

2013 DHS S&T/DoD ASD (R&E)  
CYBER SECURITY SBIR WORKSHOP

# Enabling Technologies for Proactive Cybersecurity

AVIRTEK

Salim Hariri, Founder and CEO

*July 24, 2013*



Homeland  
Security

Science and Technology



# Company Profile

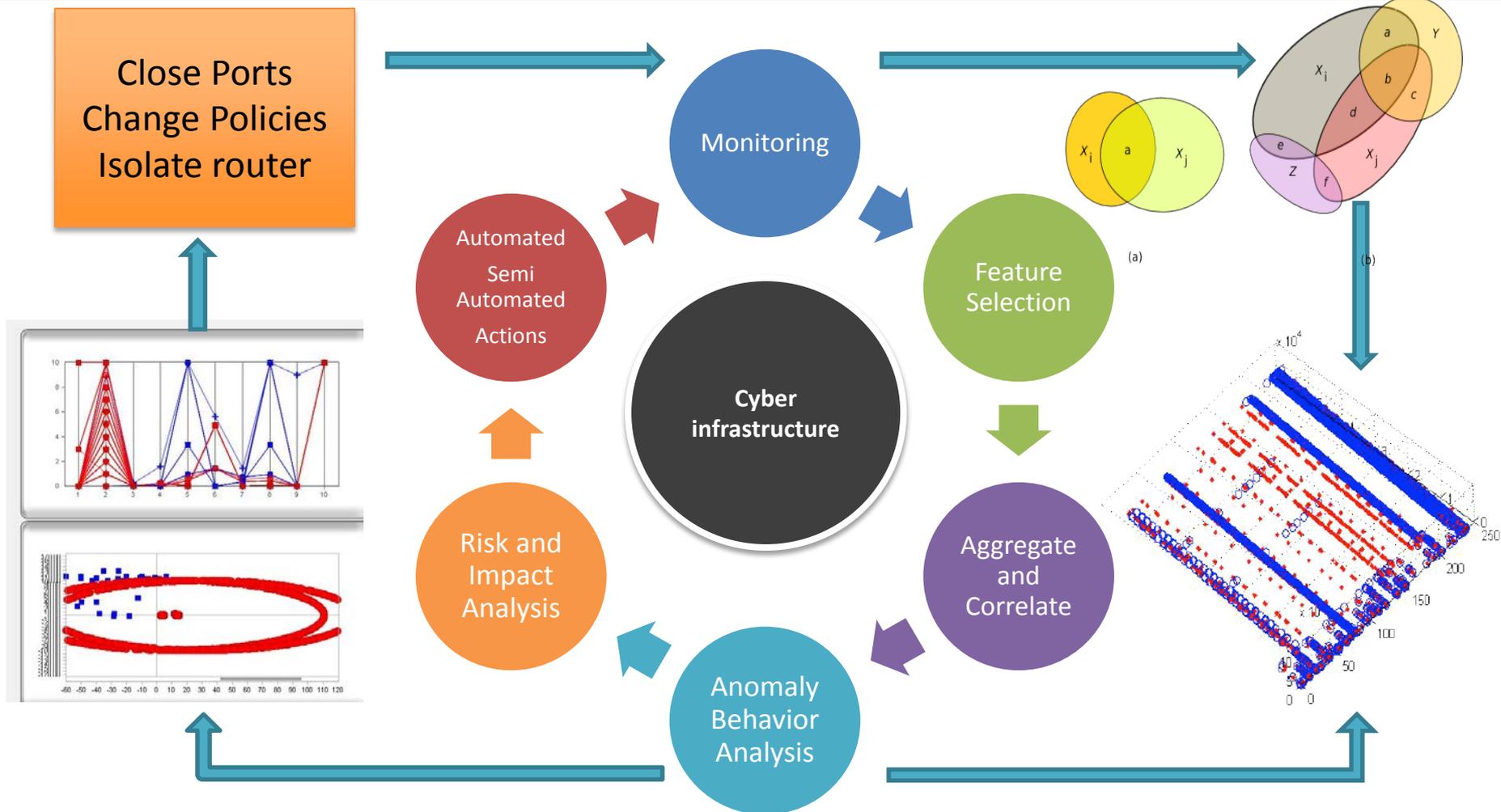
- A startup from the NSF Center for Cloud and Autonomic Computing at University of Arizona
- AVIRTEK is developing Autonomic Cybersecurity technologies (self-protect and self-manage)
  - **Software systems, computers, and networks that can *self-manage and proactively protect themselves in real-time with little or no involvement of users or system administrators.***
- AVIRTEK awarded an OSD SBIR Phase II and STTR Phase II from AFOSR to develop ACS technology
- SBIR Phase I, Air Force, started July 17, 2013
- Market Areas
  - Small /Medium and Enterprise Networks
  - Smart Buildings and Smart Grids
  - Data Centers and Cloud Computing
  - Data Analytics: Critical Infrastructures, Finance, etc.

# Customer Need

Existing management and security technologies have failed to secure and protect our cyber resources and services:

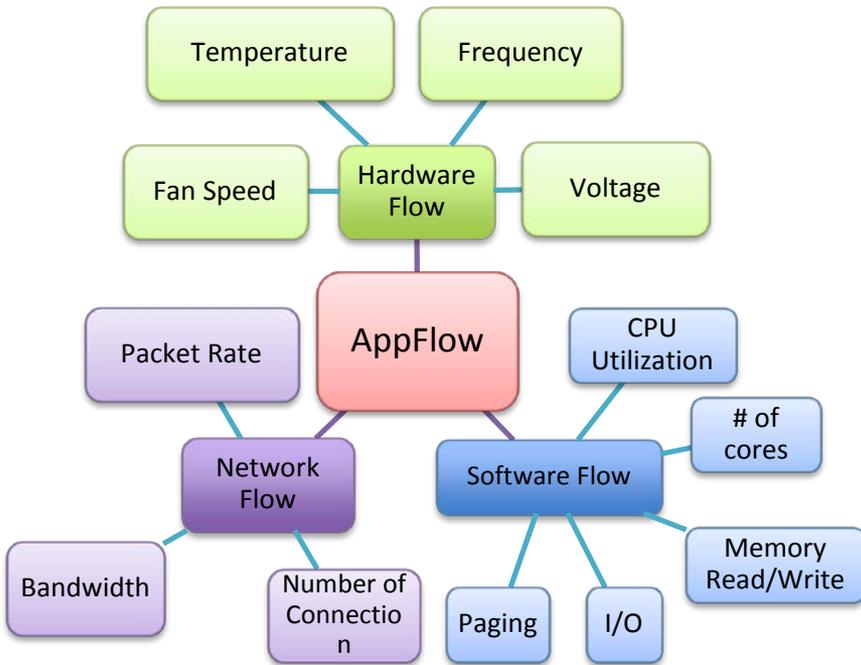
- They are mainly signature based solutions that cannot detect new and novel cyber-attacks
- They use many isolated and heterogeneous tools for monitoring performance, fault, and security that make it extremely difficult for human to comprehend and manage in a timely manner
- They are manually intensive activities that make them too slow to respond and act in a timely manner against malicious threats
  - Zero day exploits or malware that take advantage of undisclosed vulnerabilities might last up to 312 days before discovered

# Approach



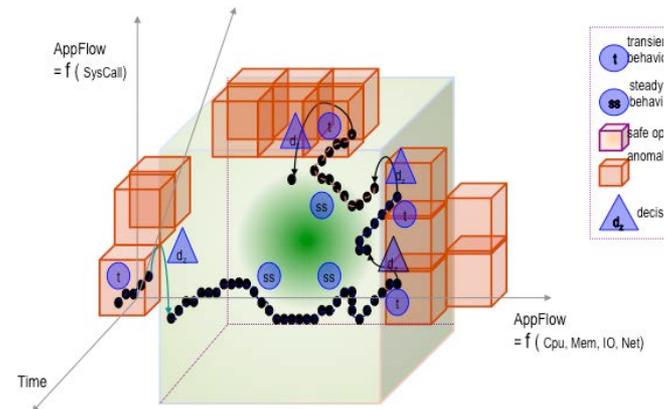
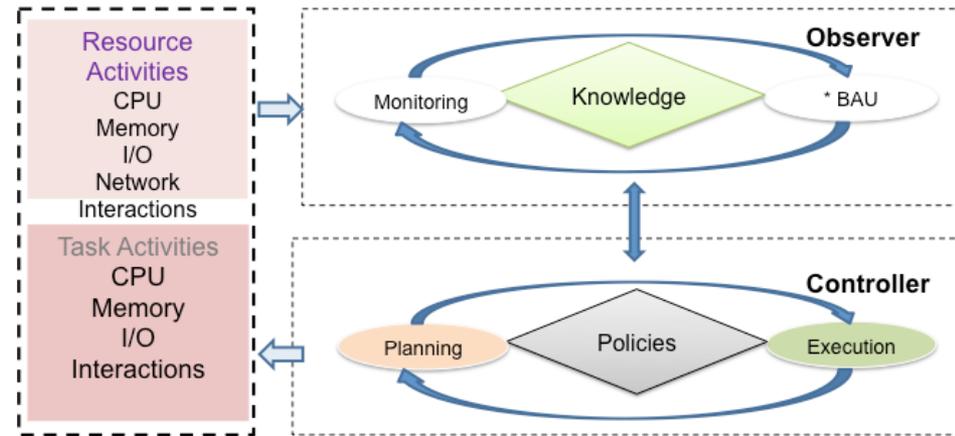
# Approach

## Application Flow (AppFlow)



Appflow is an innovative data structure to correlated Information about hardware, software, network, and Social activities to characterize current state and predict next states (Complete Situation Awareness)

## Autonomic Management (Self-Management)





# Benefits



- Real-time proactive protection against cyber attacks (known or unknown)
  - Solve the zero day attack problem
- Integration of self-management, self-optimization, self-healing, and self-protection technologies, and business services
  - Reduce operational cost through consolidation, and integration
- Provide both automated and semi-automated proactive protection actions
  - Automation solves complexity problems and the need to promptly respond to detected anomaly

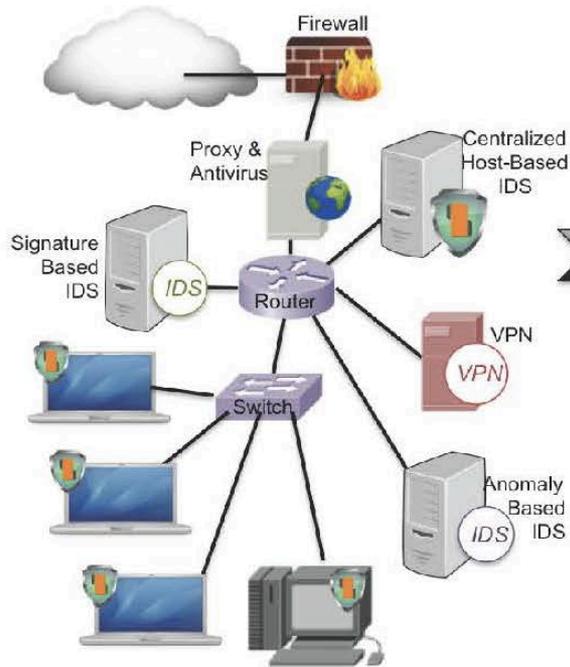
# AIM – Protective Protection System (PPS Series)



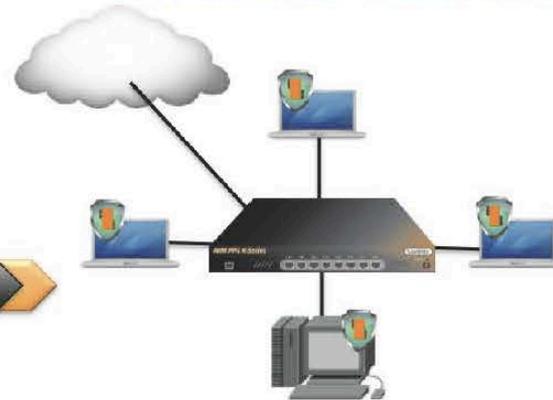
## AIM PPS X-Series

Smarter Resilience, Protection, & Management

### Current Technologies



### Avirtek's Technology



Deployed commercially at various locations in Arizona, Virginia, and more sites will be added soon

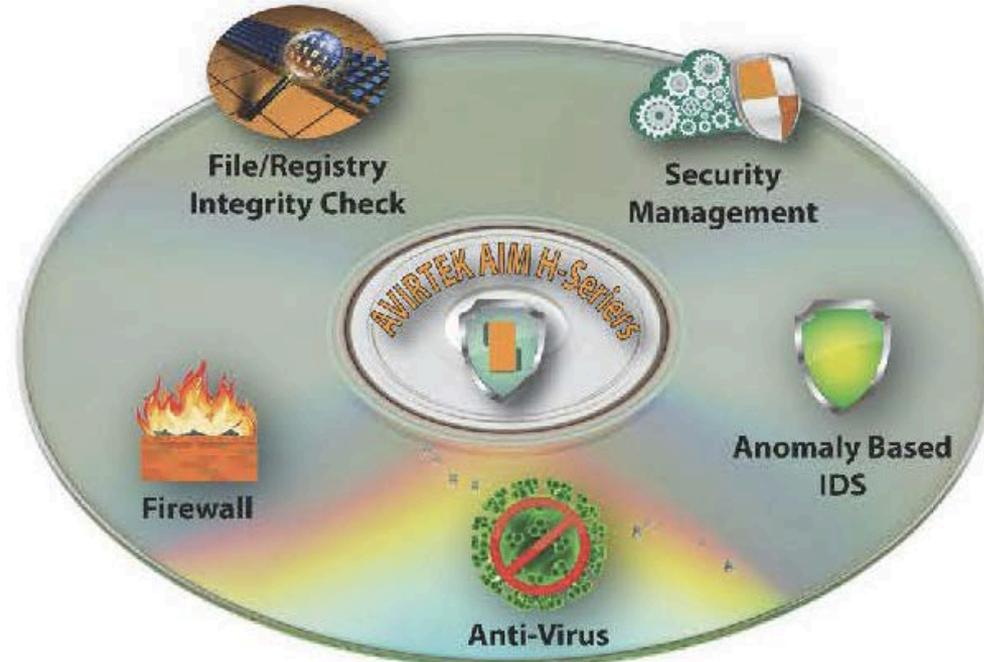
Integrated={Router, Switch, Proxy, VLAN, VPN, Anomaly Based IDS, Signature Based IDS, Anti-virus, Anti-malware, Centralized Host Based IDS}

# AIM – Host Poractive Protection System (H Series)



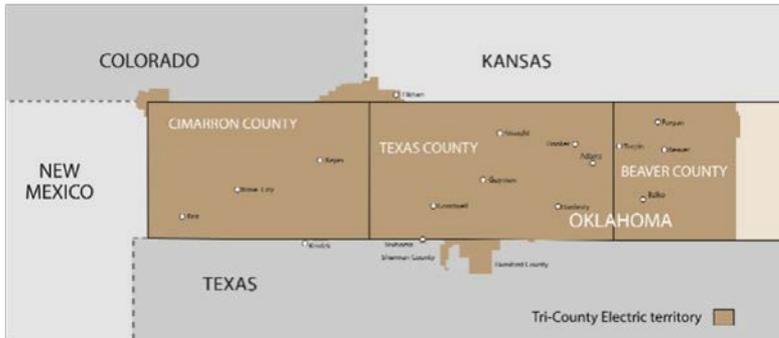
**AIM H-Series**

Smarter Resilience, Protection & Management

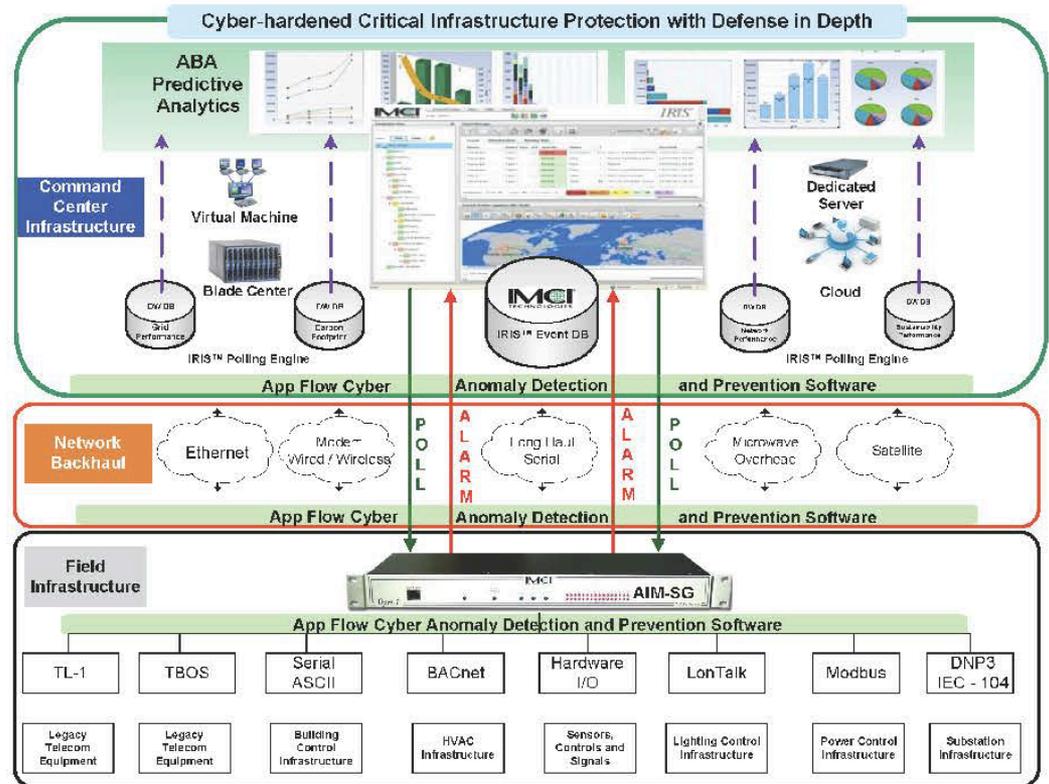


Window version will be available within a month  
Mac version will be available within 2-3 months

# AIM – Smart Grid (SG-Series)



Tri-County Electric Cooperative Smart Grid. Service Area of 23,000 households and businesses



© IMCI Technologies 2013. This information is confidential and proprietary. Do not duplicate or disclose without written permission from IMCI Technologies.

# Current Status

- Developed Automated and Integrated Management (AIM) products/services
  - Small/medium size networks; commercial deployment in Arizona, Virginia and more sites will be added soon
  - Critical infrastructures, TriCounty Smart Grid in Oklahoma
- What remains to be accomplished?
  - AIM for Enterprise
  - AIM for Cloud
  - Complete AIM Host and Network Proactive Protection System (AIM PPS Series)

# Next Steps

- Need help in securing Phase II.5 or Phase III funding
  - We have disruptive AIM cybersecurity technologies waiting for deployment and discovery
  - We need help in making that a reality
- Our technology is critically needed to solve current and future cybersecurity challenges
- We are eager to collaborate

# Contact Information

Salim Hariri, Founder and CEO

[www.avirtek.com](http://www.avirtek.com)

(520) 977-7954

salim.hariri@avirtek.com

**Acknowledgements:** This work was funded by

1. The Office of the Secretary of Defense (OSD) SBIR program under FA8650-110c1053. Program technical direction was provided by Felicia Harlow at AFRL/RWYC.
2. Air Force Office of Scientific Research (AFOSR) STTR program under FA9550-11-C-0007. Program technical direction was provided by Dr. Robert Bonneau at AFOSR/RSL