OrionX.net

Evolution

The OrionX Constellation

Cybersecurity, Artificial Intelligence, Internet of Things

Behavioral Analytics and IoT Security

Peter ffoulkes, Shahin Khan

It has become abundantly clear that cyber crime and cyber warfare are among the top issues of modern life. In a world where very little can be done without computer networks, personal life, business activities, and even national security are under threat and under constant attack. Attacks such as “WannaCry” and ”EternalBlue” have exposed significant vulnerabilities in both technology and user behavior from a personal to a corporate and even a government level.

Such high-profile attacks serve as a very good wake up call. Despite Wanncry’s rapid and global impact, one can expect the next attack to be even more wide-spread and damaging.

There are many lessons to be learned from these attacks. However, one particularly important lesson is emerging:

Current security practices and technologies designed for protect traditional IT asserts are not sufficient to identify and mitigate attacks for IoT devices. There will always be vulnerabilities and successful attacks, but new approaches to security are required and emerging that can identify and contain malevolent activity for IoT devices.

Three Dimensions of Cybersecurity

Security threats come from multiple directions, external and internal. Over the years, several approaches have been devised to protect data and/or to avoid service disruptions. In general, OrionX formulates three dimensions of cybersecurity:

- Regulate who gets in: Network Access Control
- Regulate what gets in: Malware Detection & Deep Packet Inspection
- Regulate behavior: Behavioral Analytics & Wide Packet Inspection

---

OrionX Constellation™ reports cover 5 Es: industry milestones (Events), historical view of a technology segment (Evolution), main vendors in a market segment (Environment), customer decision criteria (Evaluation), and how vendors in a segment score (Excellence) based on the OrionX methodology, which considers market presence and trends, customer needs and readiness, and product capabilities and roadmap.

A brief description of each dimension followed by a more detailed perspective follows.

- **Regulate who gets in: Network Access Control**

  Where admission into the network is regulated for all users and software entities that attempt to gain access. This is a highly developed technology today as exemplified by firewall solutions.

- **Regulate what gets in: Malware Detection & Deep Packet Inspection**

  Where packets are examined for malware signatures. This is a well-known area of technology, most visibly through anti-virus solutions.

- **Regulate behavior: Behavioral Analytics & Wide Packet Inspection**

  Where pattern analysis across many packets is performed as a way of monitoring the behavior of users, devices, and the network. This is a new area that is ripe for innovation and where several new models have been emerging. OrionX refers to these new models as **"Wide Packet Inspection"** since they rely on the analysis and correlation of many packets vs just going deep on individual packets.

In practice, cybersecurity solutions often combine elements from each dimension.

Network Access Control (NAC)

An established approach is to regulate all access and only admit authorized users or software modules into the network. This is commonly referred to as Network Access Control (NAC). It aims to authorize and manage access to network resources according to defined policies. Before granting access, in the pre-admission phase, this includes endpoint security checks, and in the post-admission, it provides controls over where users and devices can go on a network and what they can do.

Authorization and authentication can begin with simple user name and password entry but also include system level checks such as end-point identification, anti-virus protection status, system software update level, system and network configuration checks, etc. In addition, access to system resources, data, and applications can be regulated according to the user's persona, in a role-based set of protocols.

Key NAC Features

- Using techniques such as DHCP fingerprinting, NAC can gather information on the device including its underlying OS. While insightful for PCs and laptops, this technique cannot differentiate between different types of IoT devices such as an X-ray machine in comparison to a surveillance camera.
- Authorizes access according to user identification and access levels combined with required end-point access device identification and configuration.
- Often requires end-point agent software to be installed on devices to verify authentication. Although effective for known devices and configurations, it often does not apply to IoT devices that do not run a standard operating system or customizable software, thus restricting network access or compromising security.
- Manual remediation methods can be used to authorize access but are not applicable to a vast number of IoT devices for timely resolution of denied or quarantined access situations. This is especially problematic when new, unidentified or uncontrollable devices are attempting to access the network.

The key weaknesses of traditional NAC approaches is that they rely solely upon user and device authentication. Without the assumed user component of the equation, many required processes such as upgrading the OS, installing a patch or performing other remediation action cannot be accomplished, The biggest weakness to traditional NAC however, is the lack of behavioral analysis of supposedly authenticated devices. Heuristic behavioral analysis can flag anomalous behavior and send alerts for corrective action, either manual or automated.

Perhaps the main lesson here is that people tend to underestimate the risks to their IoT devices and fail to take proactive action to update their legacy security solutions. The size and complexity of an organization's IoT envirionment together with the diversity of systems in use only exacerbates the problem.

Malware Detection & Deep Packet Inspection

Short of installing agents in every endpoint, detection of malware required inspection of all incoming data packets. Once a virus is detected and characterized, its so-called "signature" can be propagated to firewalls and anti-virus software to enable them to detect the malware.

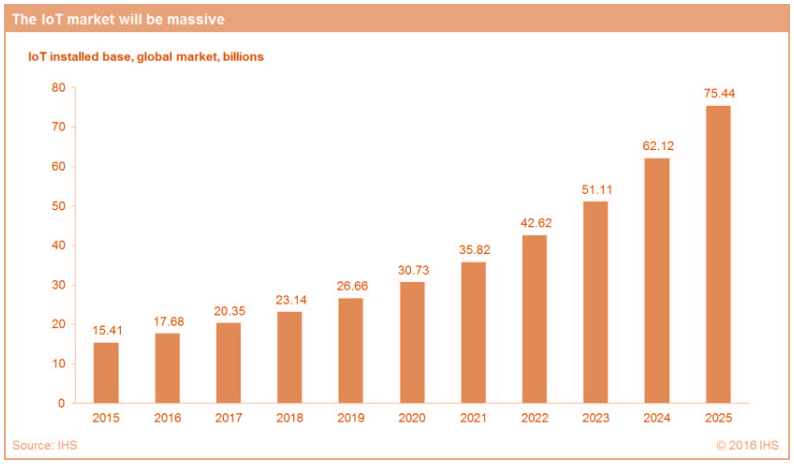
As endpoint computing power increased over time, installing clients or agents on the endpoint became common practice. This model relied on the end-user to ensure the client/agent is updated with the latest signature to ensure up-to-date security.

Despite reliance on NAC solutions to ensure the latest OS, patches, and AV signatures are installed, it's important to note that NAC solutions do not offer malware detection. Its primary function is to ensure that the device meet the necessary criteria for network access. Many zero-day and APT attacks that do not have well-defined signatures can easily bypass signature-based security solutions. Hence even if the device has been compromised, as long as it meets the necessary criteria, the NAC solution will allow network access often with disastrous consequences.

Behavioral Analytics & Wide Packet Inspection: A new approach to security in the era of IoT

The Internet of Things complicates the issue of system security by several orders of magnitude. It has to deal with the inherent weaknesses of human behavior while absorbing a huge proliferation of additional connected devices. Many of these devices have an internet presence yet have limited security capabilities. Many have default settings that restrict even basic best practices for security procedures and human nature indicates that unless good security policies are rigorously enforced, they are unlikely to be implemented successfully.

While it is possible to install endpoint software agents on the majority of traditional IT devices in a well managed environment this is frequently not the case with IOT devices whose control logic is often firmware-based. This imposes a significant burden on IT staff to be able to identify, characterize devices, track firmware levels and make security updates when and if made available. This becomes increasingly difficult as devices age, and current IoT devices are notorious for poorly implemented security, even hardwired user names and passwords making them an easy target as a point of entry to an organization. With the number of IoT devices growing exponentially it will be impossible for manual systems to keep up with device proliferation. IHS forecasts that the IoT market will grow from an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025.



The essential take away is that traditional approaches to securing end-point devices will be impractical in the IoT era if they are not already ineffectual, as demonstrated by the increasing frequency of ransomware and distributed denial of service attacks. If devices themselves cannot be secured effectively then activity at the network level becomes the natural best defense.

	Traditional IT Security	IoT Security
IT Asset Design	✦ Security capable / programmable / configurable	✦ Unknown / lack capacity to run agents / anti-malware
IT Asset Discovery	✦ Configuration Management Database (CMDB / ITIL) ✦ Automated, based on tags or end-point agents	✦ CMDB / ITIL with dynamic discovery, cloud based profiling ✦ Automated discovery, no agents
IT Asset Management	✦ Process driven with manual execution ✦ RFID tags / IP addresses ✦ End Point agents ✦ Only those that are known / or support sw agents	✦ Limited control, automation driven ✦ IP addresses ✦ Automated discovery
Network Authorization	✦ Configuration Management Database (CMDB / ITIL) ✦ Protect the perimeter ✦ Manual / time consuming ✦ Controlled by identity and user device ✦ Automated, based on tags or end-point agents	✦ Automated, Real time behavior monitoring ✦ There is no perimeter ✦ Automated and continuously monitored ✦ Automated discovery and behavioral profile ✦ Automated, Real time behavior monitoring
Operational Control and Monitoring	✦ Manual / time consuming/limited ✦ Limited and optional ✦ Manual / time consuming/limited ✦ Manual / time consuming/limited ✦ limited / manageable / controllable ✦ Vulnerable to human authorization	✦ Impractical / potentially impossible ✦ Continuous monitoring and analytics to scan for dangerous changes ✦ Automated and continuously monitored ✦ Automated and continuously monitored ✦ Unlimited / unmanageable / uncontrollable ✦ Automated and continuously monitored

Critical Requirements for IoT Security

To implement IoT security at the network level requires multiple capabilities beyond what traditional NAC solution can offer including device design attributes, the ability to discover, catalog, and classify devices, management, network authorization, and operational control and monitoring to compare with trusted activity profiles:

- **IT Asset Design** – Devices need to be capable of basic security capabilities including assigning individual device identities, user and password access controls.
- **IT Asset Discovery** – Automatic discovery of devices in the network is a necessity to overcome the challenges of IoT device deployment and proliferation. This allows for every device to be identified, registered and either granted or denied network access according to a predetermined policy.
- **IT Asset Classification & Management** – This is essential to basic network security, but many organizations simply lack a clear inventory of all their IT assets. Many are managed using different, possibly incompatible tools and across several departments. These fragmented and manually controlled policies and procedures cannot scale with the diversity and rapid adoption of IoT devices. A well-managed repository is required to build a reliable network and device profile for each device category and each device.
- **Network Authorization**– Discovery of IT and IoT devices is clearly a prerequisite to building a network map and database, but managing these devices requires the ability to classify them into appropriate categories and to manage and authorize the devices by these categories. With typical organizations having 1,000s of devices, the management and authorization of IoT devices individually does not scale.
- **Operational Control and Monitoring**– With each IoT devices purposely built for a specific function, identifying risk rating for a device requires in-depth knowledge of their intended and trusted behavior.

Traditional Network Access Control Cannot Meet IoT's Security Requirements

Even starting with devices an organization is very familiar with, it is not possible to secure them using traditional security methods. Some devices have very poor and hardwired security functions, others may be components of more sophisticated dedicated apparatus and not be able to be upgraded or to handle agent-based security monitoring software. As the number and diversity of devices grows exponentially traditional network access security methods that depend upon identifying all the devices in the ecosystem and what kinds of rights and privileges are granted to them becomes increasingly unmanageable.

The solution depends upon having a comprehensive system for automatically scanning networks, identifying and profiling all connected devices, and managing those assets. More importantly IT monitoring systems must understand the function and normal behavior of each and every device, and be able to create real time alerts for any anomalous behavior. Policies that analyze and determine what each device can and cannot do must be enforced from a comprehensive database of device characteristics that will need to extend to new and previously unknown devices in any organization's network.

IoT security is a behavioral challenge

IoT security is a behavioral challenge even more than it is a technical challenge. That means changing the IT culture to one that tolerates and actively responds to the inevitable state of IoT insecurity, constantly analyzing threats and attack vectors as well as scaling beyond the capabilities of manual processes. Systems that incorporate artificial intelligence techniques to detect, recognize and respond to behavioral changes will be essential. Only then can businesses fully and safely benefit from the full potential offered by IoT based intelligent networks.

Please visit OrionX.net/research for additional information and related reports.