USER-CYBER DNA (UCD)

Avirtek provides Biometric Software for those who are concerned about preventing Insider Threats that could compromise their computers, networks and data integrity.

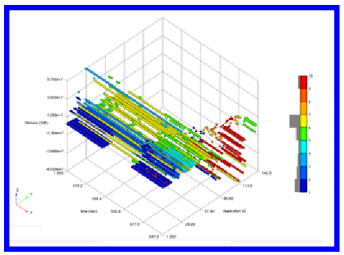

Figure 5—User Cyber Profiling

The Avirtek system analyzes every keyboard stroke and mouse movement as well all user interactions with hardware, software and network to create what we refer to as the User-Cyber DNA (UCD) as shown in ***Figure 5***, above. If someone attempts to gain access via another system or uses someone else's system password or access code, system access is immediately disabled and management is notified of an Insider Threat Detection (ITD).

INSIDER THREAT DETECTION (ITD)—WHY?

Organizations spend a lot of money to protect against hackers, cybercriminals, but the largest threats they face can be from insiders.

Existing Cyber Security technologies have failed to secure users and their applications.

- They are manually intensive activities that make them too slow to respond and act in a timely manner against malicious threats.
- Insiders can cause huge damages due to their knowledge and expertise with the company infrastructures and resources...i.e ***Edward Snowden***
- It takes more than 465 days to detect insiders!

AIM – ITD ARCHITECTURE

Monitoring and analysis tools track every user action through the server as shown in ***Figure 6.*** Avirtek's Bio-Tracker Client and Server compares each action with the specified User-Cyber DNA to validate each transaction. The combination of these tools determine if there is an Insider Threat. This process is fully automated and access is shut down immediately if a violation is determined. An Insider Threat Detection (ITD) alert is automatically reported to management.

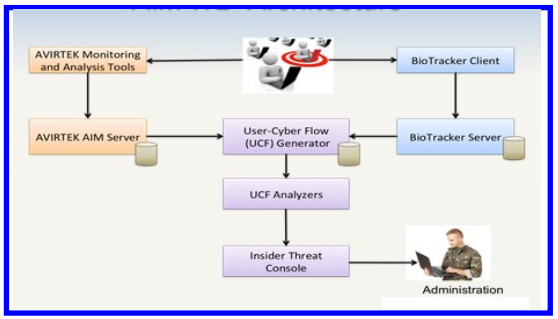

Figure 6—Insider Threat Detection Approach

AVIRTEK REMOTE ACCESS

Every Avirtek system has a Remote Access to aid in Installation and Technical Support issues. Any Cyber Threats can be analyzed to determine the source of the threat and the recommendation to eliminate or mitigate the impact of detected threats.

AVIRTEK MODELS

Avirtek combines its software with fully-integrated servers that feature multi-functionality for today's IT market. By limiting the number of access points in any system, it is possible to identify and eliminate today's Cyber Threats automatically.

Whether your business is a Small, Medium, Large, Enterprise or Cloud based system, Avirtek has a solution that will satisfy your application today.

Avirtek has architected its software to protect and manage Industrial Control Systems (ICS), which are critical elements in electrical, water, oil/gas, and manufacturing services involving Supervisory Control And Data Acquisition (SCADA), Distributed Control Systems (DCS), and Programmable Logic Controllers (PLCs). These systems allow operators to monitor sensor data and remotely control field devices.

Visit Avirtek today at www.avirtek.com and see how we can eliminate Cyber Threats.

Contact Us

Avirtek, Inc.
1236 E. Grant Road
Tucson, Arizona 85719
(520) 977-7954

Visit us on the web at: **www.avirtek.com**

AVIRTEK

Autonomic Cyber Security

Cyber Threat ...

Detection and Protection!

TODAY'S CYBER MARKET

The exponential increase of network connections, bandwidth, users, processing and global dependence on the Internet has greatly increased vulnerabilities of Information Technology (IT) infrastructure to more and more sophisticated and motivated attacks. In spite of drastically increased funding for R&D and deployment of information assurance defenses, reports of attacks on, and damage to the IT Infrastructure are growing at an accelerated rate.

ABOUT AVIRTEK

Avirtek is dedicated to Automated Cyber Threat Detection and Prevention. Using sophisticated algorithms, dedicated software monitors and analyzes every transaction run on computers, data, network, and through the Internet. A ***"Green Zone"*** is predefined and operation continues as long as this Zone is not violated. Once an action violates the ***Green Zone***, Avirtek software shuts down access to the computer, data or internet, depending on the severity of the detected threat.

Specialized Biometric software builds a user unique profile based upon keyboard strokes and mouse movement that we refer to as the User-Cyber DNA (UCD). In the event an insider should attempt to gain system access via another's computer, or by maliciously acquiring user names and passwords, the access to the computer will be immediately shut down and management is notified of an insider intrusion.

Whether the Cyber Attack is external or internal, Avirtek responds and shuts down system access to protect computers, the data and maintain integrity.

AUTONOMIC CYBER SECURITY (ACS)

The Cyber Infrastructure is continuously monitored by the Avirtek software as shown in ***Figure 1***, below. Sophisticated software algorithms determine if the cyber behaviors are operating within a well-defined ***"Green Zone"*** that is established during the training phase. In the event that a process goes outside the ***"Green Zone,"*** access is immediately shut down and a System Alert is automatically generated to management so automated and/or semi-automated responses can be taken to bring the system back to the ***"Green Zone"*** state.

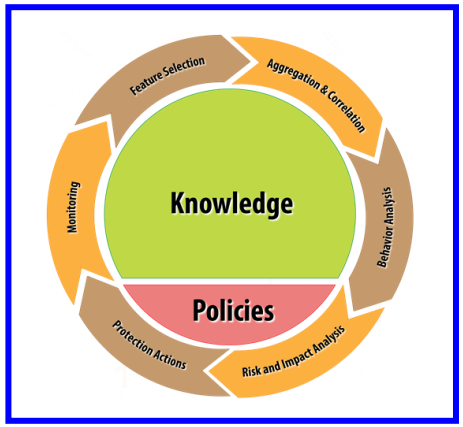

Figure 1—Continuous Monitoring, Analytics, Adaptation and Mitigation

ACS consists of three (3) specific technologies that continuously monitor system operation, analyzes its behavior and take proactive actions once a threat is detected. These technologies consist of the following processes:

- User-Cyber DNA (UCD)
- Anomaly Behavior Analysis (ABA)
- Automated and Integrated Management (AIM)

The Avirtek Autonomic Cyber Security methodology, shown in ***Figure 1***, is analogous to the human Nervous System. This highly automated software control system, monitors all activity through the Network, Hardware and Software Flows. Biometric Software is included that builds a unique user profile based upon user keyboard strokes and mouse movement that is referred to as the User-Cyber DNA, shown in ***Figure 2***. In the event an external or internal intrusion is attempted, Avirtek automatically shuts down system access to protect computers, the data and maintain integrity. An alert message is sent to management.

Right Fold to Here

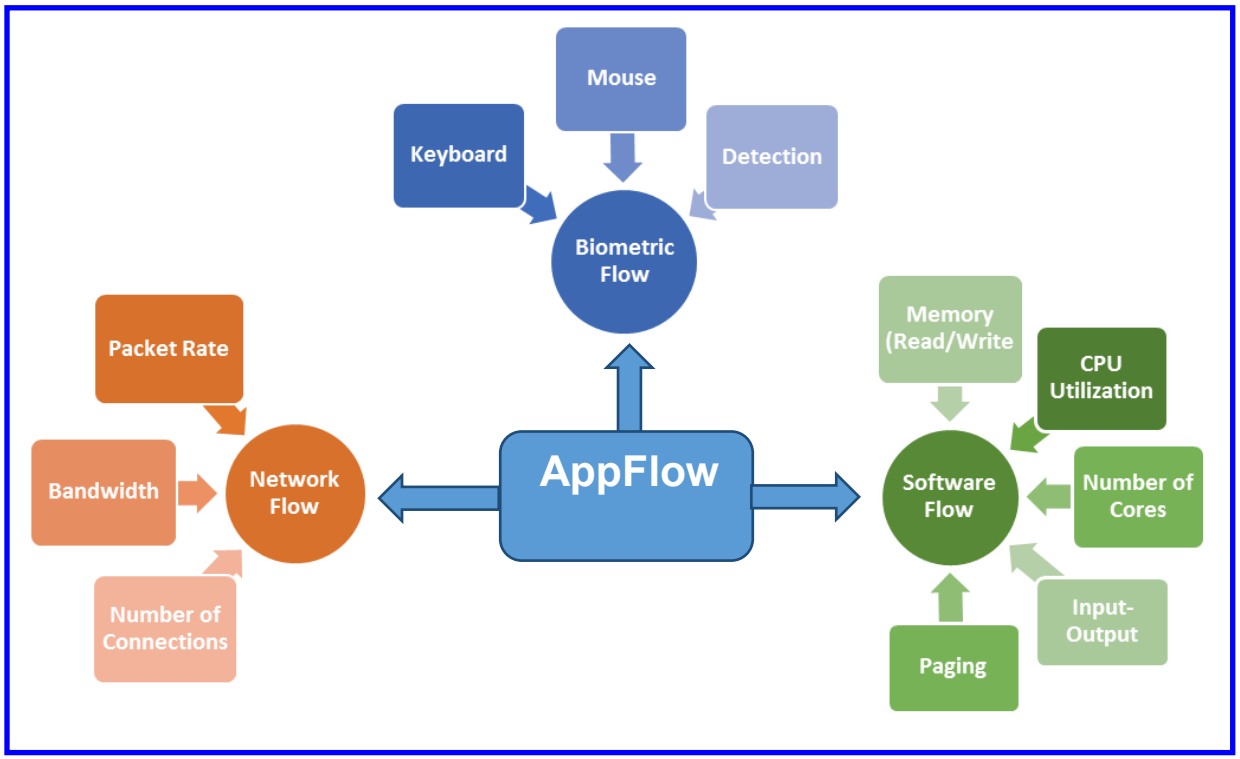

Figure 2—User-Cyber DNA Data Structure

Anomaly Behavior Analysis (ABA)

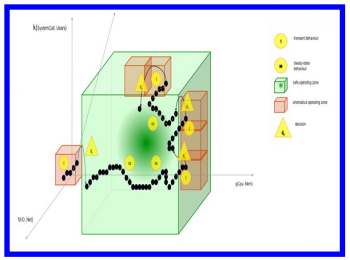

Figure 3, shows how Avirtek continuously analyzes the behavior of the system at any instant of time to make sure that the system behavior stays in the ***"Green Zone"*** all the time.

Figure 3—Continuous Analysis of System Operations

Anytime an external or internal action forces the system to go beyond the established boundaries of the ***Green Zone***, Avirtek determines the appropriate response based on policies. For example, it can automatically shut down system access to maintain system integrity and data protection.

Automated and Integrated Management (AIM)

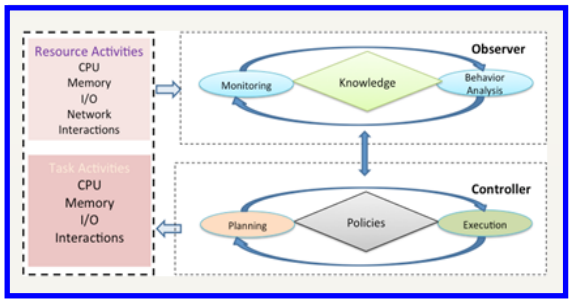

Figure 4—Automated and Integrated Management Architecture

Figure 4 shows the interrelationship between the Avirtek AIM system components. Knowledge and Polices define system boundaries. These values are essential in establishing the ***"Green Zone."*** By analyzing the data flow of the Network, Software and Biometric modules, Avirtek is able to provide Automatic Cyber Threat Detection and Protection at an unprecedented level. This Proactive, Resilient, Self-Managed solution provides the ultimate solution for any company concerned about Cyber Threats.