avast

Whitepaper

The Future of Secure Smart Homes: Network Providers to Partner with Security Vendors

Table of Contents

Introduction

The challenges associated with securing the IT landscape are already enormous, far-reaching and ever-growing, and the pressure is now ramped even further with the proliferation of the Internet of Things (IoT). Traditional cyber threats, while vast in scale, have focused on traditional IT hardware such as servers and PCs. However, the threat surface is set to become orders of magnitude larger with the billions of additional IoT devices.

Critically, the always-connected nature of IoT devices that integrate the cyber and physical worlds mean that weak cyber security can become weak physical security. If, for example, a connected car is hacked through its tyre pressure monitor, the hacker may be able to unlock the doors or even take control of the vehicle. Similarly, a poorly protected endpoint, such as a baby monitor, can provide a hacker with the necessary access to control other devices on the network, including the home alarm and even the home's smart door lock. Networks are only as strong as their weakest link - just one vulnerable device can compromise the entire smart home network - and the number of homes at risk is enormous.

The rapid growth of IoT devices, both in quantity and variety, into a nascent market, creates immense security challenges and provides hackers with a ripe threat base to exploit. The IoT ecosystem is in need of a security solution that equips modern, connected people and their families to keep their homes safe.

This paper will answer the following questions:

- What are the inherent challenges in securing the huge, complex, and highly fragmented IoT ecosystem?
- How can network-level security utilise artificial intelligence (AI) and machine learning (ML) to secure entire homes?
- Why do network providers have a unique advantage to provide IoT security solutions?
- How can network and security providers help protect the IoT market now and in the future?

1. IoT Threats - The Next Level of Cybercrime

1.1 The perfect security storm

1.1.1 Rapidly growing threat exposure

In the coming years, consumers will flood their homes with a high variety and quantity of connected devices. Juniper Research predicts over 38B smart home devices by 2020; other organizations predict upwards of 50B connected devices. With the convenience and luxury that IoT devices bring, consumers are increasing their exposure to cybercriminals.

38B
connected devices by 2020

41%
homes with at least 1 vulnerable device

1.1.2 The impracticality of on-device IoT security

However, many consumer IoT device manufacturers, such as those producing smart refrigerators, lack the core capability to incorporate security on their devices. Furthermore, by embedding third-party security software into individual devices, they often face cost or size restrictions.

Furthermore, devices that do come with embedded security rely on the consumer to properly configure settings, such as changing the default password and routinely updating and patching software. Research by Avast has found that 40.8% of smart homes worldwide have at least one vulnerable device due to weak access credentials or unpatched software. Today, users already struggle to keep up with

security practices. This challenge will only be exacerbated with the growth in quantity and complexity of IoT ecosystems.

For example, in just a one-month period in 2018, Avast blocked 22.4M malicious URLs on MikroTik routers alone. Despite MikroTik releasing a security patch for their vulnerable devices months before, 95% had not updated their router firmware to be protected against the attack.

1.1.3 Networks are only as strong as their weakest link

Despite the security implications, consumers often disregard the security concerns that come with their IoT gadgets, such as smart light bulbs. At Web Summit 2018, Avast demonstrated how a hacker can exploit a single vulnerable device to quickly access the rest of the network. A seemingly benign device can be the gateway for a hacker to access webcams, computers, house alarm systems, and more.

Graphic: A single vulnerable device can be the entry point for a cybercriminal to access the whole network.

1.2 The prevalence and scale of cyberattacks

Cyberattacks are more common than most people believe. Every month, Avast blocks around 1.5B cyber attacks, globally. While cyber security is improved over many years to protect consumers, cyber attacks are also quickly evolving. In 2018, AV-Test recorded 708M new malware strains that span a variety of malware types.

In 2016, the Mirai botnet carried out a well-publicized attack in Germany. The large-scale distributed denial of service (DDoS) attack on websites and computer systems affected almost one million routers used to access Deutsche Telekom internet services (4.5% of customer base), the German Office for Information (BSI) reported.

1.2.1 Botnets and DDoS attacks

Some malware types are designed to access a huge range of devices by exploiting vulnerabilities to create botnets, a vast network of infected devices to carry out various malicious activity. Examples like the Torii botnet are highly efficient; by targeting very popular architectures such as x86-64, x86, ARM, and MIPS architectures, the Torii botnet can quickly attack and infect a large base of devices.

1.2.2 Ransomware

Additionally, ransomware attacks encrypt private data and demand ransom from victims. In recent years, ransomware has proliferated to impact consumers and enterprises alike. According to Verizon's 2018 Data Breach Investigations Report, ransomware attacks were responsible for 39% of malware-caused breaches. Verizon registered 2,216 breaches over the year, up from 1,935 the previous year.

1.3 The digital and physical threat to consumers

The consequences stemming from IoT security breaches will vary significantly depending on the type of attack. However, it's important to note that some attacks can have enormous and potentially life threatening impact.

1.3.1 Digital attacks are not always noticeable

Despite the high-profile attacks that receive days of media publicity, many breaches stay under the radar so the consumer will never even know their network has been compromised. For example, hackers can use spyware to secretly gather information, such as bank login credentials by monitoring keystrokes. Although the spyware victim may not immediately experience the impact, the consequences can be long-lasting and severe.

1.3.2 Digital attacks can become physical

As consumers continue to rely more on connected devices in their everyday lives, the boundary between digital and physical start to blend. Attackers can exploit a network to disarm home security systems and even unlock smart door locks.

Other examples range from the hacking of a baby monitor to the insertion of malware into connected car systems. For consumers, these attacks mean hackers can have direct communication with infants or even control over a moving vehicle.

Therefore, the security stakes are being significantly raised, and it will be vital that suppliers across the IoT value chain, whether device manufacturers, network service providers or application providers, are able to demonstrate they are providing secure solutions that users can trust.

2. Protection at the Network Level

It's becoming clear that there are many moving parts associated with IoT security, so solutions must be dynamic and span the entire IoT domain. And as discussed before, embedding security into low-value or small devices, such as sensors, is not a viable or reliable model for providers.

A different approach is needed to secure end-point devices. Solutions that can monitor and secure devices at the network level in order to provide an efficient and optimised approach capable of protecting entire IoT ecosystems.

2.1 Network providers have a unique vantage point

Network providers have a key advantage and opportunity to play an important and valuable role in securing IoT devices. Their network infrastructure, whether they are routers, edge gateways, or the core network itself, is the conduit in which consumers access the Internet.

As the gatekeepers to the Internet, their extensive scale, capabilities, and reach allows them to be the ideal central security hub for this fragmented ecosystem. Admittedly, IoT represents a leap further into a multi-billion device arena, but for operators this is only a single order of magnitude greater from the connections they manage today.

Network providers are well-positioned to be the digital safety net for the modern, connected family, and homes.

2.2 Varying levels of network security

Security software today can be applied at three varying levels of the consumers' life - directly in the router, through a hardware extension, and at the network edge. The next years will be years of transition requiring network providers to address the security needs of today and tomorrow.

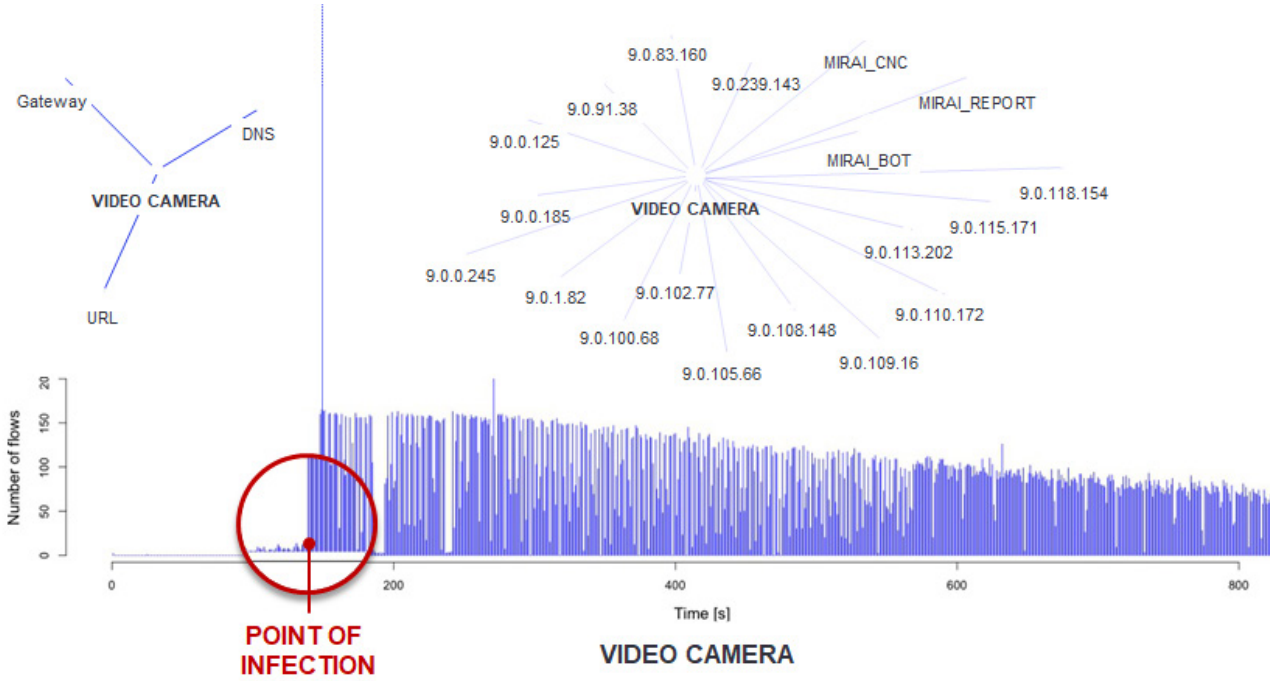
2.2.1 Routers & hardware extension - a central security hub for smart home

Network providers can embed security software directly on routers as firmware or offer

consumers a small hardware attachment to complement their own routers. The router, and attached hardware, provide the solution a powerful vantage point to be a central security hub for all connected devices in the home.

Leading-edge security solutions utilise machine learning to map network trends and patterns for each individual connected device. During an attack, the solution would detect anomalous deviations from normal network trends then work to neutralise the threat.

By abstracting the security burden away from individual end--points, central hubs prove to be an efficient and optimised path to securing smart homes today.



Graphic: Example of a smart home security breach via the Mirai botnet.

2.2.2 The advent of 5G - securing devices at the network edge

However, it is important to note that router security is limited by the boundaries of the home network. As more mobile consumer goods ship with connectivity, it's imperative that mobile operators take part in securing devices that are on-the-go.

Additionally, the advent of 5G and Network Function Virtualization (NFV) in the coming years will begin to blur the distinction between home and mobile networks. More devices will connect directly to mobile networks via hot-spots or virtual routers than ever before.

Network providers can apply the same network-based security solution on the edge infrastructure, such as virtual routers and gateways. Security at the network edge provides consumers with seamless security as their devices fluidly transition between mobile and ISP network connections.

2.3 Benefits for network providers

Certainly, consumers will reap tremendous benefits - for example, the peace of mind knowing their smart homes are secure. However, the clear need for a centralised security solution can be an attractive opportunity for network providers.

2.3.1 Bolstering revenues

Globally, mobile average revenue per user (ARPU) is declining with the introduction of unlimited / cheaper data plans. Mobile network operators (MNOs) are relying on value-added services (VAS) to bolster ARPU, and security services are a great example of that.

Grand View Research predicts the smart home and consumer application segment of the IoT security market will reach $2.9B by 2025. With network providers' strategic vantage point, they can capture a significant portion of the smart home and consumer application segment.

Mobile and internet network providers alike can monetise IoT security to increase ARPUs while maintaining the seamless monthly billing cycle with customers.

2.3.2 Improving retention

Additionally, continued market saturation for networking services has diminished the acquisition scope of new customers. Amidst stronger competition, providers are vying for the same set of customers. Thus, there has been a growing emphasis on retention. Providing compelling services, those beyond traditional connectivity solutions, can achieve more stickiness. Conversely, in some cases, the lack of valuable services can be a driver for customer churn.

2.3.3 Reducing infrastructure load

NETSCOUT's annual infrastructure security report reveals that 57% of enterprises and 45% of data centre operators saw their internet bandwidth saturated in 2017 because of DDoS attacks. There were 7.5M DDoS attacks in 2017, according to NETSCOUT's data, illustrating the already huge scale of the problem even at the earliest stages of the IoT boom.

2.3.4 Avoiding negative publicity

Furthermore, more than half of respondents to NETSCOUT's research that experienced a DDoS attack resulted in downtime. Apart from an increase in operational costs due to technical overload, cyberattacks can also impact end consumers in a variety of ways - ranging from network disconnectivity, loss of corporate intellectual property, or even exposure of personal data. Ultimately, network providers face reputational and branding challenges that are inherent as the conduit of network traffic and data.

3. Partnering with Security Providers

Network providers hold the key to an attractive opportunity, but carry a significant responsibility to keep their customers safe. However, network providers are not expected to reinvent the wheel and develop security solutions outside their core business. Joint partnerships with security specialists, like Avast, can help deploy leading security products to their networks.

Achieving a successful partnership between security vendors and MNOs requires collaboration. This partnership aims to create tangible benefits for both network providers and security vendors.

- Network providers are able to operate a more secure and stable network
- Security vendors attain greater scale, further improving their threat detection and machine learning networks

In a truly non-zero-sum partnerships, network providers hold the key to providing a safe, connected future. Consumers can have peace of mind knowing their digital, and often physical, lives are protected.

4. About Avast, the global leader in digital security products

Avast has 30 years of experience in cyber security, and keeps more than 400M global devices protected from cyber threats today. Its threat detection network is among the most advanced in the world, using machine learning and artificial intelligence technologies to detect and stop threats in real time. Artificial intelligence is only as good as its data - Avast's cloud-based machine learning engine receives a constant stream of data from the company's global users that facilitates rapid learning.

Additionally, Avast has more than a decade of experience integrating with partner network systems to deliver successful white-labeled solutions to market. These partnerships are supported with 24/7 support and operations monitoring.

4.1 Avast Smart Life Platform

Avast Smart Life is a security platform that is deployed within homes, either as router firmware, a small hardware extension, or directly onto network gateways. The solution communicates with Avast's proprietary Cloud Intelligence Platform (CIP) to provide an asynchronous and always up-to--date layer of security for all connected devices in the home.

Avast's CIP works by uniquely identifying each connected device on a network, learning its normal behavior and comparing it with like devices around the world, and detecting anomalous behaviour. During an attack, the platform can quarantine the infected device and prevent the threat from expanding through the network.

Furthermore, customers also receive Avast's parental controls and digital family wellness product suite that allows them to:

- Impose digital controls to curb excessive screen-time and restrict inappropriate content
- Use Avast's AI-driven insights to teach children responsible digital habits
- Have peace of mind knowing loved ones are safe with Avast's locator service

To learn more about parental controls, also read the whitepaper of Juniper Research, "Safety in the Connected Family".

Avast Smart Life Platform, inclusive of the parental controls suite, is controlled by a single companion app. Using a simple interface, customers can rest assured their digital lives are protected by a brand trusted globally.

5. Conclusion

The growing IoT ecosystem provides an enormous opportunity for network operators, but conversely, opens the door for that ecosystem to be exploited.

Network providers are uniquely positioned to be an enabler of IoT security through strategic partnerships with security experts. By enabling cloud-based security solutions on network equipment such as routers and gateways, providers can offer secure networking for their customers.

They can capitalise on branded security services to develop a more trusting relationship with customers. This trust can be the tipping factor in reducing customer churn in competitive markets and providing a more robust portfolio of services to bolster ARPUs. Lastly, providers themselves can reap the cost benefits of a more secure and stable network.

To find out more about how network providers can take a central role in securing the IoT, visit
www.avast.com/IoT