be part of any scan, the type of scan, and scan frequency.

ADMINISTRATION

The ASV and the client share responsibility for the administration of this service. That includes maintaining the portal and important information pertaining to upcoming scans.

REPORTING

You will be provided email-based notifications in advance of scheduled scans as well as the status of the scan once completed. Scan reports will be available in the portal for you to view and download. In addition, Armor will receive scan results for all subscribed customers. This information can be used to assist with remediation and appeals initiated by the customer.

LEARN MORE

For Armor Anywhere customers, the service runs and is fully supported on AWS, Azure, Google Cloud Platform, and Rackspace. The service is supported on all 5 Armor Complete datacenters (Amsterdam, Dallas, London, Phoenix, and Singapore) for Armor Complete customers.

Click to learn more about Armor Anywhere or Armor Complete.

OPTIMIZED FOR

aws Microsoft Azure Google Cloud vmware

ARMOR