Solution Showcase

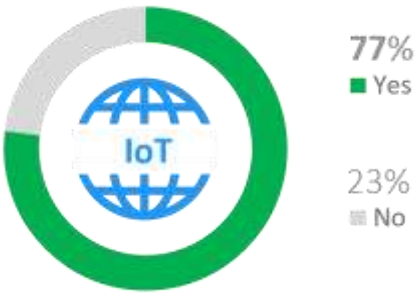
HP Enterprise and IoT Connectivity

Date: March 2016 **Author:** Dan Conde, Analyst

Abstract: Connectivity forms the foundation for all the pillars of an IoT strategy within an enterprise. Given the variety of data sources, protocols, and devices, understanding where to place trust into the flow of the data through the connectivity stack is important. Using an appropriate IoT methodology enables the conversion of untrusted devices into trusted data that can feed business applications and data mining engines.

Introduction – Market Overview

Internet of Things (IoT) consists of connected devices that share information with people, applications, and other machines. The scope and breadth of IoT requires close consideration of security, interoperability, compute, and scalability requirements that cut across information technology (IT), operational technology (OT), cybersecurity, and even marketing organizations. An IoT solution needs to account for and address the requirements of each of the primary stakeholders.



ESG recently surveyed 306 IT and information security professionals from North America, of which 31% worked at midmarket organizations and 69% in enterprise. 77% of organizations surveyed responded that IoT is already impacting their network architecture.[1]

Considerations for IoT Design: Information Technology and Operational Technology

Developing a successful IoT strategy requires addressing the six pillars of IT: connectivity, compute, security, analytics, applications, and services. Connectivity forms the foundation on which the other pillars are built, channeling data to and from the compute systems that handle data aggregation, analytics, and device control. Compute may be done within endpoints, or at the network edge, but without secure connectivity, the data and its sources can't be considered trustworthy.

IoT data sources may be stationary or mobile, wired or wireless, analog or digital, and low or high speed. New contextual data like user or device location may be generated as data traverses from device to data center, opening new data sources that can be mined for business intelligence.

Networking IoT devices present some unique challenges versus traditional enterprise IT networks. Physical media, communication protocols, packet payloads, latency, bandwidth, and even response times vary widely. Data sources can be

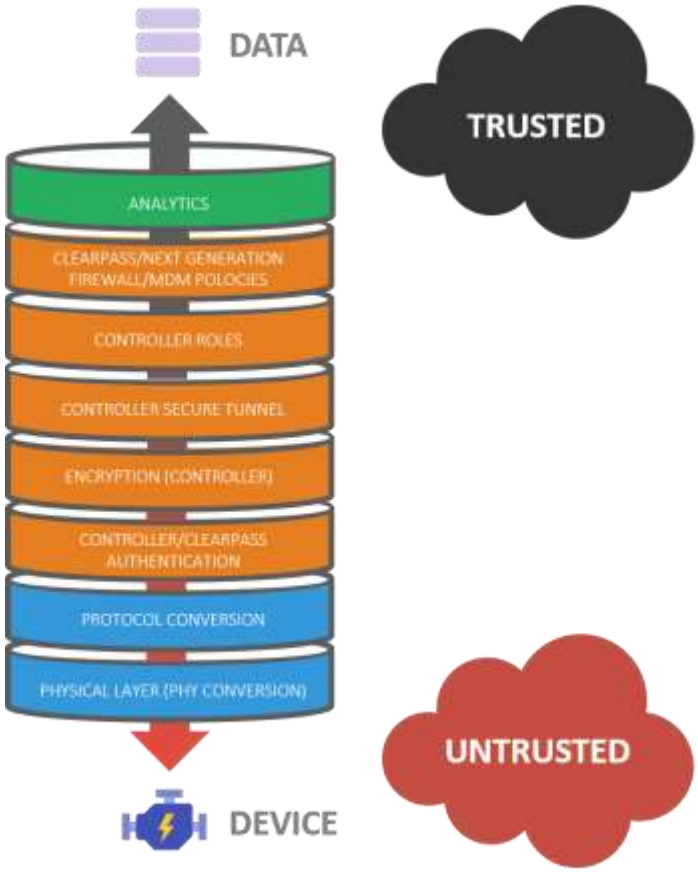
[1] Source: ESG Research Report, *Trends in Data Center Networking*, February 2016.

very diverse, spanning from embedded sensors and actuators, through BLE devices, to oil platforms and aircraft engines. As a result, the IoT connectivity and infrastructure need to work across many protocols and media. Accordingly, solutions are tailored for each application type or vertical market; there is no "one size fits all" IoT solution.

Security Considerations for IoT Design: Connect and Protect

Regardless of the sources of IoT data, it can't reliably be leveraged, or shared with other applications, systems, and services, if the originating devices and transportation mechanisms aren't trusted. Doing so threatens all of the devices, processes, applications, and business decisions built on the untrusted data.

The solution is to build trust where it doesn't exist today, and that is the objective of HP Enterprise's Connect and Protect methodology for IoT. Connect and Protect inserts layers of protective services at points where there is a convergence of native device capabilities, standards-based tools, and access to business-critical data. Protection is augmented by security analytics, SIEM, EMM, and firewalls. The solution is applicable to both legacy and new IoT devices, incorporates security appropriate for both commercial and governmental IoT systems, and is scalable from SMEs to the largest enterprises.



Starting with physical layer (PHY) connectivity and extending through protocol conversion, authentication, encryption, secure tunneling, and role- and policy-based access, and ending with supervisory analytics, the Connect and Protect architecture helps convert untrusted devices into trusted data that can feed business applications and data mining engines.

The Bigger Truth

Any enterprise embarking on an IoT strategy first needs to assess and take inventory of the existing infrastructure to understand the current connectivity requirements and capabilities. Standalone IoT devices may already be in use, and new systems planned, so defining an extensible and flexible architecture that can accommodate both is an important first step. It is best to start small, even in the context of an enterprise-wide IoT project. Choose a small subset in a domain that is well known, and work through the connectivity aspects. Once that project succeeds, apply the lessons to a larger implementation.

HPE Technical Consulting can help review your existing systems and define a Connect and Protect secure connectivity platform tailored to your unique requirements and budget.

This approach will optimize the secure transport and utilization of IoT data by business-critical applications, and create the right framework to generate maximum business value.

For more information, please refer to:

The Connect Protect Whitepaper: Building a Trust-based Internet of Things for Business-Critical Applications
Internet of Things web page for Aruba
The ESG/HPE IoT whitepaper: How to Choose an IT Platform to Empower Your Internet of Things