WelbeckConnect

Assuring the Internet of Things

- ***$2.5 million***
  Spending on IoT hardware per minute
- ***28%***
  Annual growth rate of the IoT market
- ***50 billion***
  Connected devices by 2020
- ***$1.7 trillion***
  Market size by 2020

The Internet of Things (IoT) is reshaping every aspect of business and modern life, ranging from building security, healthcare, power and water, to manufacturing and industrial control systems. The IoT enables new applications and business services such as robotic manufacturing equipment and self-driving vehicles that can communicate real time data to the cloud and receive back instructions – all without any human intervention.

With annual growth of 28% the IoT is becoming one of the largest IT markets globally. According to Gartner, 2016 spending on new IoT hardware will exceed $2.5 million *a minute*. The total value of the IoT market is expected to exceed $1.7 trillion by 2020 according to IDC, and Cisco estimates that there will be 50 billion connected devices by then.

IoT is not without its challenges – assured connectivity and security are not a given. Connecting special-purpose devices to the internet is not always easy, and the reliability it demands is not always available. Moreover, the vulnerability of the IoT devices, their data, and the computer systems to which they connect all increase as more control surfaces become visible to and accessible from the internet.

The Internet of Things' Biggest Challenges

> "Devices, designed and fielded with minimal security requirements and testing … could lead to widespread vulnerabilities in civilian infrastructure and U.S. Government systems. 'Smart' devices incorporated into the electric grid, vehicles, and household appliances … can threaten data privacy, data integrity, or continuity of services."
> -Director of National Intelligence James Clapper

The challenges you face with applying the IoT to your business model or mission/purpose are not how the data will be generated or utilized; rather, the greatest challenges rest with achieving *assured connectivity* and *security* of the devices, transactions and networks. Implementing and operationalizing IoT applications and devices can only deliver on the promise if connectivity is available, reliable, and secure.

Assured connectivity is a challenge. Connecting reliably to the internet and remote networks is not easy. Communications may not be available and establishing the connection will often require complex, expensive network configuration. Moreover, to protect the networks to which devices connect requires device authentication – not an easy task with millions of remote, unmanned devices.

Security of IoT systems must address the threats from outside agents such as man-in-the-middle attackers who can hack into the communication stream to access data and devices. Yet *most IoT devices have no or low encryption* – indeed many older devices and some modern ones do not have the computing power to encrypt data or to run protective software.

Internet of Things' Security Risks

- ***73,000 security cameras hacked***
- ***30 million health records breached***
- ***POS terminals/card swipes hacked daily***
- ***20% of smart buildings "digitally vandalized" by 2018.***

The security challenges of IoT expose not only the data in transit (such as 73,000 streaming video cameras that were exposed by a Russian website in 2014) or personal health records (almost 1,000 HIPAA violations since 2009 reported by HHS, affecting more than 30 million Americans), but also the critical equipment with which the IoT devices communicate, such as automated mass transit systems and GPS systems.

The supply chain of the equipment has become a major vulnerability, often yielding a threat from within. Built or modified by bad actors, the communications devices themselves may allow unknown backdoors that divert or corrupt sensitive traffic or allow unauthorized access. This has already been seen, for example, in the case of point-of-sale credit card terminals that are actually sold to merchants pre-provisioned to steal and transmit credit card information when a card is swiped.

The Welbeck Solution

WelbeckConnect
IoT Implementations

- Healthcare
- Facilities Security
- Critical Infrastructure
- Water Quality
- SCADA Systems
- Access Controls
- Smart Buildings
- Video Surveillance

WelbeckConnect was formed to address IoT's connectivity and security challenges and enable IoT-based applications and businesses to operate reliably and securely. The company is U.S. owned and its proprietary software was developed in the U.S. with FIPS 140-2 compliant encryption.

The Welbeck IoT Gateways provide the same assured connectivity and security for the Internet of Things that is already in use by Fortune 500 companies and others for enterprise networking. Our Ethernet-over-IP approach to connectivity is agnostic to the interface or protocol, enabling us to connect legacy systems that were not designed to use Internet Protocol at the transport layer. Our proprietary technologies automatically authenticate the IoT device (X.509 certs) and establish an encrypted (TLS v1.2, AES 256, FIPS 140-2 compliant) tunnel end-to-end without port-forwarding or other configuration on the remote router or firewall. Our approach to encryption uses very little bandwidth, allowing us to encrypt to AES 256 levels and higher without creating the latency that can disrupt many IoT applications using older IPsec VPNs.

We also solve the challenges of poor internet service quality. We overcome latency, packet loss, jitter and fragmentation issues that often render connections unreliable or even unusable. If internet connections are not readily available, our 3G/4G cellular units provide secure access over existing cell networks. The Welbeck IoT Gateways are also fully interoperable with any communications medium including RF, Satellite and TV Whitespace. All of our products provide integrated failover redundancy and the capability to bond multiple links and load-share.

Our products range from cost-effective compact appliances for remote connections up to rack-mounted concentrators, virtual appliances (VMware, ESXi, Hyper-V and Oracle VirtualBox environments) and cloud instances (Microsoft Azure and Amazon Web Services – AWS). Our self-contained devices provide their own computing power and OS to run our suite of assured connectivity and security software – so that we can connect and protect even low-end/low power devices such as PLCs, RTUs, unitaskers and legacy sensing equipment.

Contact:

Walt Rogers
wrogers@welbecksecure.com
240 395-2401

Bob Smith
rsmith@welbecksecure.com
240 395-2411

WelbeckSecure.com

WELBECK
SECURE