Why IDS Can’t Adequately Protect Your IoT Devices
Introduction

As a key component in information technology security, Intrusion Detection Systems (IDS) monitor networks for suspicious activity or violations of policies. IDS has been a mainstay in cybersecurity for years. Now, however, with the arrival of the Internet of Things (IoT) revolution and the need to protect all these diverse “connected” devices, IDS with its signature-based approach is not sufficient for addressing the new and growing security issues that come with the proliferation of “smart stuff.”

In this white paper, we will explore why and how IoT security needs a new framework and a new type of solution. ZingBox IoT Guardian represents a new kind of security solution that when used in addition to IDS is the best approach for safeguarding IoT devices, the networks they reside upon, and ultimately, the organizations that own them.

Back in the Day…

In the early days of IT security, IDS was designed to expose suspicious intrusions and identify irregularities by internal users – in other words, insider threats. Rules were created and baselines were established. Threats were detected after audit logs were analyzed. This manual method worked fine for a time but as the Internet made the jump from government usage to commercial and general public usage, automation and packet sniffing solutions were introduced and the focus changed to external threats.

As IDS (which only detected threats in an offline manner) evolved into IPS (Intrusion Prevention Systems, which detect new threats based on matching signatures of known threats and take control actions), the wire speed and performance of devices became more important. Together, IDS/IPS became a standard and similar to firewalls (another “control tool”), evolved into self-contained, in-line appliances. This was an adequate solution before the advent of IoT.

The Need to Maintain Speed

A major challenge for IDS/IPS vendors is that they are not permitted to slow down or introduce latency in the network traffic. As a consequence, IDS/IPS solutions are boxed into only using signature-based or pattern-based detection and prevention. They basically play a “match game” of known threats that can be performed quickly, using as little system memory as possible.
Due to the restriction on memory usage and the need for speed, the typical IDS/IPS solution isn’t even referencing all the signatures of known threats, forcing IT security teams to make compromises regarding which signatures are scanned for and which are not. Furthermore, with an IDS/IPS tool, the time frame for reviewing threats is also limited, which prohibits long-term monitoring and evaluation of multiple sessions or behavior analytics over time.

One of the main problems with IDS/IPS is that they can only detect known malware using heuristics and signatures. To generate these heuristics/signatures, the vendors have to source the malware, analyze it, and then describe its behavior so that it can be detected when it’s seen the next time. This reactive approach is limiting and rarely works to detect new zero-day threats.

The biggest issue with traditional IDS/IPS solutions is that they can leave endpoints and networks vulnerable to more sophisticated threats, particularly ones that don’t use existing malware or leverage exploits. Cybercriminals are using evasive tactics, including zero-day attacks where there is no known signature; encrypted and customized attacks; and attacks that blend in with trusted users and well-known apps.

The reason attackers target IoT devices is because the devices are a weakly-guarded side door that permits access to the victim’s network. IoT devices can be used like stepping stones to other systems inside the organization. This type of behavior is called “Lateral Movement.”

**How IoT is Different from Traditional IT**

Internet of Things is the term that is being used to identify “smart” devices (examples: home appliances and medical equipment) that are connecting to the Internet to provide consumers and businesses with more control, convenience, speed, accuracy, and savings. As the number of IoT devices grow, the need to secure them also grows. 25 billion IoT devices with little or no built-in protection are predicted to be online by the year 2020. For IT staff trying to manage security on their corporate networks, most of these IoT devices will be unseen.

You can’t protect what you can’t see, so security risks are multiplying with even basic devices like lights and fans now become network-aware but that lack visibility. Traditional signature-based security solutions often fail to protect the diverse IoT infrastructure. The challenges to securing IoT devices are numerous, including visibility into what’s on the
network, blind spots, long lifecycles, difficulty in patching, diverse deployment models, and non-standard and legacy communications protocols.

Unlike traditional general-purpose IT devices that include PCs, servers, mobile phones, and others, IoT devices are more purpose-built systems, designed to perform a small number of specific tasks without much human interaction. Therefore, IoT devices have stable, limited, and very predictable behaviors that allow new security solutions to establish accurate baselines of their behavior. So if an IoT device begins to “color outside the lines” of their normal behavior, it will become very visible very quickly when being monitored by a security solution like ZingBox IoT Guardian.

Real-Time Discovery, Visibility, and Threat Detection

In order to secure IoT devices properly, the standard IDS/IPS solution alone is not enough. An IT security team needs an additional tool like ZingBox’s new solution IoT Guardian that can detect today’s cyber-threats wherever they may lurk.

Also, this new kind of IoT security must be able to find assets on the network, no matter where and what kind they are. Then it must be able to profile them and protect them. To do this well, it will require getting visibility into the devices’ behavior as it connects with entities inside and outside of the network perimeter and observing how their behavior changes over time.

Technology research company Gartner also recognizes that IoT security requires different kinds of solutions for IoT devices, stating: “Companies should assign business ownership of IoT security, focus on vulnerable or unpatchable IoT devices, and increase IoT-focused budget.” The ZingBox solution fits precisely into the new IoT security product category that Gartner recently created and calls: Real-Time Discovery, Visibility, and Threat Detection. Previously, there were only two major cybersecurity categories: Endpoint Security (Agent-based) and Network Security (Inline/Active).

Currently, most cybersecurity vendors offer solutions that are focused on Endpoint Security and Network Security for monitoring the perimeter. ZingBox IoT Guardian is an innovative, cloud-based Security-as-a-Service solution that is agent-less and signature-less. It provides visibility and control for all IoT device behaviors, without disrupting or slowing down the IoT operation.
Machine Learning

All IoT devices have limited and stable behavior. Because there are so many different kinds of IoT devices, machine learning is the best way to compile data regarding an IoT device’s behavior. This form of artificial intelligence is much more reliable than a human and scales much better as well.

IoT security solutions that use machine learning provide visibility and protection, and are generally configuration-free. They use machine learning algorithms to automatically discover, identify, classify, and generate normal baselines of IoT device behaviors to secure enterprise IoT infrastructure. The behaviors learned are not just about networking traffic, but also about what applications run on each device and the applications’ behaviors as well.

In addition to using machine learning, IoT Guardian also:

▪ Analyzes IoT traffic
▪ Provides real-time IoT visibility
▪ Identifies and classifies devices
▪ Provides automatic IoT risk assessment
▪ Learns automatically the normal behavior of each device
▪ Establishes a baseline of normal activities and forms IoT situational awareness
▪ Employs anomaly detection to discover threats in real-time
▪ Provides context-aware policy enforcement

ZingBox’s Technology Vision:
A New Framework for IoT Security

A new kind of IoT security that provides real-time discovery, visibility, and threat detection is needed. ZingBox is playing a leading role with IoT Guardian – a cloud-based, machine learning solution that automatically discovers and classifies connected IoT assets; extracts their context; and builds a comprehensive profile to provide real-time protection.

IoT device visibility is key to effective security. ZingBox’s solution inspects and analyzes IoT device behaviors in a completely passive mode so that IoT Guardian has zero impact on IoT operation. It uses protocol analysis, deep packet inspection, and multiple signals ranging from device MAC address, to SSL certificate exchange messages, to application behaviors, to automatically learn and model the normal behavior of connected devices.
Most of the current IDS/IPS products today (including the more recent ones that focus on the Industrial sectors) rely on deep packet inspection (DPI) for protocol level analysis to inspect the network traffic and interpret the content in transit. Unfortunately, DPI has limitations.

Deep packet inspectors offer full visibility into certain networks by analyzing known pre-identified protocols and detecting unfamiliar activities or changes in configurations. Since DPI solutions only focus on protocol analysis, they have the following limitations:

- Restricted to just a few industrial verticals that mainly use ICS/SCADA protocols
- Works only if the traffic is not encrypted. If traffic is encrypted, the approach stops working (In comparison, the Machine Learning approach works in all cases. See below for more details.)
- Only addresses a small set of the security problems. Not all security attacks will cause protocol level changes. For example: business espionage, DDoS attacks, and lateral movement do not change protocols at all

IoT Guardian works effectively in both unencrypted and encrypted traffic environments because it does not solely rely upon protocol analysis (ICS/SCADA/etc.). Its patent-pending machine learning technology enables IoT Guardian to work efficiently across multiple sectors such as Healthcare and Industrials. The solution automatically builds IoT device context through continuous learning of IoT behavior changes and attack scenarios, so you can employ context-aware policy enforcement.

The ZingBox solution is based on a simple assumption. In order to succeed, an attacker must perform key actions. Once actions are taken, it will cause some deviation from the standard behaviors the IoT device normally exhibits; otherwise, the attacker won’t be able to achieve anything. So with machine learning, IoT Guardian is able to uncover the underlying behavior of a bad actor that is not visible in logs. To extend the Theatre analogy, these bad actors can change their costumes and put on different masks, but they still must behave out of the ordinary to cause damage and that’s how ZingBox is able to identify them.

In this way, ZingBox IoT Guardian is able to provide unparalleled visibility into an organization’s IoT infrastructure, revealing vulnerabilities and hidden threats, and thus allow real-time policy enforcement to be applied.
A New Framework for Securing Vulnerable IoT Devices

The new ZingBox framework for securing a vulnerable IoT infrastructure is as follows:

<table>
<thead>
<tr>
<th>Vulnerable IoT Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT Discovery &amp; Visibility</td>
</tr>
<tr>
<td>Fing, identify, and classify IoT assets for situational awareness</td>
</tr>
<tr>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Analyze IoT behaviors to detect overall risk exposure</td>
</tr>
<tr>
<td>Context-Aware Policy Enforcement</td>
</tr>
<tr>
<td>Apply context enabled policy framework to manage categories of IoT devices</td>
</tr>
<tr>
<td>Real-Time Threat Detection</td>
</tr>
<tr>
<td>Employ machine learning threat detection without any presence on IoT devices</td>
</tr>
<tr>
<td>Forensic Analysis</td>
</tr>
<tr>
<td>Apply threat analysis and correlation to identify root-cause</td>
</tr>
<tr>
<td>IoT Threat Intelligence</td>
</tr>
<tr>
<td>Share IoT threat intelligence and knowledge</td>
</tr>
</tbody>
</table>

Secured IoT Assets
ZingBox IoT Guardian’s Three-Step Process

With a three-step process of Discover, Profile, and Protect, ZingBox IoT Guardian delivers a real-time threat detection and mitigation solution for IoT infrastructure. It safeguards IoT devices from both external and insider threats without intruding on operations or impacting performance.

- **Discover** — IoT Guardian finds, identifies, and classifies all of IoT devices into various device categories.
- **Profile** — IoT Guardian performs risk assessment by analyzing the IoT assets’ behaviors. The ZingBox solution also generates IoT context and sends them to a SIEM (Security Information and Event Management) for enhanced correlation of threat vectors.
- **Protect** — With its machine learning algorithm, ZingBox IoT Guardian applies real-time anomaly detection to proactively secure IoT devices. It also provides a context-aware policy framework for real-time enforcement.

Summary

To fully secure IoT devices and an organization’s other assets and networks, IDS/IPS solutions are not up to the task. An additional new kind of solution is required, like the one developed by ZingBox. Using machine learning and other innovative technologies, the ZingBox IoT Guardian security solution provides you with unparalleled visibility into your organization’s IoT infrastructure. It will reveal existing vulnerabilities and hidden threats, so you can employ context-aware policy enforcement.

ZingBox currently has successful deployments in Fortune 500 multi-national corporations. To learn more or sign up for a free trial, please visit our website at [www.zingbox.com](http://www.zingbox.com).

About ZingBox

ZingBox is an enterprise Internet of Things (IoT) security provider. The company was founded in 2014 by veteran tech industry leaders in networking and security. ZingBox was recently named one of *Silicon Valley’s hottest security startups* by NetworkWorld.