Secure Your Entire IoT Ecosystem

Equipping inanimate objects with microprocessors and Wi-Fi connectivity and linking those "things" with powerful analytics engines in the cloud is fundamentally altering the way we live and work. The productivity gains are astounding, yet the rate with which we are expanding our cyber-attack surfaces is unprecedented.

This need to control and manage the rapid influx of connected devices and the supporting cloud and network infrastructure makes managed security services more critical than ever. Managing connected things as signals transit from the cloud to the application and back again is a large and complex problem requiring a foundational approach and framework to support an organizational strategy.

New Endpoints; New Attack Vectors

Every new endpoint or asset you connect to your network potentially adds another attack vector, and multiple endpoints often involve a mixture of sensors, networks, systems and software from a variety of vendors. For the most part, no two IoT devices are alike and they often utilize custom protocols, for which there is no support.

Additionally, IoT devices lack a lot of the handy data features such as syslog, of modern desktop operating systems, and many devices do not use TCP/IP to communicate, so basic connectivity checks such as ping don’t apply. Repeat this 1,000 times for 1,000 different devices and protocols, and the complexities spiral.

An IoT Cybersecurity Architectural Framework

The nature of the endpoints and the scale of aggregation require a unique approach in the overall architecture to accommodate these challenges. This why we developed a patented IoT Cybersecurity Architecture that we provide our clients free of charge to assist with their planning for the future support of their IoT management initiatives.

Because IoT entities will generally not be defined in a single-use, single-ownership configuration, the devices and the control platform on which data may be consumed and shared could have different ownership, policy, managerial and connectivity domains. Consequently, devices will be required to have equal and open access to a number of data consumers and controllers concurrently, while still retaining privacy and exclusivity of data where that is required between those consumers.

Information availability while providing data isolation between common consumers is critical.

Identity Controls and Trust Relationships

Therefore, appropriate identity controls must be established and trust relationships developed between entities to share the right information with the right entities at the right time and place.

We have created a platform framework that addresses

- The ability to authenticate multiple networks securely while ensuring that data is available to multiple collectors concurrently
- The need to manage the contention between that data access and privacy concerns between multiple consumers
- The requirement to maintain availability of the data or the service while allowing for contingent evolution through the discovery of unknown risks.

These issues are uniquely important to IoT because the secure availability of real-time data is critical. As in one simple example, an industrial process may rely on continuously accurate and timely temperature measurement and if that endpoint is undergoing a Denial of Service (DoS) attack, the process collection agent must immediately recognize the attack and be able to execute counter-measures in real-time.

These counter-measures may involve re-directing the sourcing of data to a secondary connection, or an alerted delay in the transmission of information. Our IoT platform architecture accommodates this condition and may others that are endemic to the IoT world.

A Complimentary Architectural Service

We offer the patented architectural framework as a complimentary service to our customers because we understand the enormity of the complexity that integrating IoT presents. We believe the framework provides our customers with a baseline for developing their own IoT strategy and managed services definition.

With more than 20 years of penetration testing, product security risk assessment, managed security services and Netswitch's award-winning integrated security defense system, Securli®, our team has been operating on the front lines of cyber-defense where the real battle has been joined.

Never Breached

Netswitch is a unique cybersecurity company in that we offer the background, credentials and successful track record in complete IT and OT assessment, 24x7 operational monitoring, management and remediation with the skills to develop advanced architectural frameworks for future paradigm shifts.

As of today, no Securli® customer has ever been breached.

About Us

Founded in 2000, Netswitch provides advanced IoT Managed Security Services and IT/OT infrastructure support in the U.S. and Asia through offices in San Francisco, Phoenix, St. Louis, Bangkok, Thailand and Hong Kong.

To contact us, please send us an inquiry through our website at www.netswitch.net or to your local Customer Success Manager.