AT&T Business

Help increase the security of your IoT deployments with Cybersecurity Consulting from AT&T

The Internet of Things (IoT) is the process of deploying network-enabled devices, communications solutions, and applications, layered with analytics, to help enhance business processes and operations.

The benefits of adopting IoT are tremendous as it helps reduce costs to the business, while improving efficiency and productivity. Gartner Says 8.4 Billion connected "things" will be in use in 2017, up 31 percent from 2016.

However, as IoT continues to grow, securing the IoT ecosystem becomes more imperative. The security of this technological ecosystem and the data that it generates should be a fundamental requirement for every enterprise seeking to increase the agility of their operations through IoT deployments.

Potential Benefits

- Holistic approach
- Modular and layered security services
- Understand and manage risks around security and privacy
- Prepare response strategies for IoT

Program Management Services

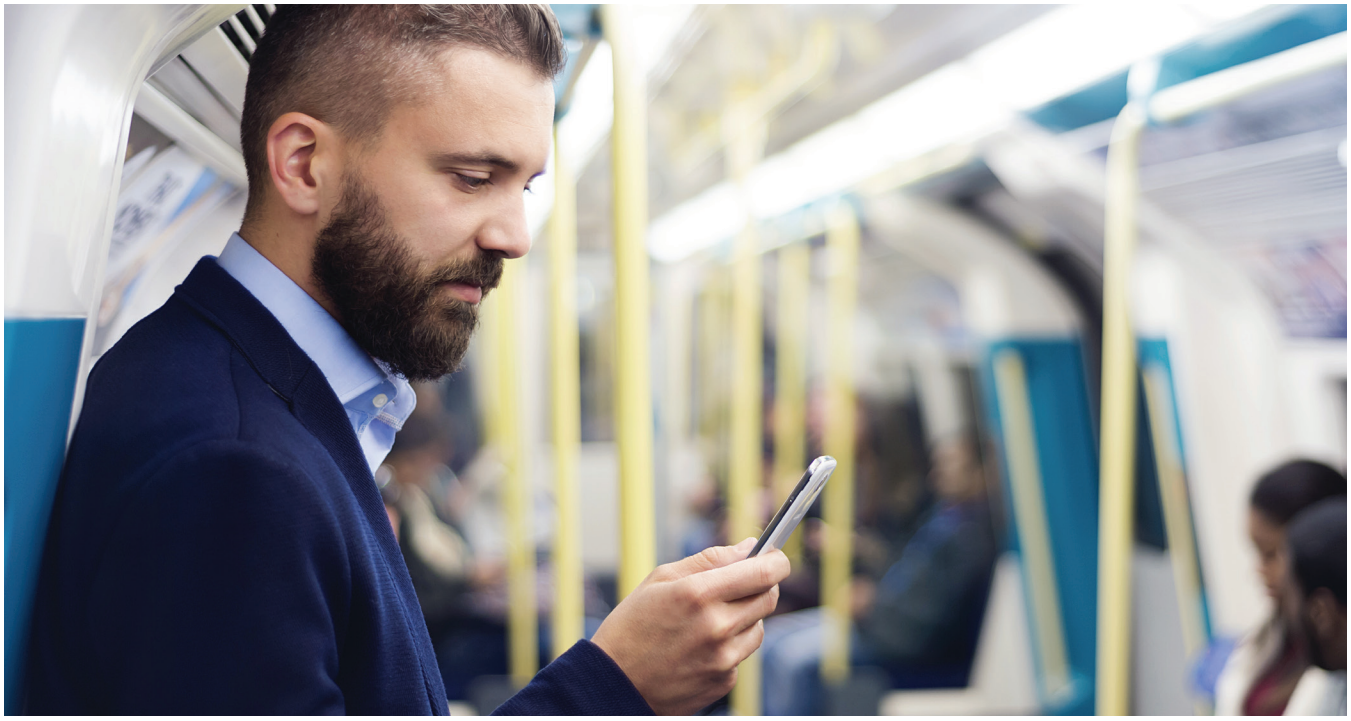
IoT-enabled processes should not only align with business objectives but also take into account the possible positive and negative impacts they may have for the organization and its users. In order to help minimize the potential impacts to enterprise security and compliance programs, it is necessary for organizations to take a holistic, risk-based approach when evaluating the security of IoT devices and their deployment. Effectively securing IoT environments involves security for both IT (Informational Technology) and OT (Operational Technology). We suggest organizations follow a multi-layered security strategy to help see to it that critical security considerations are included throughout the project lifecycle. This is in the context of an over-arching risk management framework to properly align the cost and complexity of controls with the level of exposure posed to the environment by identified risks.

For this reason, AT&T Cybersecurity Consulting offers security services for IoT. Through our IoT Security lifecycle services, we help you to see to it that the entire IoT ecosystem is designed, implemented, managed, and monitored efficiently and in a manner consistent with internal security policy, best practices, and industry regulations. Ultimately, we help you develop a sustainable model for your IoT security practices.

Our IoT Security Lifecycle services start with a review of a customer's objectives, current processes, and compliance requirements. We then combine elements of information risk management, security operations and response capabilities to help enterprises establish a comprehensive approach to IoT security.

With a full suite of IoT Cybersecurity professional services we can provide a breadth and depth of services, matched to the specific needs of your business which includes helping with issues such as:

- Continual vulnerability assessments and targeted penetration testing;
- Risk and threat analysis;
- Maintaining privacy;
- Providing data integrity;
- Security of software applications supporting IoT;
- Reviewing and developing operational processes;
- Standards compliance.



Layered Approach to IoT Security

The Internet of Things (IoT) promises different value based on your industry and role within your organization. For you, it may be bringing your building's existing climate control system online to conserve energy and save money. For someone else, it may be embedding a new networked medical device that improves health and increases quality of life. The IoT is made up of the convergence of two worlds----- cyber-enabled legacy systems and connecting newly emerging smart devices. But along with the multitude of benefits, this IoT convergence creates attractive new targets for malicious threats. Traditional security strategies have focused on prevention. They use one general line of defense (called a perimeter) to help prevent attackers from accessing privately stored information. Due to emerging technology trends and the surge of connected devices, hackers are always finding new ways to attack.

IoT security risks continue to be more complex and frequent. Malicious attempts can now be staged from multiple points. Implementing security at multiple layers throughout the enterprise helps keep businesses protected at each tier of defense. AT&T Cybersecurity Consulting Services span the end to end security needs of organizations adopting IoT. Our offerings help address the security needs across the different layers of IoT.

IoT security requires a multilayered approach

Multiple threat types across IoT devices, data, and networks require a variety of cybersecurity methods --- including a proactive approach to identifying and responding to threats.

Data and Application Security

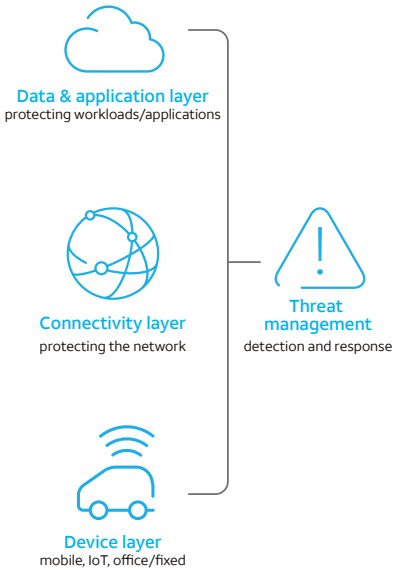
- Sensitive Data (PII) security/Privacy and governance review.
- Security analysis of the critical applications driving your IoT product ecosystem.
- Web and mobile application security testing to uncover software vulnerabilities, demonstrate the impact of weaknesses, and provide recommendations for mitigation.
- Performing code review and evaluating highly secure coding practices.

Connectivity Layer Security

- Security testing includes an assessment of the wireless protocols used for local device communication, such as ZigBee, 6LoWPAN, and Bluetooth LE, to provide for proper implementation and security best practices.
- Security assessment of external cloud services and RESTful APIs used to exchange data with IoT networks, applications, devices, and sensors. Vulnerabilities are identified, and if desired, exploited during a penetration test.

End Point (Device) Security

- Conduct an in-depth security assessment to identify physical and logical security threats to the embedded system, such as local controllers/ gateways, and determine risk at the device level of an IoT ecosystem to help your organization establish appropriate mitigations.
- Conduct an analysis of the connected devices to the organization's network and explore the interconnections of the connected IoT devices.
- Conducting ongoing vulnerability assessments and penetration testing exercises to see to it that end points are protected against the latest threats.
- Analyze the security of device firmware and firmware patch update process to see to it that security best practices have been implemented, such as cryptographically signing firmware updates and using authentication capabilities in hardware devices to verify signatures.



Threat Management

It's crucial to have an IoT security analytics capability that helps you best understand your network by allowing you to flag anomalies that might be suspicious or dangerous, malicious or not. We offer threat intelligence based on deep network visibility and continuous monitoring at the network level. We use context aware/behavioral analytics to understand how hardware is being used, where it is being used and who is using it in order to detect abnormalities. This can be done at the connectivity, device, or data/application level. We also provide threat vector insights on specific IoT implementations based on our experience and visibility in the IoT space.

Why AT&T

AT&T is a global leader in IoT, connecting millions of devices and machines globally through the experience of AT&T's highly secure network. As a leader in both IoT and Security, AT&T is uniquely positioned to provide key insights and end-to-end security capabilities to our customers.

AT&T is committed to providing security and reliability to our IoT customers, offering and unparalleled visibility into threat detection across our network, applications and customer devices.

It's our business to help protect your business.

- Network visibility and control with threat intelligence and response capabilities.
- Expertise of global security experts and researchers combined with best-in-breed strategic alliances.
- Experience managing customers' networks.

For more information, contact an AT&T Representative at 877.542.8666
or visit https://www.business.att.com/solutions/Family/cybersecurity/consulting.

Share this with your peers