

The Actionable Insight & Response Platform

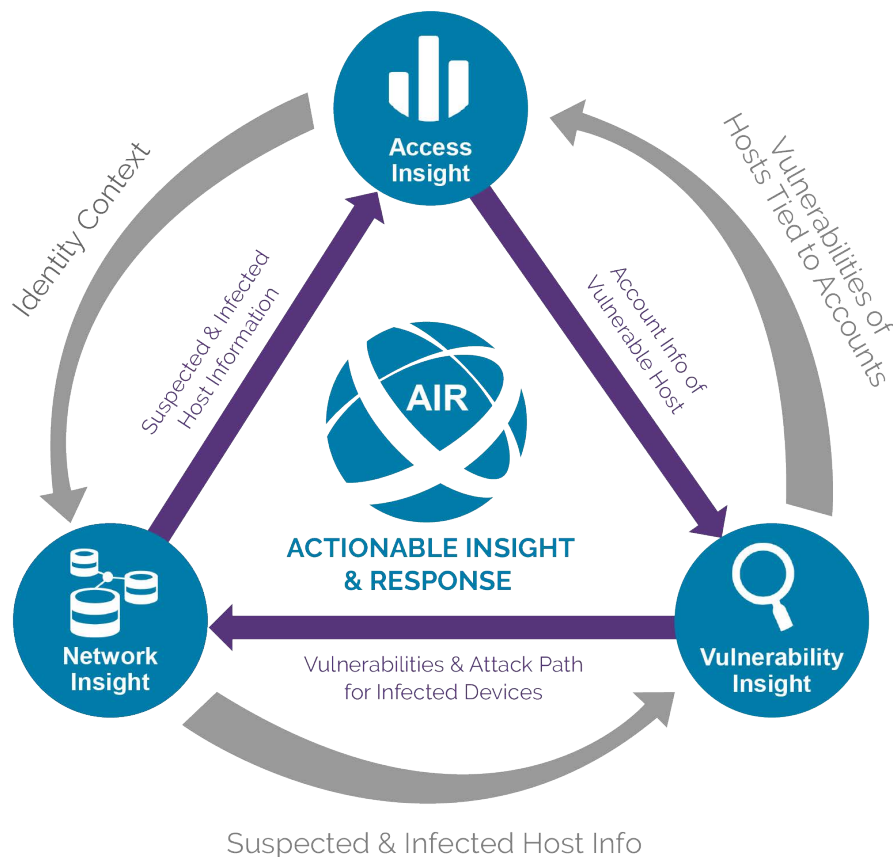
Benefits of Actionable Insight & Response Platform:

- **Continuous Monitoring:** The ability to monitor your devices, applications, infrastructure, and accesses holistically to understand every security risks
- **Comprehensive and Historic Visibility:** Provides context necessary to perform incident root cause analysis
- **Speed:** Empower you to act fast and minimize the impact of risk
- **Management Discipline:** Provides a governance process that will help you improve your security posture
- **Evidenced Prioritization:** Gives you a recommended prioritization plan to address immediate threats
- **Response:** Provides options to mitigate risk quickly with both manual and automated processes.

Enabling Security Professionals to Interpret, Prioritize and Act on Data

Everywhere you look you will find data, telling us everything. But do security professionals really know where and what to look for in order to find risk? Turning mountains of data into valuable, practical, actionable information is not as straightforward as people may think. First and foremost, there are a lot of raw data logs being collected, mostly across separate applications. In addition, most security solutions work in silos, which means for example- using one system for your organization's identity and access controls and other systems for your network and vulnerability data management. This not only leaves you with data overload but gives you a myopic view of your risks, as there is no way for you to understand the interdependencies and interrelationships of these disparate data sources. Secondly, you face the challenge that most information security departments face—not having enough people to go through the data, make sense out of it, identify the risks, and act on the information.

The Actionable Insight & Response Platform (AIR) can help solve these challenges. It breaks down the solution silos and provides a comprehensive view of your organization's high risk identities, their access to entitlements, suspicious and malicious network device activity and vulnerabilities. Moreover, it continuously prioritizes these risks for you so that you can focus on the most critical items and more efficiently use your team's time and resources. AIR is made up of three solutions – Access Insight, Network Insight, and Vulnerability Insight, all working together to help you continuously and comprehensively monitor and manage your risk.





Components of AIR

Core Access Insight resolves immediate threats by using big data analytics to continuously evaluate identity and access risk in your organization. By creating in-depth visually intuitive access heat maps, Core Access Insight provides a comprehensive, continuous view of the multi-dimensional relationships between identities, access rights, policies, resources, and activities across a multitude of enterprise systems and resources. This enables you to:

- Automatically Evaluate And Act Upon At-Risk Identities such as Orphaned & Abandoned Accounts
- Spontaneously Identify and Remediate Improper Access including Excessive & Nested Privileges
- Continuously Govern Risk, Eliminating 'Point In Time' Assessments
- Model Activity Patterns

Core Vulnerability Insight unifies, regulates, and prioritizes vulnerability management initiatives enterprise-wide. It consolidates multiple vulnerability scans across scanners, while matching known exploits and simulating attacks, enabling you to focus on the most vulnerable points of your network. This is combined with business prioritization rules as well as network topology to enable you to:

- Identify The Vulnerabilities That Matter
 - Consolidate and De-duplicate Vulnerabilities
 - Prioritize Using Configurable Risk Criteria & Determining Which Vulnerabilities are Exploitable
- Modeling How Actors Can Pivot & Move Laterally Inside Your Network - *"Think like an attacker."*
- Eliminate Attack Paths to Critical Assets & Validate Response Actions
- Leverage Flexible Reporting Options


Core Network Insight automatically and accurately identifies hidden infections in real time by analyzing live network traffic. When Core Network Insight confirms a device is infected by advanced persistent threats (APT) or malware, it terminates criminal communications and presents a full case of evidence, prioritized by risk – thus, no more chasing False Positives. It allows you to:

- Analyze Network Behaviors, Malicious Payloads and Threat Actor / APT Activity
- Pass information to an Automated Case Analyzer which Corroborates Evidence
- Verify True Positive Infections and Apply Risk-ranking
- Present Response Teams with Prioritized Workflow for Immediate Action

Bad actors are fast and sophisticated. With such powerful insight at your fingertips, you can prioritize your efforts to protect your businesses' critical assets and start remediation actions sooner, reducing the risk of an inevitable data breach or damage to your network.

The AIR Platform: Today AIR provides the collective visibility and prioritization security professionals need by customers combining the analytics and telemetry within Access Insight, Vulnerability Insight, and Network Insight. The AIR Platform is being implemented to bring the telemetry of any two or more Core products together to build a comprehensive analytics and response engine and interface for your security operations.

The AIR Platform will arm you with a continuous and comprehensive view of your security investments. It provides the ability to truly comprehend the situation and make timely and sound decisions by both helping you reduce your attack surface and automate the discovery of high risk conditions such as:

- Which Identities and Access Rights are At-Risk
 - If You Are In Compliance To Your Access and Vulnerability Policies
 - Which Vulnerabilities Actually Pose a Threat
 - How An Attacker Can Move Throughout Your Network
 - What Identities and Access Rights are Available To Attackers on At-Risk or Compromised Devices
 - Which Devices are Behaving in Suspicious or Malicious Ways
 - Where Hidden Compromises Exist in Your Network
 - Who is Attacking Your Company and How
- 

AIR Provides Enterprise Security Risk Governance:

- Continuously Monitor the Network for infected devices, the infrastructure and application landscape for any vulnerabilities, and accounts and privileges to better understand any access risks.
- Provide holistic visibility of both present security risks as well as historic risks as well to better learn over time where root causes might be. It also allows you to better understand how your security teams are performing with managing down the threat surface over time.
- Get the right information to make the right decisions and act on security risks to minimize any business loss or disruption that may be due to an inevitable breach or to be proactive to prevent possible loss by getting ahead of the security risks before anything happens.
- Provide a governance process and the management discipline with KPIs to understand how you are performing as a security organization and where you can continue to improve over time.
- Provide data and evidence to support a recommended prioritization plan to remediate and address security risks.



Learn More

To learn more about Actionable Insight and how it can help your organization get a more holistic view of your information security, contact us at (678) 304-4500 or info@coresecurity.com.

ABOUT CORE SECURITY CORPORATION

Core Security provides companies with the security insight they need to know who, how, and what is vulnerable in their organization. The company's threat-aware, identity & access, network security, and vulnerability management solutions provide actionable insight and context needed to manage security risks across the enterprise. This shared insight gives customers a comprehensive view of their security posture to make better security remediation decisions. Better insight allows organizations to prioritize their efforts to protect critical assets, take action sooner to mitigate access risk, and react faster if a breach does occur.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com.

blog.coresecurity.com | p: (678) 304-4500 | info@coresecurity.com | www.coresecurity.com

Copyright © 1996-2017 by Core Security Corporation. All Rights Reserved. The following are trademarks of Core Security Corporation "Core Impact", "Core Vulnerability Insight", "Core Password", "Core Access", "Core Provisioning", "Core Compliance", "Core Access Insight", "Core Mobile Reset", and "Think Like an Attacker". The following are registered trademarks of Core Security Corporation "WebVerify", "CloudInspect", "Core Insight", and "Core Security". The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The names of additional products may be trademarks or registered trademarks of their respective owners.

