

# 2012 DHS S&T/ASD(R&E) CYBER SECURITY SBIR WORKSHOP



Homeland  
Security  
Science and Technology



## Automated and Integrated Management (AIM) Technology

AVIRTEK, INC.

Salim Hariri

[Salim.hariri@avirtek.com](mailto:Salim.hariri@avirtek.com)

(520) 977-7954

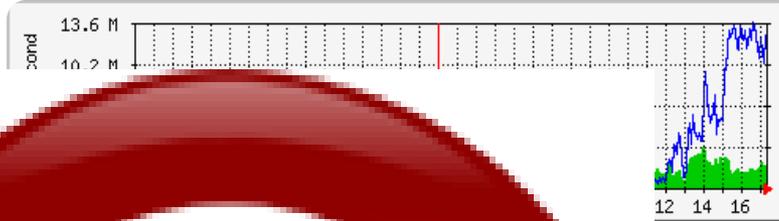
# AVIRTEK Profile

- Tucson based founded by Dr. Hariri in 2006
- AVIRTEK is developing Smarter Cyber Resilience technologies and services based on anomaly behavior analysis (ABA) and autonomic management.
- AVIRTEK is a startup company from the NSF Center for Cloud and Autonomic Computing at the University of Arizona
- Our technologies are the results of two SBIR/STTR awards:
  - AFOSR STTR (Phase I and II): Autonomic Cyber Battle Management System (ACBMS)
  - OSD SBIR (Phase I and II): Autonomic Software Protection (ASPS)
- Targeted Market Areas
  - Small /Medium and Enterprise Networks
  - Smart Buildings and Smart Grids
  - Resilient Cloud Computing Services

# Current Cybersecurity Management Techniques: Suffer from Click and View Syndrome (CVS)

IP	Host Name	IP	Host Name	IP	Host Name
8000_www_1801	IP	08-17-2009 14:34:20	10 17 18 47s	PRNG OK	
8000_photo_loader	RENDING	N/A	97s 1h 0m 25s+	Host has n	
8000_print_server	RENDING	N/A	97s 1h 0m 25s+	Host has n	
8000_server	RENDING	N/A	97s 1h 0m 25s+	Host has n	
8000_ssi1	IP	08-17-2009 14:34:25	1s 21m 51m 57s	PRNG OK	
8000_ssi2	IP	08-17-2009 14:34:26	0s 5h 45m 4s	PRNG OK	
8000_ssi3	IP	08-17-2009 14:34:26	0s 5h 45m 54s	PRNG OK	
8000_ssi4	IP	08-17-2009 14:34:26	0s 4h 45m 44s	PRNG OK	
8000_ssi5	IP	08-17-2009 14:34:26	0s 2h 45m 34s	PRNG OK	
8000_ssi6	IP	08-17-2009 14:34:26	17s 3h 5m 27s	PRNG OK	
8000_ssi7	IP	08-17-2009 14:34:26	0s 5h 29m 44s	PRNG OK	
8000_ssi8	IP	08-17-2009 14:34:26	4s 0h 5m 17s	PRNG OK	
8000_ssi9	IP	08-04-2009 04:00:13	23s 0h 5m 42s	PRNG OK	
8000_ssi10	IP	08-17-2009 14:34:10	0s 5h 29m 34s	PRNG OK	
8000_ssi11	IP	08-17-2009 14:34:11	14 15h 59m 47s	PRNG OK	
8000_ssi12	IP	08-09-2009 08:09:29	19s4 9h 14m 27s	PRNG OK	
8000_ssi13	IP	08-17-2009 14:34:11	41d 0h 44m 59s	PRNG OK	
8000_ssi14	IP	08-17-2009 14:34:12	0s 0h 48m 15s	PRNG OK	
8000_ssi15	IP	08-17-2009 14:31:33	0s 0h 59m 7s	PRNG OK	
8000_ssi16	CRITICAL	08-17-2009 14:31:43	137s 22h 40m 54s	CRITICAL	
8000_ssi17	IP	08-17-2009 14:31:53	0s 2h 22m 47s	PRNG OK	
8000_ssi18	IP	07-31-2009 17:59:13	16d 20h 52m 27s	PRNG OK	

31 Matching Host Entries Displayed



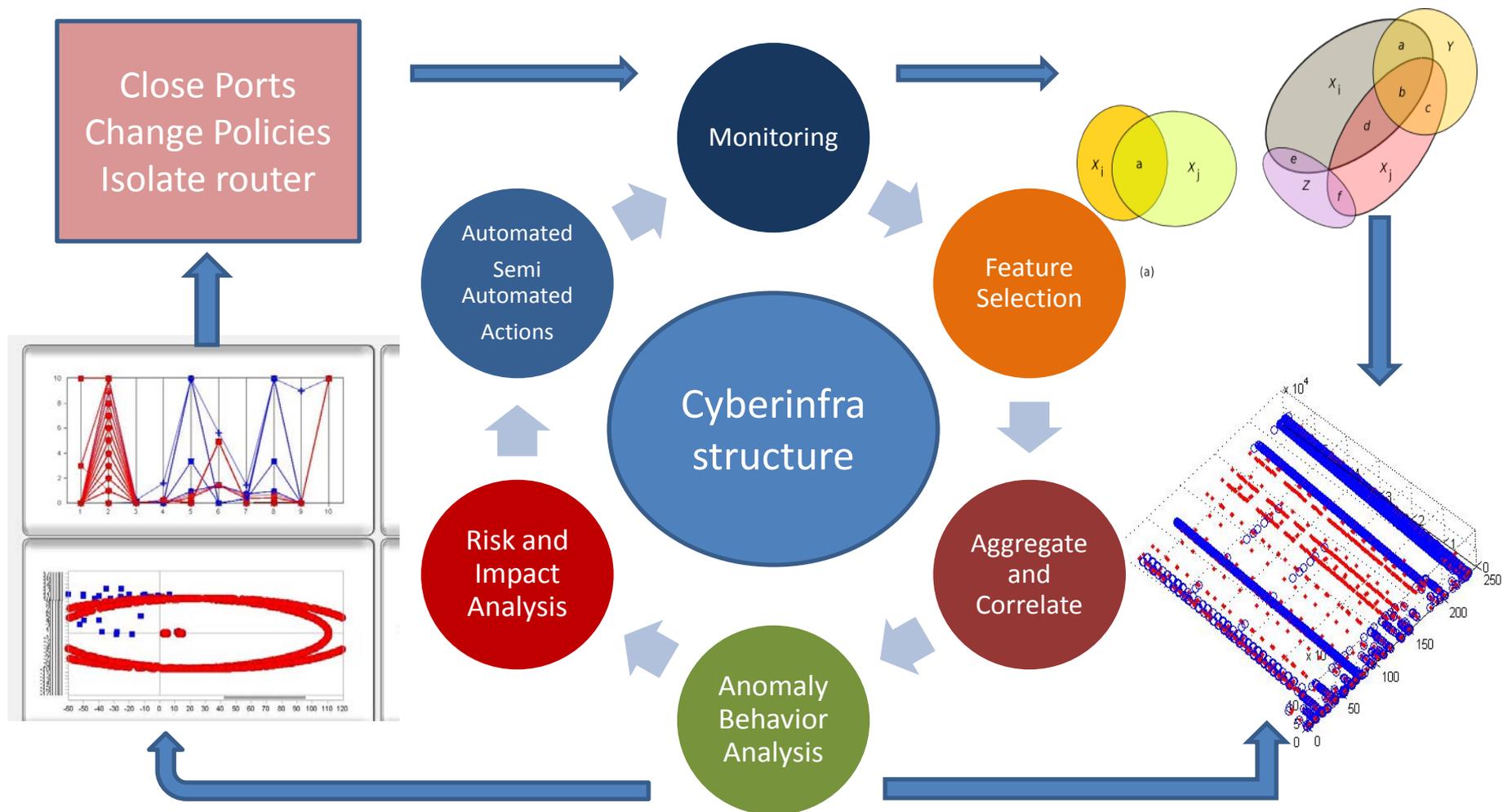
Attention



Logged in as 'admin' | Data Profiles/Settings | Reports | Config | Help | Logout

- Top Categories by Page Views
- Top Domains by Requests

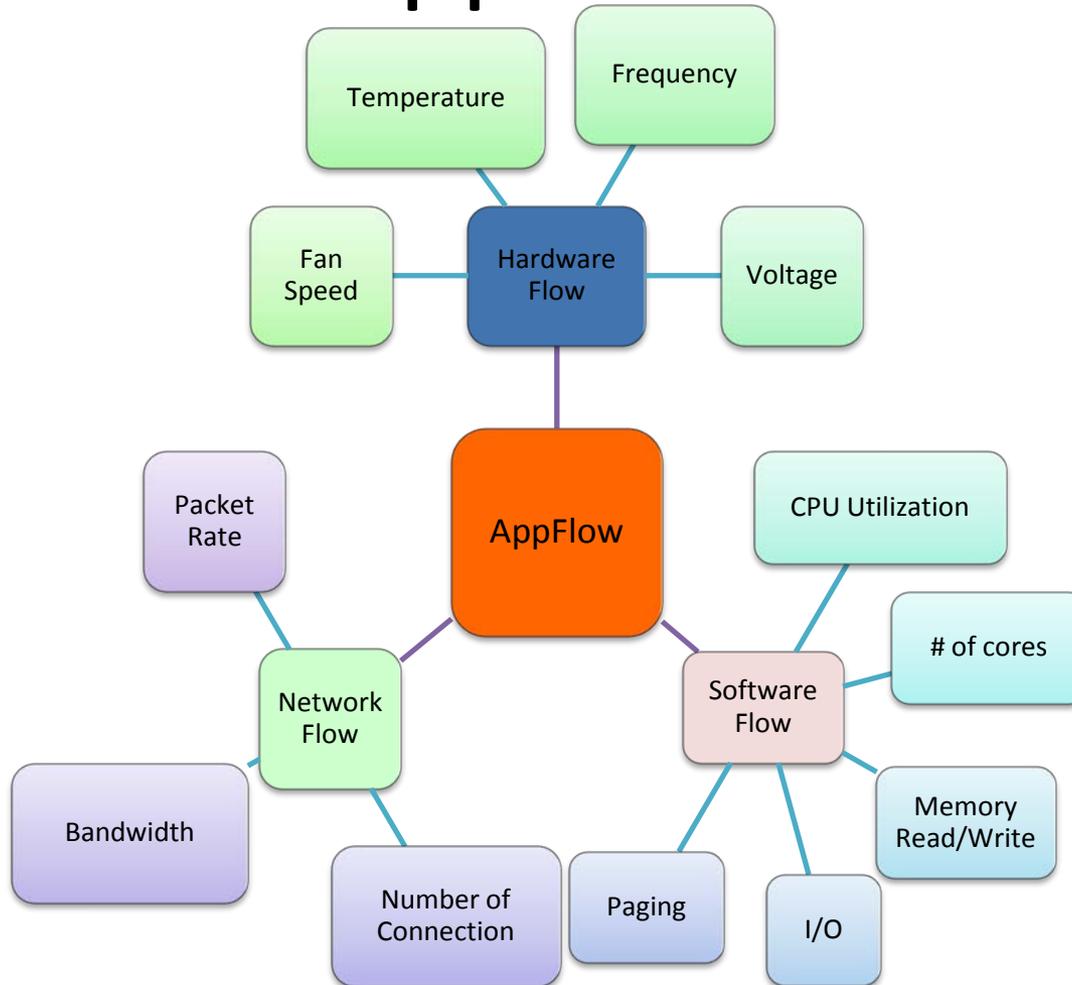
# AVIRTEK Automated and Integrated Management (AIM) Technology



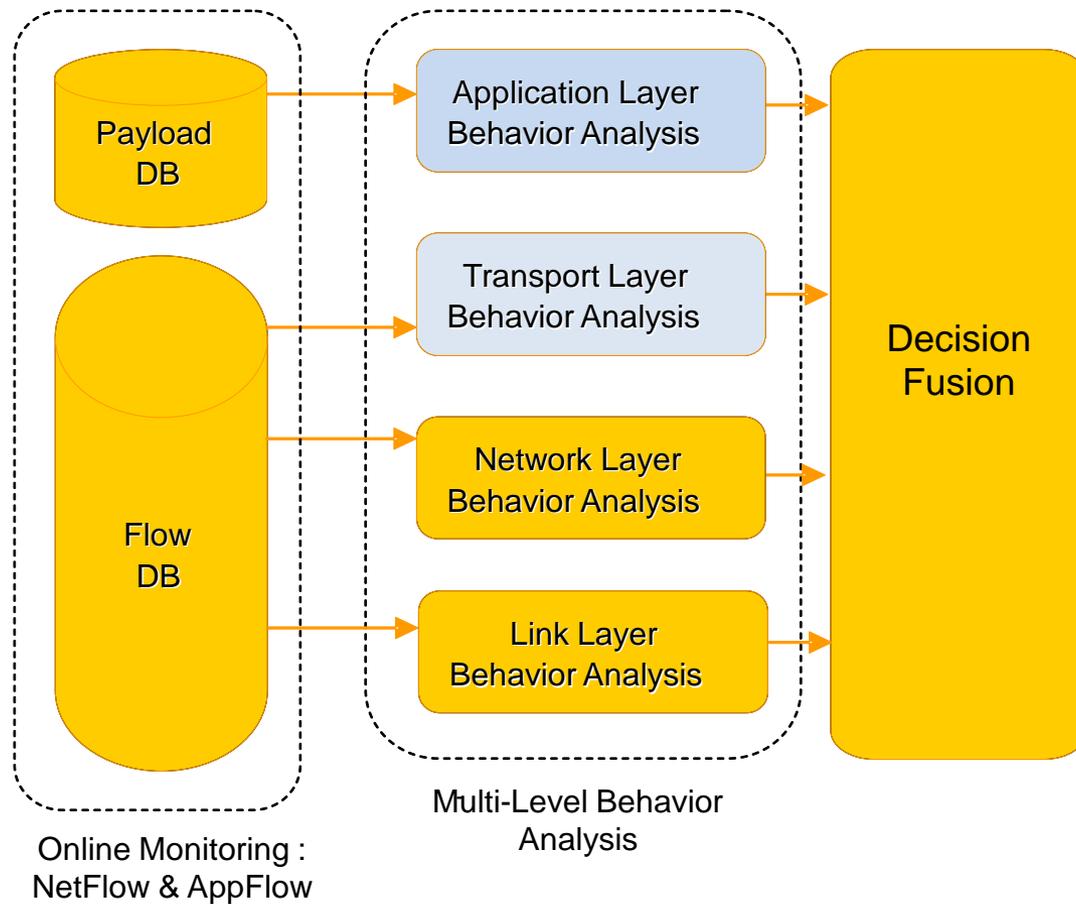
# Avirtek Innovative Technologies

- Appflow: A data structure that captures the current state of the system
- Anomaly Behavior Analysis (ABA) Methodology – low false alarms, and successfully implemented to TCP, UDP, IP, MAC, DNS, HTTP, WiFi, Modbus, etc.
- Self-Management: It is a software engine to provide automated and adaptive management services for hardware/software resources

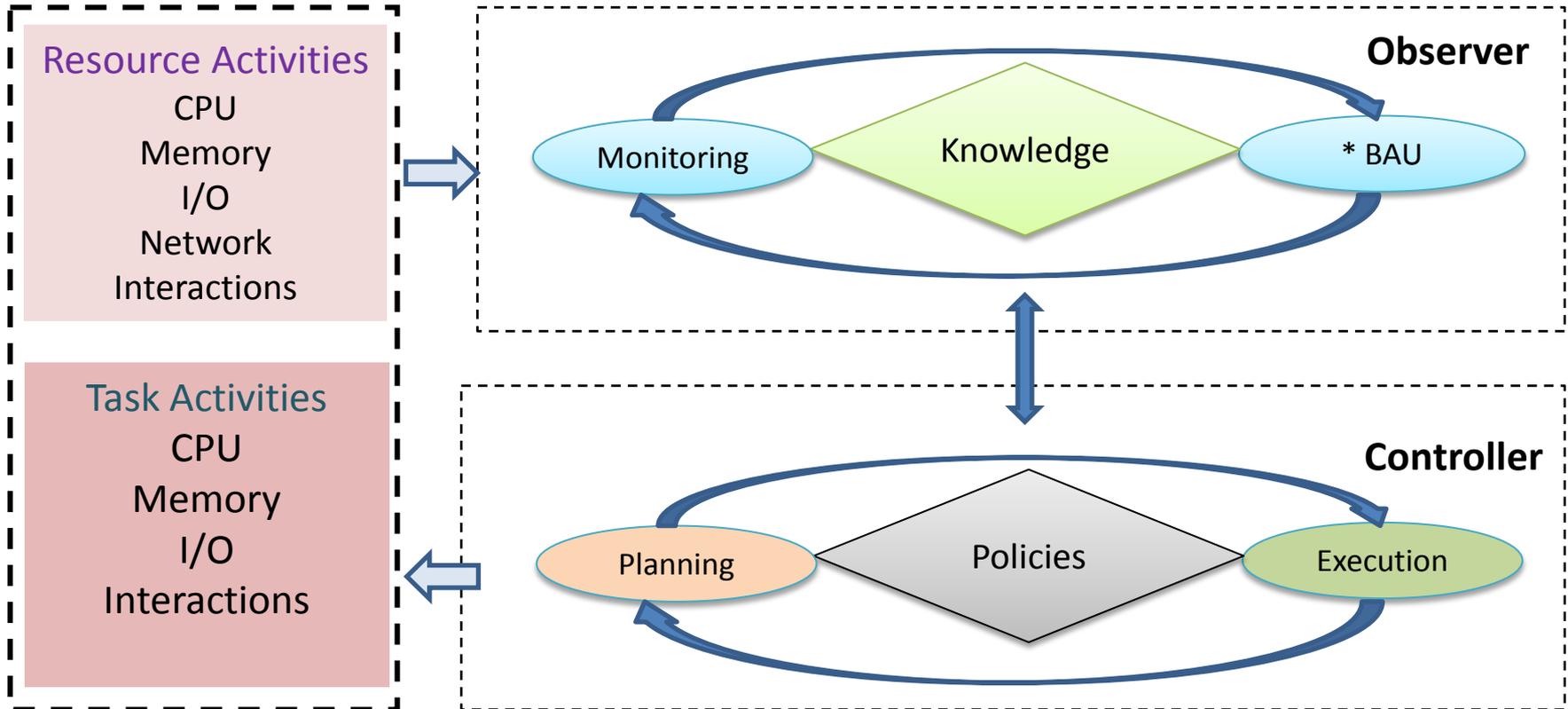
# AppFlow



# AVIRTEK Anomaly Behavior Analysis (ABA)



# AVIRTEK Self-Management Architecture: Automated/Semi-automated control actions



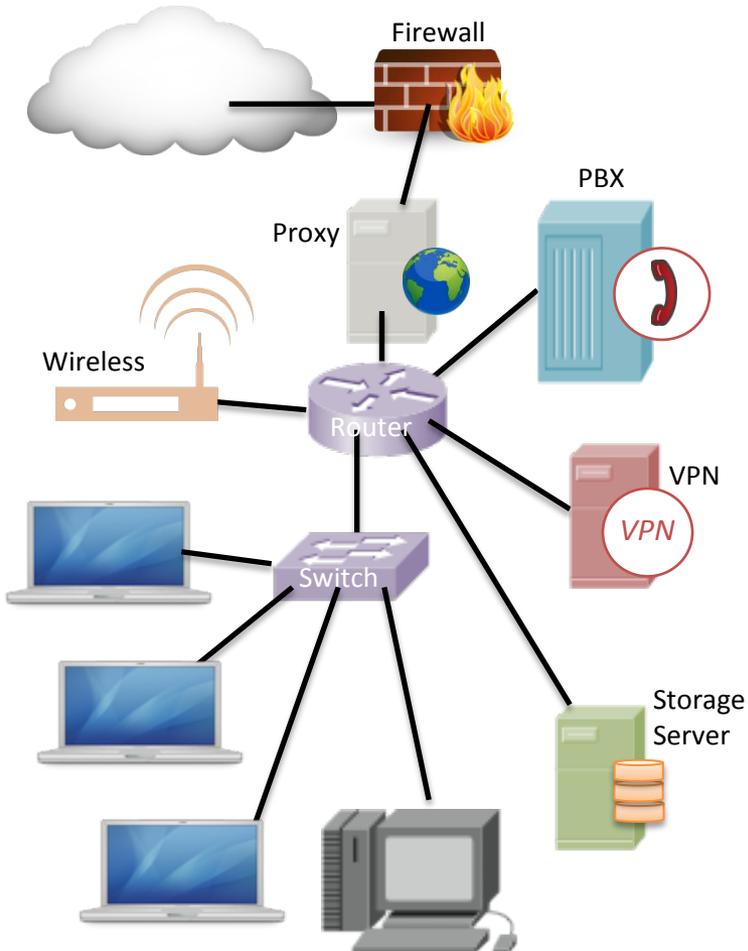
# AVIRTEK PRODUCTS

Our goal is to deliver unprecedented smarter cyber resilience management services for the following three market areas:

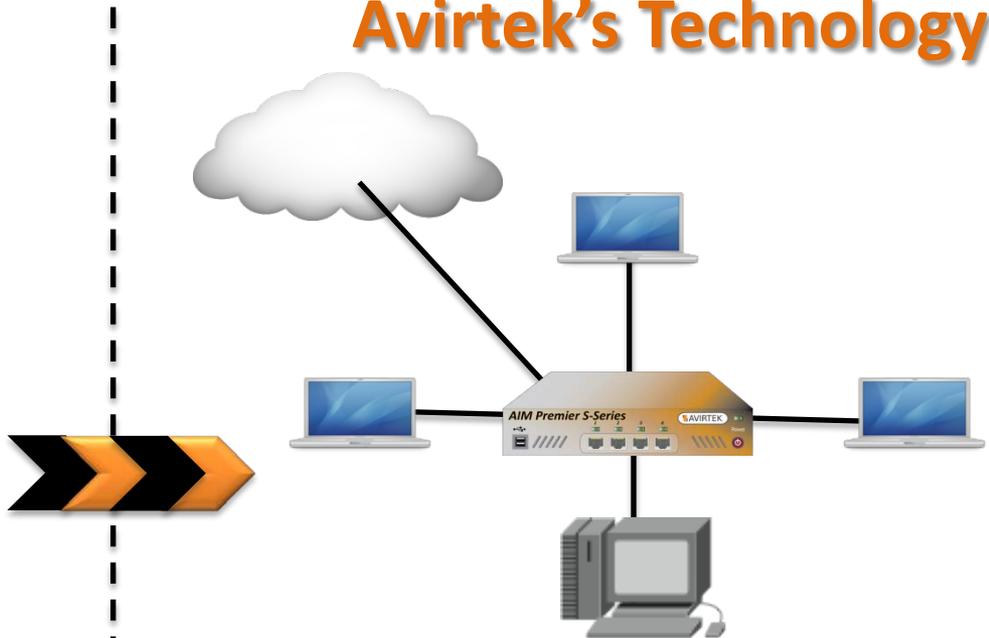
- Next Generation Smarter Cybersecurity Appliances for Small/Medium and Large Networks
- Critical Infrastructure Protection
- Resilient Cyber Microgrids
- Resilient Cloud Computing Services

# AIM Small Appliance

## Current Technologies



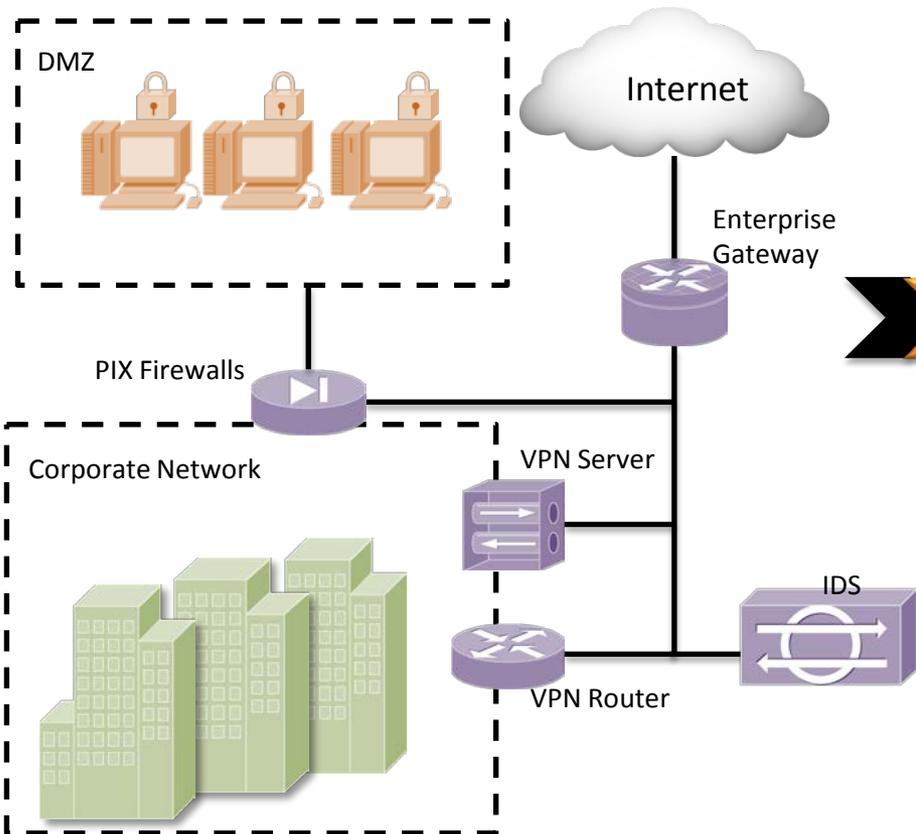
## Avirtek's Technology



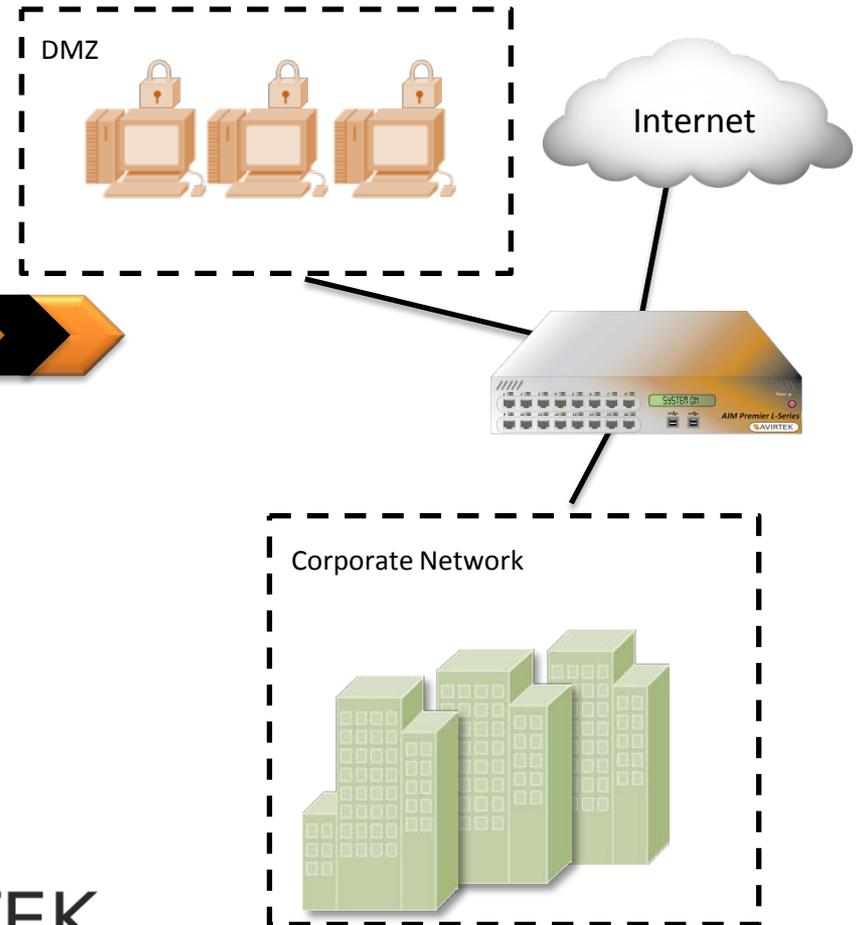
Integrated={Router, Switch, Wireless, Proxy, PBX, VPN, Storage Server, Firewall, Anti-virus, Anti-malware}

# AIM Large Appliance

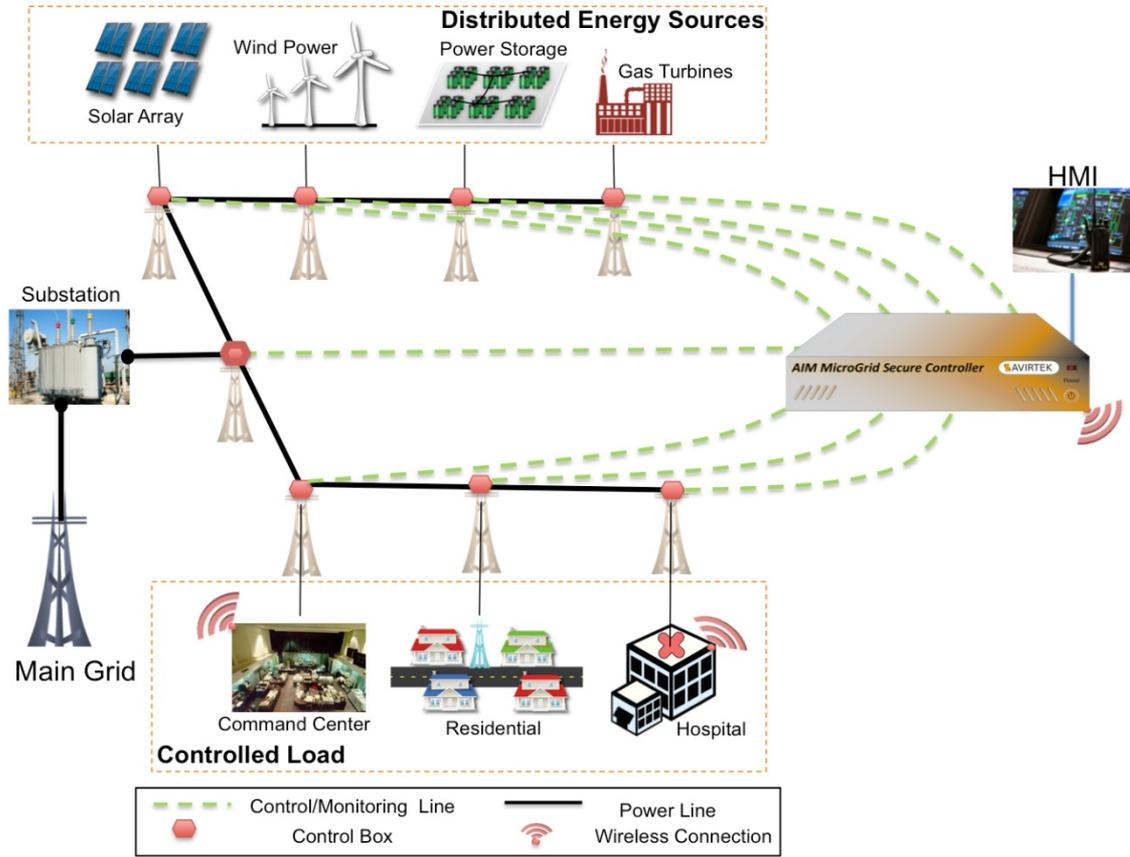
## Current Technologies



## Avirtek's Technology



# AIM Resilient Cyber Microgrid



THANK YOU