

Inseego, Huawei and ZTE: A Side-By-Side Security and Performance Snapshot

Inseego “5G Born in the U.S.A.” Report Supplement

Introduction

When choosing 5G equipment and devices, the most important consideration for governments and enterprises are often security, performance, and cost. Huawei and ZTE, Communist Party of China-backed original equipment manufacturers (OEMs), have won over customers with their claims about performance and low cost, notwithstanding concerns about their security. But a closer look shows that U.S. products made by Inseego outperform these Chinese competitors, in addition to providing superior security features. Given these important advantages, the risk of compromised security and performance associated with Huawei and ZTE devices just isn't worth the “cost.”

Inseego stands apart from Huawei and ZTE for four key reasons:

- A superior security track record
- Trusted U.S.-based design and development processes
- Superior performance
- Strong ecosystem partnerships that place Inseego in a trusted and secure allied supply chain

This supplement brief to the “Inseego: 5G Born in The U.S.A.” white paper by Moor Insights & Strategy provides a comparison of Inseego with Huawei and ZTE in each area, delineating differences in the three companies’ design philosophies, technologies and performance.

Comparing track records

- Inseego follows a “no backdoors” policy, and has a history of market-leading innovation with secure devices that have long been trusted by U.S. government agencies and enterprise customers.
- Huawei has a history of IP theft and security incidents related to backdoors and malware going back nearly 20 years.
- ZTE has been accused of including unusual backdoors in some products and was caught selling equipment containing U.S. technology to Iran and North Korea, in violation of trade agreements.

A look at the headlines



Inseego's 5G MiFi® M1000 Mobile Hotspot Named Mobile Broadband Solution of the Year

PRESS RELEASE BusinessWire
© Nov. 19, 2019, 04:30 PM

Inseego Corp. (Nasdaq: INSG) today announced that its 5G MiFi M1000 mobile hotspot has been named Mobile Broadband Solution of the Year by Mobile Breakthrough, a leading independent market intelligence organization that recognizes the top companies, technologies and products in the global wireless and mobile market today.

This press release features multimedia. View the full release here:
<https://www.businesswire.com/news/home/20191119006051/en/>

"We're thrilled that our first-to-market 5G mobile broadband solution is receiving global recognition, not only from Mobile Breakthrough, but also from our global 5G customer base, which now includes service providers in nine countries, and many more in active trials," said Wendy Caceres, Inseego CMO.

Source: [BusinessWire](#), November 2019.¹



US finds Huawei has backdoor access to mobile networks globally, report says

The Chinese tech giant has reportedly had access to carrier equipment for over a decade.

Corinne Reichert Feb. 12, 2020 11:27 a.m. PT

Source: [CNet](#), February 2020.²



Top intelligence official says Chinese ZTE cellphones pose security risk to U.S.

President Trump wants to help the Chinese firm, but a top intel official told the Senate that ZTE cellphones may be used by the Chinese government to spy.

Source: [NBC News](#), May 2018.³

Although there have been both positive and negative press reports about Huawei and ZTE, these headlines make it clear that the track records of these companies are problematic at best when it comes to security and original innovations.

Quick searches related to Huawei, security and IP theft turn up article after article about incidents and issues going all the way back to 2003 when Cisco sued Huawei for patent infringement and copying proprietary Cisco software.⁴ Just last year, the U.S. Justice Department indicted Huawei⁵ for stealing technology from T-Mobile and violating U.S. sanctions against selling technology to Iran. Early this year, major news outlets reported that the U.S. government determined that Huawei can likely use backdoors in its network equipment, which are supposedly designed for law enforcement agencies, to secretly access sensitive information.⁶

Like Huawei, ZTE has been identified by U.S. intelligence agencies and regulators as a national security threat. In 2012, for instance, the company confirmed the existence of backdoors in some handsets. At the time, ZTE officials claimed the backdoors were flaws and issued a security patch. Security researchers, however, noted that the backdoors were “highly unusual” and appeared intentional because they were supporting software updates.⁷

Throughout its 24-year history, Inseego has built its reputation as a cellular industry pioneer, contributing dozens of innovations with each generation of cellular technology. In 2019, Inseego led the industry again with the world’s first commercial 5G mobile hotspot, earning the Mobile Breakthrough award for “Mobile Broadband Solution of the Year.”⁸

Unlike Huawei and ZTE, Inseego restricts remote access to its devices to legitimate, customer-authorized purposes such as providing security patches.

Design and development considerations

- Inseego designs and develops its products in the U.S. for best-in-class security, performance and reliability.
- Huawei must comply with requests from the Chinese Communist Party to protect national interests, and its development processes and products are replete with security vulnerabilities.

Detecting hidden backdoors in proprietary software is often difficult because sophisticated bad actors can conceal them well. That’s why trust among technology providers and their customers is critical. Although the leadership of both Huawei and ZTE claim to be independent actors, the Cyber Security Law of the People’s Republic of China states that all enterprises must help “maintain national security”⁹ and grants the government access to enterprise networks within China.¹⁰ Given state expectations and pressures, it’s difficult to accurately gauge all of the measures Huawei and ZTE have taken to make their equipment compliant with government edicts.

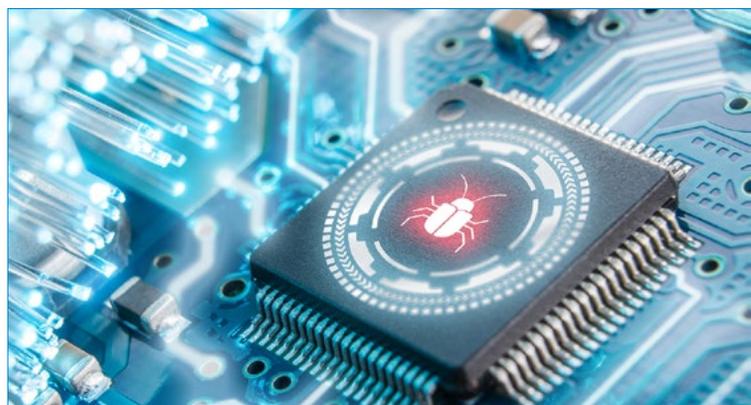
In addition to these “unknowns” there are many known risks associated with Huawei’s products which studies have found to be riddled with security issues. In scans of files and firmware of more than 558 Huawei products, the cybersecurity research firm Finite State found that 55 percent of Huawei devices had at least one backdoor and an average of 102 vulnerabilities associated with each firmware release. Researchers noted a reliance on outdated software libraries had led to insecure development practices.¹¹

Inseego answers only to our customers and shareholders, and we focus solely on meeting their expectations and needs. We prioritize their security and data privacy at every level, starting with the design and development of our products, which takes place entirely in the U.S.

Designing and delivering secure devices starts with employing the latest security protocols – along with a process to test and validate these protocols. Security protocol testing and validation are at the heart of Inseego’s product development process, including third-party penetration testing to identify and address vulnerabilities.

Inseego also follows industry best practices based on the intended use for each device combined with a design philosophy that integrates a high level of security throughout our technology stack, from silicon to software. For example, a mobile gateway may include a firewall, VPN client, strong encryption and port filtering. We often go beyond standard features and capabilities and add complementary layers of security that enterprises can use to gain visibility into device use and the overall network.

For consumers, Inseego provides guest networks with better password management, improved network separation, content filtering and the latest wireless encryption protocols to ensure the highest levels of privacy.



Backdoors at a glance

Backdoors in software can refer to both legitimate and illicit access points for accessing systems and their data. Legitimate backdoors may be used for administrative purposes or law enforcement access, but any type of backdoor, whether known or not, increases software vulnerabilities.

Inseego is trusted by:
U.S. Department of Defense, U.S. Department of Justice, U.S. Intelligence Community, federal, state, and local governments, first responders, educational institutions, financial institutions, large enterprises, and leading mobile network operators

For enterprises, Inseego helps safeguard corporate resources and intellectual property through its extensive virtual private network (VPN) appliance testing, its encryption of software updates and backup/restore functions, and its port and MAC filtering capabilities. We ensure maximum network uptime through cybersecurity offerings such as threat detection and mitigation, malware detection, content filtering, and controls.

Inseego provides service providers with remote management and frequent software and firmware updates to deliver a dependable and secure subscriber experience.

Our security story begins at the core of each device, which embeds features designed to protect and provide peace of mind, such as:

- Secure boot
- Admin security
- Configuration backup and restore
- Advanced firewall
- VPN client
- Strong encryption
- Port filtering
- Wi-Fi privacy separation
- Secure DNS
- Cross-Site Request Forgery Mechanisms (CSRF)

We take extensive measures to harden security with stringent third-party penetration testing to validate the resiliency of the code and ensure that no vulnerabilities exist.

Inseego goes beyond these core features and offers additional layers of security to provide visibility into device use and the network as a whole, including:

- Intrusion protection
- Threat detection and mitigation
- Policy enforcement
- Content filtering and management
- Network health assessment
- Network vulnerability management
- Real-time fleet-level alerts

Inseego's superior performance

A side-by-side performance comparison

- In benchmark tests by two telecom services providers, Inseego devices dramatically outperformed their ZTE and Huawei counterparts.
- Inseego devices have also been proven to deliver 2 Gbps download speeds with Verizon, which is well beyond what the Chinese vendors have been able to demonstrate.

In a comparison of an Inseego 5G MiFi® M1100 mobile hotspot and Huawei 5G CPE Pro device, a European telecom provider found that the MiFi device outperformed the Huawei device — often dramatically — in the majority of scenarios.



Telecom provider 1 benchmark test results

Location 1 (indoor)

Inseego MiFi M1100		Huawei CPE device	
Download speed (DL)	Upload speed (UL)	Download speed (DL)	Upload speed (UL)
629 Mbps	48 Mbps	291 Mbps	18 Mbps
677 Mbps	44 Mbps	307 Mbps	28 Mbps
808 Mbps	47 Mbps	321 Mbps	32 Mbps

Location 2 (indoor)

Inseego MiFi M1100		Huawei CPE device	
Download speed (DL)	Upload speed (UL)	Download speed (DL)	Upload speed (UL)
1.04 Gbps	50 Mbps	226 Mbps	73 Mbps
925 Mbps	85 Mbps	218 Mbps	75 Mbps
847 Mbps	83 Mbps	232 Mbps	79 Mbps

Location 3 (indoor)

Inseego MiFi M1100		Huawei CPE device	
Download speed (DL)	Upload speed (UL)	Download speed (DL)	Upload speed (UL)
1.12 Gbps	83 Mbps	686 Mbps	82 Mbps
1.06 Gbps	87 Mbps	752 Mbps	82 Mbps
1.04 Gbps	85 Mbps	754 Mbps	73 Mbps

Technical details

RAN	Ericsson
Bandwidth	100 MHz
LTE Bands	1,3,7, 20
Anchor band	3
MIMO layers	4X4
Modulation	256QAM
5G NR	N78

Telecom provider 2 benchmark test results

In a comparison of an Inseego MiFi M1100 mobile hotspot versus a ZTE Axon 10 Pro as a hotspot, a different European telecom provider found that the MiFi device outperformed the Axon 10 Pro device in the majority of scenarios.

Indoor results

Inseego MiFi M1100		ZTE Axon 10 Pro	
Download speed (DL)	Upload speed (UL)	Download speed (DL)	Upload speed (UL)
782 Mbps	37 Mbps	467 Mbps	44 Mbps
632 Mbps	43 Mbps	286 Mbps	29 Mbps
596 Mbps	39 Mbps	490 Mbps	38 Mbps

Technical details	
RAN	ZTE
Bandwidth	80 MHz
LTE Bands	1,3,7
Anchor band	3
MIMO layers	4X4
Modulation	256QAM
5G NR	N78

Outdoors results

Inseego MiFi M1100		ZTE Axon 10 Pro	
Download speed (DL)	Upload speed (UL)	Download speed (DL)	Upload speed (UL)
1.07 Gbps	42 Mbps	778 Mbps	41 Mbps
1.06 Gbps	41 Mbps	819 Mbps	44 Mbps
1.06 Gbps	42 Mbps	742 Mbps	45 Mbps

Strong ecosystem partnerships

It's important to consider the quality and integrity of every product component and manufacturing process. Huawei and ZTE rely on their own components for the products they build themselves, in-house, which provides less visibility into these aspects of their design and production. In contrast, Inseego has partnered with trusted leaders to provide best-in-breed technology and components. We work side-by-side with leading global mobile network operators and companies like Qualcomm (for 5G chipsets), Ericsson, Nokia and others to design, build, test and deploy our secure, high-performance products.

Conclusion: Trust Inseego for security and performance

Inseego is proud to have earned the trust of our government, consumer and business customers. As we work internally and with our partners to advance 5G capabilities, security remains a top priority. Moving forward, given all that will be at stake on 5G networks, Inseego is continually adding the latest, most advanced measures to identify and mitigate security risks in every layer of our products. With superior performance, a history of U.S.-based innovation, strong and trusted partners, and the industry's most advanced security features, Inseego is clearly the preferred choice for 5G devices and solutions.

Sources

¹"Inseego's 5G MiFi M1000 Mobile Hotspot Named Mobile Broadband Solution of the Year," BusinessWire, November 2019.

²"US finds Huawei has backdoor access to mobile networks globally, report says," CNet, February 2020.

³"Top intelligence official says Chinese ZTE cellphones pose security risk to U.S.," NBC News, May 2018.

⁴"[Huawei controversies timeline](#)," Computerworld, September 2019.

⁵"US indicts Huawei for stealing T-Mobile robot arm, selling US tech to Iran," arsTechnica, January 2019.

⁶"US finds Huawei has backdoor access to mobile networks globally, report says."

⁷"[ZTE confirms security hole in U.S. phone](#)," Reuters, May 2012.

⁸"Inseego's 5G MiFi M1000 Mobile Hotspot Named Mobile Broadband Solution of the Year."

⁹"[We can't tell if Chinese firms work for the party](#)," Foreign Policy, February 2019.

¹⁰"[What are the new China Cybersecurity Law provisions? And how CISOs should respond](#)," CSO, March 2019.

¹¹"[Huawei products riddled with backdoors, zero days and critical vulnerabilities](#)," SC Magazine, June 2019.