ARC4DIA

Cyber Defense

SNOW FACT SHEET

What is SNOW?

Developed by cyber specialists from the Canadian national security community and some of the top minds in the cyber security world, SNOW is ARC4DIA's proprietary cyber defense platform and one of the most comprehensive solutions on the market today. No other cyber security platform offers the same capabilities, reach, and scope.

Operating on a managed platform that proactively searches through networks 24/7 to detect and respond to Advanced Persistent Threats (APTs), SNOW's next-gen technology combines enhanced detection mechanics with a robust suite of constantly evolving analysis tools, offering the most extensive endpoint protection.

How does SNOW work?

- SNOW uses a host-based sensor which works across multiple platforms enabling it to assimilate the information it receives from different sources.

- SNOW seamlessly integrates with an enterprise's existing cyber-defence network, protecting all endpoints to ensure there are no gaps for cybercriminals to penetrate. Enterprises do not need to change their infrastructure or existing products.

- ARC4DIA's team of experts monitors the networks and collects data in real-time looking for suspicious activity. All of the information is then sent back to the central cloud for analysis. On watch 24/7, the company's highly skilled investigators ensure there are no "down" moments for hackers to take advantage of.

Why SNOW is the smarter choice

- SNOW is the only solution to exclusively operate in the background – its existence is hidden from view to avoid detection from intruders on a network. This also enables ARC4DIA's investigators to constantly analyze and change their footprint in order to stay one step ahead, and ensure intruders cannot adapt to their techniques.

- Unlike competitors, SNOW has hunt capabilities that offer system-level watchdog services that can sense, and detect malicious hackers from stopping or pausing a system's sensors. Hackers will often destroy sensors to get around the network, and move without observation. When a sensor is stopped or paused, SNOW triggers an immediate alert for ARC4DIA to move into action.

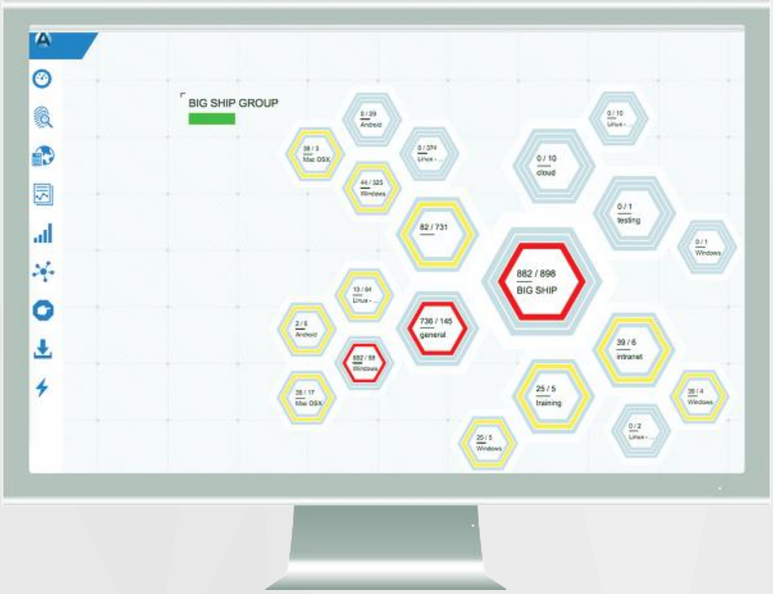
- SNOW is the only solution that can suspend threats (essentially freezing malicious components of software) for further analysis by remotely suspending threads, and processes.

SNOWboard

- SNOWboard is ARC4DIA's central command system, where all SNOW enabled devices are monitored, and client data is analyzed and stored.

- Clients are given access to SNOWboard via a live dashboard, where they receive immediate reports on threats that have been identified, as well as the actions taken to defend them.

- SNOWboard can identify multiple threats from different hackers, and has the ability to build a profile behind the attempted attack. This allows ARC4DIA to predict behaviours, and create better defenses against the intruder's next move.



Where can SNOW be deployed?

SNOW can be used across multiple systems including:

- Linux
  CentOS 5 & higher
  Ubuntu 12.04 & higher
  Debian 7 & higher

- Windows XP SP3 & higher

- Android 5.0 & higher

- Mac OS X 10.8 & higher

SNOW is mobile

ARC4DIA's SNOW solution offers an enhanced mobile security platform for complete coverage anytime, anywhere.

Here's why we are the best choice in mobile security:

Full Coverage - The only cyber defense solution covering system, and kernel security.

Centralized Threat Watch - SNOWboard command system monitors all mobile SNOW enabled devices.

Constant Integrity Monitoring - Continuous 24/7 network endpoint analysis against sophisticated attacks.

Cybersecurity Specialist Team - A group of highly skilled cyber security experts detect, analyse, and respond to threats.

Remote Forensic Analysis - Reverse engineer APTs from around the world.

Remote Response - APT and malware neutralization beyond geographical limits.

Virtual Private Network (VPN) for sensitive networking environments

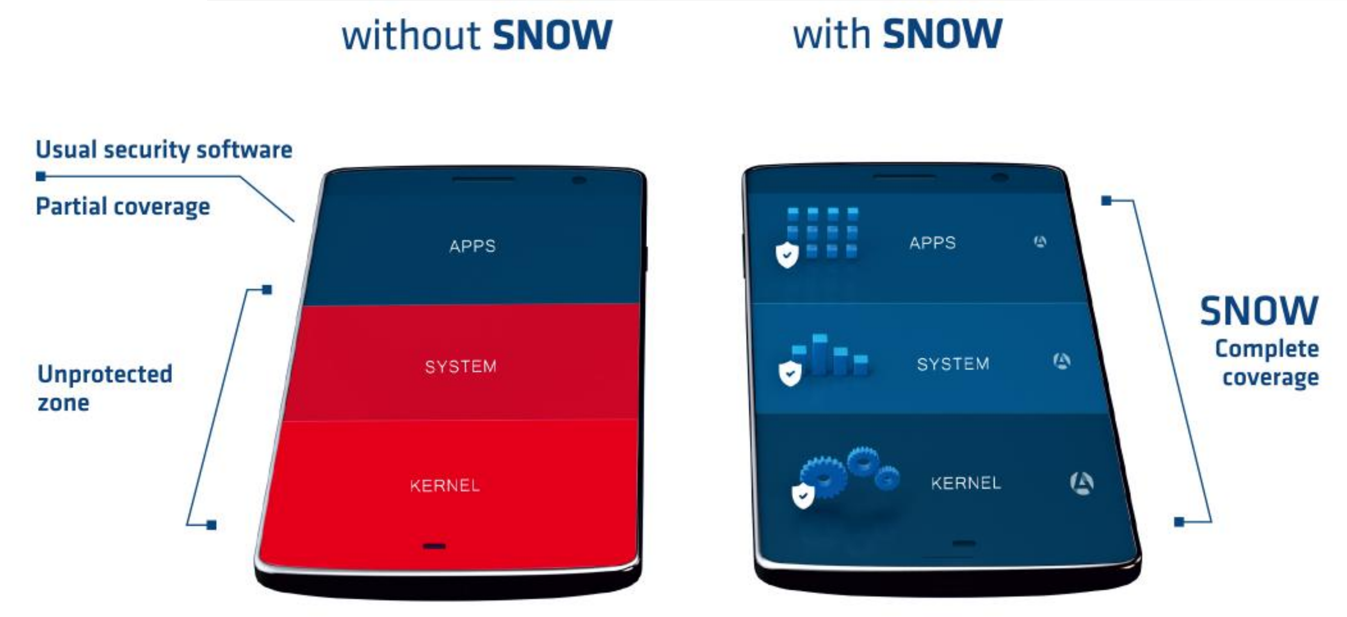
- Control channel: TLS, 2048 bit RSA keys with SHA-256 certificates, AES-256 + HMAC-SHA1
- Data channel: AES-128 + HMAC-SHA1
- A secure, encrypted connection is provided which makes the device invisible on a Wi-Fi network with unreadable data. The VPN also blocks tracking attempts to provide anonymous browsing while scanning for malware, tracking cookies and sites, as well as trackers and apps that want to forward data without consent.

Secure Voice & Text Communications

Provides encrypted end-to-end (using Curve25519, AES-256, and HMAC-SHA256) data communication which prevents data travelling between parties from being read or tampered with by unintended recipients.

Customized Android Operating System (Cyanogen) with enhanced privacy features (Privacy Guard), compatible on the following devices:

- Samsung Galaxy S7 Edge
- OnePlus One
- OnePlus Two
- Nexus 9P
- Google Nexus 5X
- Google Nexus 6P


without SNOW
with SNOW
Usual security software
Partial coverage
Unprotected zone
APPS
SYSTEM
KERNEL
APPS
SYSTEM
KERNEL
SNOW
Complete coverage