

Internet of Things:
**Enterprise Security
and Control**
OVERVIEW

The Internet of Things (IoT) refers to all the network-connected electronic devices that are becoming common place in the consumer and enterprise markets. They range from TVs, cars and home automation systems for consumers; to medical devices and enterprise energy efficiency systems that add ease and convenience to our daily lives.

The challenges presented by this new generation of devices are:

- They communicate by automatically connecting to networks and so present new unsecured interfaces or entry points.
- The effect of compromise of IoT devices can be very real and result in physical impact (even death) when things go wrong.
- Targets for IoT devices are often consumers for use at home or the workplace; or they can be enterprise solutions that have a wireless/web/cloud/mobile/app capability added to their operation.

ENTERPRISE SECURITY CONSIDERATIONS

Many IoT products in their current incarnations are aimed at the home market, however, enterprise-class equivalents will find a market too.

Securing these embedded devices isn't easy as they don't run traditional anti-malware solutions or allow secure configuration. Four researchers from EURECOM France conducted the first large scale analysis of firmware in embedded devices and found that "[M]ore than 140,000 internet-of-things devices, from routers to CCTV systems contain zero-day vulnerabilities, backdoors, hard coded crackable passwords and blurred private keys"¹.

Check Point research notes that 'Security relies on users changing passwords and other settings away from defaults, and ensuring the devices are not left open'².

When this laissez faire approach carries over to the enterprise market, the risks magnify and go way beyond the traditional security implications of data theft, damaged corporate reputation, fraud or lost privacy. In the healthcare sector as an example, there is a huge responsibility on organisations where serious risks could result from poor security design, operation and monitoring. Beyond the specific risks of this sector, the challenge with many devices is their inherently weak security model that can result in privileged access being gained to any system or the network they're connected to.

There is an inevitability in the rate of adoption of IoT devices and the exponential increase in the number of security weaknesses they bring.

¹ Boffins find hundreds of thousands of woefully insecure IoT devices, The Register, August 17, 2014
² Beware of Suspect Devices, SC Magazine, March 5, 2014

THE “ENTERPRISE NETWORK OF THINGS”

There are a number of proactive steps that can be taken to ensure that effective security is maintained as this next wave of technical innovation spreads through your business:

- **STEP 1** — Plan an IoT-aware enterprise network
- **STEP 2** — Drive business engagement in IoT
- **STEP 3** — Strive for “IoT visibility”

BOTTOM LINE BENEFITS

IoT technology doesn't change the core objective of the security function of the business, however it will change the risk profile of an organisation that adopts it. You must have adequate systems and processes to be able to detect IoT adoption, device activity, failures and any impacts that they may have on the operation of the IT environment and the proper functioning of the business. Rules based policy engines are grossly inadequate in detecting and analysing potential security threats from IoT devices because they don't fit the 'normal' model for IT systems.

Huntsman® intelligent SIEM technology, with its Behavioural Anomaly Detection engine (BAD2) and its machine learning ability to detect anomalous activity in real time, will enable organisations to continuously monitor their estate and IoT facilities so they can quickly respond in the event of any unacceptable security risks. There is an inevitability in the rate of adoption of IoT devices and the exponential increase in the number of security weaknesses they bring.

Huntsman | Tier-3 Pty Ltd

Asia Pacific

t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

100 Pall Mall, St James
London SW1Y 5NQ

North Asia

t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas

toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105



huntsmansecurity.com



linkedin.com/company/tier-3-pty-ltd



twitter.com/Tier3huntsman