



Edge Network Fabric™
the Internet *for* Things

Now That Everything Is Connected, Everything Will Get Hacked

Popular Mechanics- April 11th, 2014

Get hacked, compromise data, and deal with a catastrophic business failure, *or* lead with security as a forethought with Xaptum

The current Public Internet was designed to facilitate information download, not to securely orchestrate data exchange between connected Things. The evolution of IoT will bring more than 50B Things online¹ - creating unique security, connectivity, bandwidth, packet routing and onboarding challenges. Consequently, the influx of connected Things on the Public Internet is exponentially increasing companies' attack surfaces, exposing them to unknown cyber threats that have the potential to cripple business operations.

IoT Landscape

- IoT is expected to add over 50B Things to the Public Internet over the next decade.
- With billions of Things coming online and sending data frequently, IoT packets will be small and have predictable payload and security fingerprints.
- Currently, companies are attempting to use historic approaches designed for PCs and personal devices to connect Things at a massive scale.

IoT Challenges

- Poor device security from manufacturers makes connected Things outside of the corporate firewall extremely vulnerable to unknown cyber threats and data theft.
- Manual key provisioning / onboarding used for PCs and personal devices on the Public Internet cannot scale to billions of Things.
- Current cryptographic transport protocols (e.g., IPsec, TLS) are not optimized for IoT traffic patterns.

Xaptum's Offer

- Xaptum is the first licensed ISP for IoT in North America.
- Xaptum's Edge Network Fabric (ENF™) is a software defined, IPv6-overlay network for connected Things, securely orchestrating the flow of data between Things at the edge and backend cloud-based applications.
- ENF™ is a purpose-built, multi-tenant network-as-a-service that puts control in the hands of the data owner.
- ENF™ solves today's largest challenges in IoT through multi-layered security, zero-touch provisioning and intelligent traffic routing - orchestrating trusted data exchange between Things and clouds.

¹ Software.org | BSA Foundation, 2017

Xaptum's Offer: Edge Network Fabric (ENF™)

Xaptum ENF™ is the world's first edge computing infrastructure operating a secure IPv6-overlay network that is purpose-built for IoT. As a software-defined network sitting on top of the Public Internet, the ENF™ secures all of a company's connected Things anywhere in the world and protects the bidirectional exchange of data between generation at the edge and consumption at the backend. In addition to providing a foolproof layer of security, the ENF™ enables touchless IoT onboarding, assigns permanent IPv6 addresses on first use, and dynamically orchestrates data exchange between Things and clouds with 99.999% service assurance.

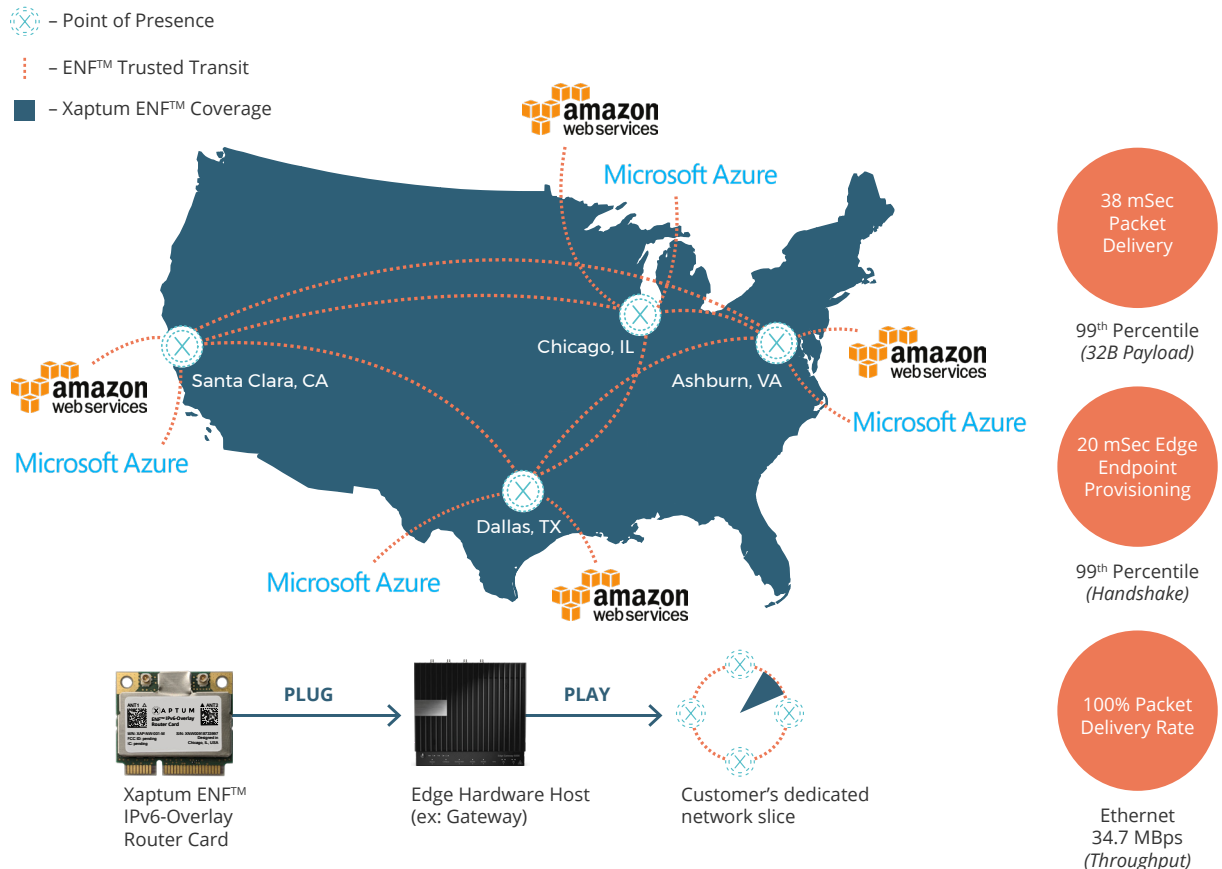



Figure 1: Xaptum ENF™ IPv6-Overlay Network in North America

Xaptum's ENF™ IPv6-Overlay Router Card



- Form Factor: Half Mini PCIe
- Reserved Capacity: Up to 4 MBps on ENF™
- LAN Connection: 1 to 256 (IP Endpoints)
- Access: Ethernet, Wi-Fi, NB-IoT, LoRa, Lte-M
- Power: 350 mA (Peak)/40 mA (Idle)
- Hardware Security: SHA-256, AES-256 Cryptographic Co-processor
- Transit Security: Direct Anonymous Attestation (DAA) with ECDHE Curve 25519 Crypto Suite

Figure 2: Xaptum ENF™ IPv6-Overlay Router Card

Use Case: How Xaptum is Protecting the \$40 Billion Intermodal Freight Industry in North America

\$40 BILLION
NORTH AMERICAN INTERMODAL FREIGHT MARKET

Intermodal freight is a \$40 billion market in North America and it's growing at 8% year-over-year. However, costly fulfillment losses are presenting a serious challenge for 3rd party logistics (3PL) companies, carriers and shippers. Intermodal containers carrying high-value and high-risk goods are experiencing significant issues with damaged, delayed, lost and stolen cargo.

\$900 MILLION
OPPORTUNITY IN LOSS AVOIDANCE FOR SHIPPERS & CARRIERS

Xaptum is working with a leading 3PL to deliver a software-defined, connected freight offering which tracks and monitors freight location along with environmental conditions like temperature, humidity, shock, tilt and more – providing the visibility and insight required to make informed, real-time decisions throughout the logistics journey.

\$300 MILLION
REVENUE OPPORTUNITY FOR A 3PL COMPANY

Thousands of intermodal containers can be quickly onboarded to the ENF™ via a router card that plugs into an IoT gateway that sits inside the container. Once the gateway is turned on, it is automatically provisioned and starts collecting data from cargo sensors and sending back control messages. Additionally, relevant data is sent to the cloud for further analysis when necessary.

Over the next three years, the connected freight offering presents an opportunity of **\$900 million in loss avoidance** for shippers and carriers and a **\$300 million revenue opportunity** for the 3PL company selling the offering to shippers, carriers and other 3PLs. This is an industry-changing opportunity of **\$1.2 billion** based on less than 5% of the available installation base, which is growing at 8% year-over-year.

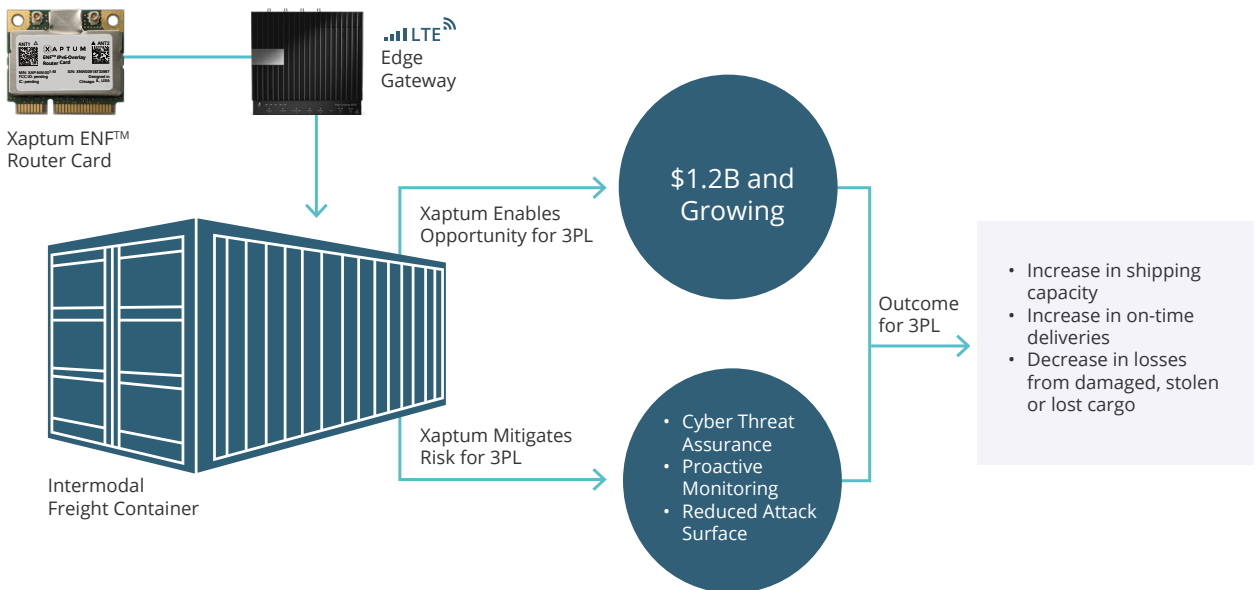


Figure 3: Illustration of Plug-n-Play onboarding with Xaptum ENF™

² Intermodal Association of North America; CNBC News

Our Mission is to Simplify Secure Communication in IoT Forever

Xaptum began its journey in late 2013 as part of the AT&T Foundry's research into 'web of things' concepts. By 2014 the company started its product/market fit and captured initial non-recurring revenue. In 2015, Xaptum became the first licensed ISP in North America to build secure backbone communication infrastructure for IoT. In 2016, Xaptum was seeded by early-stage technology investors, including Jai Shekhawat (SAP-Fieldglass), Wim Elfrink (Cisco), Dan Hesse (former CEO of Sprint) and midwest institutional investor KDWC Ventures (\$300M+ Fund).

Why Xaptum?

451 RESEARCH ON XAPTUM

"....an IP-overlay network similar to a CDN but built specially for the needs of IoT use cases. While many approaches address performance, identity and security challenges in IoT via a variety of device, edge and cloud platform techniques, Xaptum's focus on creating a purpose-built IP peering network, its use of software-defined networking and network virtualization, and its standing as a registered ISP, make it unique and worth tracking..."

AUGUST, 2017

IDC RESEARCH ON XAPTUM

"...only startup listed alongside RSA, Symantec and other heavyweights in the IoT security landscape...."

OCTOBER, 2017

CB INSIGHTS ON XAPTUM

"...leading startup creating edge infrastructure, transforming heavy IoT..."

MAY, 2017

VDC RESEARCH ON XAPTUM

"...digital nervous system for instrumented internet devices - a compelling demo..."

SEPTEMBER, 2013

XAPTUM ENF™ EXTENDS TO THE MOBILE EDGE WITH INTEL & VODAFONE

Xaptum led the way in extending the secure IoT Backbone to the Mobile Edge in a collaborative demonstration to ETSI (European Telecommunications Standards Institute) where Xaptum proved how it could "invoke edge computing". Follow-on over-the-top (OTP) testing on the T-Mobile LTE network resulted in consistent deterministic performance gains of 10x for customers without any changes to the carrier network core. During the testing, ENF™ was benchmarked and endorsed by channel partner, Intel, who has helped to accelerate Xaptum's market leader position.

MARCH, 2017

AT&T INCUBATES XAPTUM!

"....awarded IoT innovator of North America after incubation at the AT&T Foundry for packet routing technology thesis in 'Web of Things'"

SEPTEMBER, 2013

QUICK FACTS

>1 BILLION

Secure packets exchanged on ENF™
100% delivery rate

37

Product and technology gurus who built Xaptum

140

Patents approved or pending by 2018

100%

Focus on security & core networking for IoT

\$8.2 BILLION

Value of companies exited by Xaptum's backers

2

Companies taken public by Xaptum's backers with market caps > \$1B

Get more information: Call: 1-800-398-3694 | Chat : www.xaptum.com | E-Mail: Info@Xaptum.com