Thingate™

Cybersecurity for the Internet of Things

THE INTERNET OF THINGS AND CYBERSECURITY

The definition of what constitutes an IT endpoint in the modern enterprise has changed profoundly, as hardware innovation coupled with advances in networking technology have made it possible to network a vast collection of previously disconnected and highly-varied devices. Abstractly referred to as things, since they lack any kind of common physical, computational or functional identity to warrant a more descriptive label, these newly interconnected devices and objects have expanded the breadth of the internet and intranets exponentially. Standing at more than 7 billion today, some forecasts estimate more than 20 billion unique devices will be operating in the global Internet of Things by 2020[1].

While this explosive expansion indicates another remarkable innovation in networking, the rapid pace of IoT has far exceeded the advances in cybersecurity necessary to ensure its safe and measured growth. IoT devices with minimal or absent security are potential weak links in the enterprise, and can be used both as pivots and exfiltration points for attackers. Because so many devices in the IoT connect directly to high-value cyber targets, such as financial and personal data, and are many times cyber targets themselves due to their critical functional roles, a strong IoT cybersecurity strategy is an essential component of today's enterprise security architecture.

IOT SECURITY CHALLENGE

Enterprise networks with an IoT subnetwork have exposed a new, large, and highly vulnerable attack surface to the cybercriminal community. And even

COMMON IOT DEVICE VULNERABILITIES

- Weak or absent authentication procedures
- Not designed to support endpoint security technologies
- Direct accessibility from multiple points on the network
- Weak or absent data encryption over the network
- Limited cybersecurity support from OEM
- Detectable and collectible wireless broadcast signals
- Published and open operating procedures

1 Impact of IoT on Business. Gartner, 2016.

as device OEMs have increased their cybersecurity awareness and begun to take measures to shore up their devices' vulnerabilities, many questions remain unaddressed:

- Do all IoT devices have the compute resources necessary to support effective endpoint security?
- Will IoT device manufacturers commit to lifecycle maintenance to include security patches?
- Are IoT devices patchable and upgradable as new vulnerabilities are identified?
- Given the relative simplicity of some IoT devices, is it cost-practical to build in security for all endpoints?
- What cybersecurity features are most appropriate for which IoT devices, and is there a common security framework that can be applied to all IoT devices?
- Is there enough commonality among IoT devices to provide a singular, comprehensive solution that meets all IoT cybersecurity requirements?
- What can be done to prevent the IoT from devolving into an unmanageable collection of disparate IT platforms, each with their own unique vulnerabilities and separate cybersecurity requirements?

These are daunting issues for any CIO or CSO responsible for the security of the enterprise. As the boundaries between operational technology and information technology continue their convergence, cybersecurity must be at the forefront of any IoT growth and management strategy, and the unique topology and composition of the IoT requires a new approach to traditional cyber defense strategies.

What is needed is a single cybersecurity platform that can protect the entire IoT, regardless of the devices' resources and functional role in the IoT. Such a platform would remove the burden of managing the cybersecurity of each individual device, and render concerns such as the discovery of new vulnerabilities, cybersecurity requirement diversity, and life cycle security

support irrelevant. It is these objectives that are the very basis of the Thingate™ product line.

THINGATE™

The Thingate solution has been expressly designed for the diverse function, platforms and topology of the IoT, with a feature set that can:

- Render the networked IoT device invisible to hacker reconnaissance
- Prevent the unauthorized command and control of the IoT device
- Isolate the IoT device so that it may not be used as a pivot point to other network assets
- Obscure data transmitted to and from the IoT
- Prevent the exfiltration of data through an IoT device
- Prevent intentional disruption of service
- Distinguish malicious intent from normal operational control
- Detect and report suspicious cybersecurity activities
- Generate, store, and forward forensic data for security event analysis

Designed specifically as a security solution for the devices comprising the Internet of Things, Thingate™ by Vaxxin, Inc. provides comprehensive defense of the IoT. Thingate can be incorporated seamlessly into an existing cybersecurity architecture, or function as a stand-alone solution, creating a protective barrier around the IoT. By combining both well-established and newly developed security principles with a thorough understanding of IoT device networking topologies, Thingate defends the IoT from both internal and external exploitations.

Thingate is a software-based solution, delivered on a small form factor security appliance. A best practice deployment of the technology dedicates one Thingate appliance per area of defense, such as a wing, a production floor, or

even an individual room. Thingate establishes IoT micro-segments, resulting in a series of secure enclaves. Any device, whether wired or wireless, within Thingate's protective halo will be defended by the Thingate cybersecurity feature set:

1. **Device Obscurity** – Thingate renders devices effectively invisible on the network. Devices within the protective halo are readily visible and accessible to valid, authorized users. Unauthorized users probing the network will only see Thingate--an unidentifiable, hardened platform, with no indications of its location, purpose, or the fact that there are protected devices behind it.

2. **Wireless Signal Security** – Thingate limits the propagation of the device's wireless signal making it impossible to detect and collect the wireless dialogue necessary to conduct an attack from beyond the Thingate security halo.

3. **Access Contro**l – Thingate provides strong authorization and authentication controls for adding devices to the secure IoT enclave. Network administrators can view and manage the authorized devices in the IoT through a single user interface.

4. **Traffic Management** – Thingate provides traffic control for any devices within the halo, both wired and wireless, inspecting and vetting all inbound and outbound traffic. Devices are configured to be accessible only via Thingate, which protects all network actions targeting or originating from the device.

5. **Encryption and Authentication** – Thingate AES-encrypts the payloads of transmissions made to and from the devices it protects. Network transmissions through the protected channels require strong, validated credentials issued by the originating end of the channel and authenticated by the destination upon receipt.

6. **Logging and Eventing** – Thingate generates logging data on behalf of the IoT, and triggers events to alert network operators of suspect traffic and likely attack attempts. This data can be analyzed either locally, or formatted and forwarded to a SIEM or other network forensics system for analysis.

7. **Anomaly Detection** -- Deep packet inspection and the Thingate analytics engine inspect and analyze traffic bidirectionally for anomalous network behavior and content.

8. **Packet Capture** – Thingate can be configured to provide rolling packet capture of data going into and out of the IoT. PCAPs can be stored and analyzed locally, or forwarded to other cyber forensics tools for post event analysis or general usage monitoring.

THINGATE TOPOLOGY

The Thingate™ solution consists of two separate components; Thingate Defender, a small form-factor cybersecurity appliance deployed at the intersection of the enterprise network and the IoT, and Thingate Controller, a management and control server deployed either on premises or in the cloud.

The Defender serves as the cybersecurity gateway into and out of the IoT. Depending on the client's IoT topology and network architecture, a single Defender could protect the entire IoT, although a typical deployment involves Defenders installed at multiple locations throughout the IoT. The Thingate cybersecurity feature set is applied to all traffic bidirectionally, creating separate secure enclaves at each Defender location.

The Controller provides management and configuration services for the Defenders, as well as access controls for all authorized IoT devices. In addition to the Thingate cybersecurity feature set, the Controller also serves as the central system for:

- Configuring Defender security policies
- Managing security certificates
- Storing and forwarding PCAP files
- Storing and forwarding log files

The Controller can be deployed on an enterprise class server when organizational security policies require data to remain on premises, or run entirely in a public or private cloud.

AGENTLESS EXTENSION OF ENTERPRISE CYBERSECURITY SYSTEMS INTO THE IOT

When integrated into an existing security infrastructure, Thingate complements the capabilities of enterprise cybersecurity systems and extends their reach to the devices comprising the IoT. Through close collaborative relationships with Vaxxin's cybersecurity partners, the Thingate feature set has been built to interoperate seamlessly with:

- Security Event and Incident Management (SIEM) Systems
- Traffic Flow and Packet Analysis Systems
- Informatics Systems
- Proprietary Enterprise Security Management Systems

Thingate generates log data on behalf of the IoT, and creates events based on correlative analysis of IoT data. The Controller can be configured to format and forward this data for ingest by a designated SIEM engine for further data analysis and broader event correlation.

The Controller can also be configured to perform rolling packet capture on data going into and out of the IoT. The PCAP files can then forwarded by the Controller to 3rd-party cyber forensics tools for packet analysis and visualization.

Because Thingate is agentless, every device within the IoT can be brought under the protection of the network's enterprise security systems, regardless of the IoT device's compute and networking resources.

Thingate's close relationship and proximity to the devices it protects allows for the extension of function-rich endpoint management solutions to include the devices on the IoT network. When deployed in conjunction with an endpoint management system, Thingate enables enterprise features such as inventory and asset discovery, use analysis, and security compliance at the very edge of the enterprise network. For clients that have made the investment in both an endpoint management capability and a SIEM, Thingate makes it possible to achieve a true closed loop detection, investigation, and resolution solution for all enterprise endpoints to include the network of IoT devices.

Thingate maximizes the investments made in enterprise security systems by extending their reach and visibility to include the endpoints in the IoT. Deploying Thingate as part of a comprehensive enterprise security strategy is a non-invasive way to bring visibility and cyber management to the previously unseen, unmanaged and unprotected IoT subnetwork.

BLOCK ILLICIT SIGNAL COLLECTION AND EAVESDROPPING IN THE IOT

The wireless technologies that support the IoT are subject to interception and eavesdropping. Common wireless attack methods involve the collection of the dialogue between the devices in the IoT and their assigned wireless access points. This can lead to either on-premises attacks against the access point and IoT device, or an offline exploitation of the collected traffic.

Thingate protects the wireless signals emanating from the IoT through strong encryption, and management of wireless signal propagation. The Defender functions as a highly localized wireless access point, providing close range wireless connectivity to the devices in the IoT, then connecting via VPN to the existing wireless infrastructure and encrypting all traffic transiting the Defender. The Defender can be tuned to restrict the broadcast range of the wireless signal to a controllable and observable radius that prevents concealed and illicit collection. Whether a wing, a floor, or a single room, the wireless signal range of the Defender can be customized to meet the specific security requirements of the environment in which it is deployed.

A NEW SECURITY MODEL FOR THE INTERNET OF THINGS

Thingate represents a new paradigm in cybersecurity, adapting traditional network defenses to the evolving topologies of the Internet of Things. By consolidating all IoT-relevant security measures into a single platform, the devices within the Thingate secure enclave are protected, regardless of their networking technologies, computing resources or inherent vulnerabilities.

Thingate™

Cybersecurity for the Internet of Things

Moreover, as a purpose-built infrastructure IT device, Thingate is not subject to the same regulatory oversight as some IoT devices, and can be updated and patched routinely in response to the rapidly evolving cyberthreat landscape. The IoT is often the intersection where the network meets operations, and it is that proximity that makes IoT device security such a critical requirement. Thingate provides a comprehensive cybersecurity solution for that most vulnerable subset of the enterprise, protecting devices from the increasing threat of cyberattacks and ensuring the safe operation of the IoT.

About Vaxxin

Vaxxin was founded in response to the rapid cross-industry growth of the Internet of Things (IoT), and the increasing cyber vulnerabilities that threaten to impede IoT growth. By combining deep expertise in cybersecurity, encryption, wireless technology, and traffic analysis with patents-pending design concepts, Vaxxin delivers purpose-built solutions designed for the cyberdefense and cybersafety of the Internet of Things.

sales@vaxxin.com

1-844-IOT-CYBER (468-4283)

6701 Democracy Boulevard
Suite 300
Bethesda, MD 20817

www.vaxxin.com

Vaxxin™

Vaxxin-BR100001.0317-Technical-Brochure