dish wireless

DISH lays the foundation for 5G network security.

White Paper – April 8, 2021

This white paper describes the security posture and customer benefits of DISH 5G — the nation's first, cloud-native, 5G Open Radio Access Network.

Table of Contents

Executive Summary

As DISH builds the nation's first, cloud-native, 5G Open Radio Access Network (O-RAN), this white paper discusses how the company is prioritizing network, system and end-user security from the outset of network deployment.

In today's software-driven world, secure connectivity is essential, enabling businesses to increase productivity, transform the way they operate and generate a higher return on investment. 5G connectivity unlocks a new level of innovation, supporting new business models and delivering innovative services and products.

There are always challenges with the deployment of any new technology. The cloud-native environment allows for dynamic orchestration and optimization of workloads in both private and public clouds. Secure mobile connectivity is essential for an increasingly diverse and distributed workforce.

DISH has been engaging with customers that require a robust security solution. These customers are seeking greater control over their networks, data and tools that optimize resources supporting their businesses.

Traditional wireless networks are challenged to adequately meet customers' future security requirements and expectations. This is because traditional wireless networks are built upon vertically integrated proprietary systems, which are based on closed-network security models.

To meet customers' needs, DISH needed to design and build an alternative, next-generation network and systems architecture that offers state-of-the-art technology and security.

As a result, DISH developed DISH 5G — a cloud-native solution that integrates network security from the foundation up. To support DISH 5G, the company has selected next-generation strategic partners that provide innovative and best-in-class security solutions, giving much of the control back to the customer. With these key strategic partners, DISH 5G offers customers unprecedented visibility, APIs, tools and security capabilities to complement their existing security model.

A key tenet of the DISH 5G security framework is a zero-trust model. Components of the company's 5G security design include real-time threat identification and correlation, 5G network slice-based security support with a software chain of trust and end-user controllability. These components improve DISH 5G's threat detectability and the capability to automatically serve, act and adapt.

This white paper describes how DISH 5G's network security is more controllable, agile and scalable than traditional networks, and how the company's strategic security partners contribute to the security model of DISH's cloud-native, 5G O-RAN.

The DISH Competitive Advantage

The timing of the deployment of DISH 5G puts the company at an advantage, providing it with the opportunity to build a state-of-the-art, cloud-native network without the burden of traditional 2G, 3G and 4G systems. The technology DISH has chosen to deploy integrates a new level of threat correlation, 5G network slice security, end-user visibility and customer control from day one, with a zero-trust posture.

DISH evaluated whether to deploy a modern, cloud-native, open 5G network or a traditional, monolithic network, considering the possible security ramifications of each approach. Traditional networks are commingled with vertically integrated environments that create end-to-end security challenges and software supply chain security risks. The global nature of software development and the obscurity of the supply chain can allow malicious code to be inserted during the software development process. This can enable the deployment of compromised code within a vertically integrated network, into which a traditional service provider has no visibility throughout the supply chain. Therefore, DISH chose to pursue a modern, cloud-native 5G network.

DISH consulted with customers and numerous security companies to begin architecting a 5G network that is more secure than traditional networks. As a result, DISH 5G was born, addressing the need for a new security model and taking advantage of the industry shift toward a disaggregated, cloud-native architecture with security built into each layer of the network.

Management and transparency through all aspects of the supply chain are critical to understanding the security posture and reducing the attack surface. While it's fairly straightforward to manage and monitor the supply chain for physical assets, software is more challenging. As part of a zero-trust security posture, transparency and monitoring of the end-to-end software supply chain are mandatory to reduce security risks and vulnerabilities.

While traditional networks may critique DISH 5G's open network security, an open environment allows for security hardening through independent software audits, code validation, community testing and adaptation.

With traditional networks, every client traverses the same network, inherently increasing the threat exposure and attack surface.

By contrast, DISH 5G is using today's cloud-native technology, coupled with sophisticated, embedded chipset security and open interfaces, to enable the adoption of a "best of breed" approach. This approach leverages a software supply chain of trust and a CI/CD process for software development, testing and deployment. DISH 5G allows components to be switched out, upgraded and specialized for specific use cases to satisfy customers.

DISH is working closely with strategic partners that share its vision of a highly secure, open, cloud-native, intelligent, containerized and interoperable 5G network.

Containerization and virtualization provide the ability to dynamically react at the speed of the software, allowing for near-instantaneous identification, response, isolation, redirection and quarantine management models. Real-time response rates are of utmost importance for security, customer control and flexible consumption. Moreover, virtualization technologies, including micro-services, containerization and network slicing, provide enhanced security and isolation at every layer of the 5G network.

As DISH deploys the nation's first, cloud-native, 5G O-RAN, it supports customer-defined network slices, slice-encrypted connections, containerized security, UPP to protect against DDoS and botnet attacks, improved end-user security control and policy management.

The Zero-Trust Model

Security is foundational and must be considered at the beginning of any network deployment, from a hardware-based root of trust up through each software layer in the network. Networks are only as strong as their weakest link; therefore, security solutions need to continually adapt to the threat environment, which is constantly evolving and becoming more sophisticated.

DISH 5G adopted a "secure by design" strategy based on a zero-trust model. This model incorporates certification and key management with advanced, multi-factor client authentication, allowing DISH 5G to integrate best practices into its products while embracing security design principles. With this construct in place, DISH 5G is able to rapidly respond to the ever-changing security needs of network customers.

DISH 5G drives to continuously iterate, modify and enhance the network at the speed of its customers and the velocity of the attack area.

As part of the zero-trust model, DISH 5G is taking the "never trust, always verify" approach. Zero-trust provides threat prevention and more control for both DISH 5G's internal operations and the customers on its network.

Customer Empowerment Through Network Slicing and Service Orchestration

DISH 5G offers innovative ways to empower customers on the network. Using the most advanced security solutions, DISH 5G is free from the limitations of traditional technology and gives customers more control with access to on-demand secure network slices, encrypted connections and secure, immersive experiences. A key enabler of this level of control is support for 5G secure slicing, providing customers with their own private 5G network.

5G network slicing in a cloud-native, O-RAN environment enables virtualized, logical networks to be interleaved on top of a common physical infrastructure, essentially functioning as a next-generation VPN. Each network slice is provisioned logically as a separate end-to-end network, tailored to meet the unique requirements and SLAs for customers' applications. This network slicing leverages software-defined networking and the virtualization of 5G core network functions.

In addition to 5G network slicing, service orchestration delivers customized, end-to-end services. Through the orchestration process, DISH 5G defines the customized configurations for customers' unique applications. Here, wide-ranging security capabilities will be added to ensure customers' data — both in motion and at rest — is safe and secure.

Finally, rules, workflows and various physical components lie underneath the orchestration canvas before getting coupled together to form customer-specific network slices.

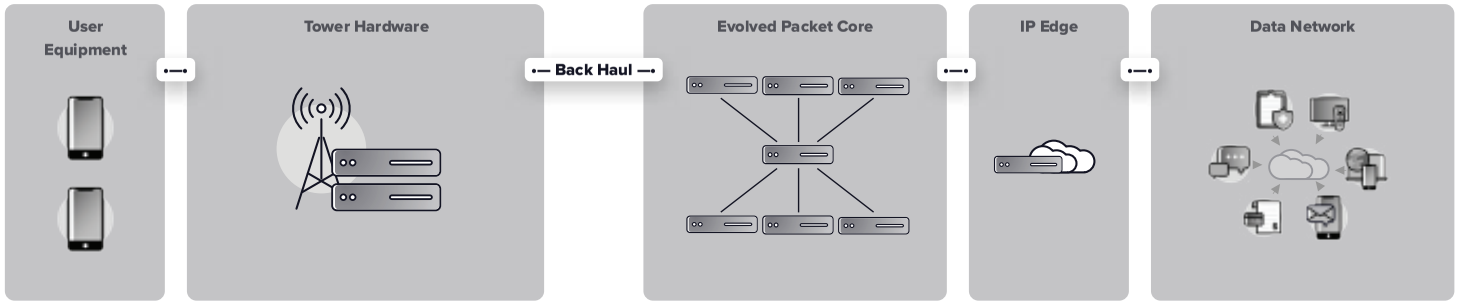
Figure 1 on the following page illustrates DISH 5G's secure, state-of-the-art architecture and how it's better equipped to meet customer requirements and demands than traditional networks.

Figure 1

Retrofitted 5G

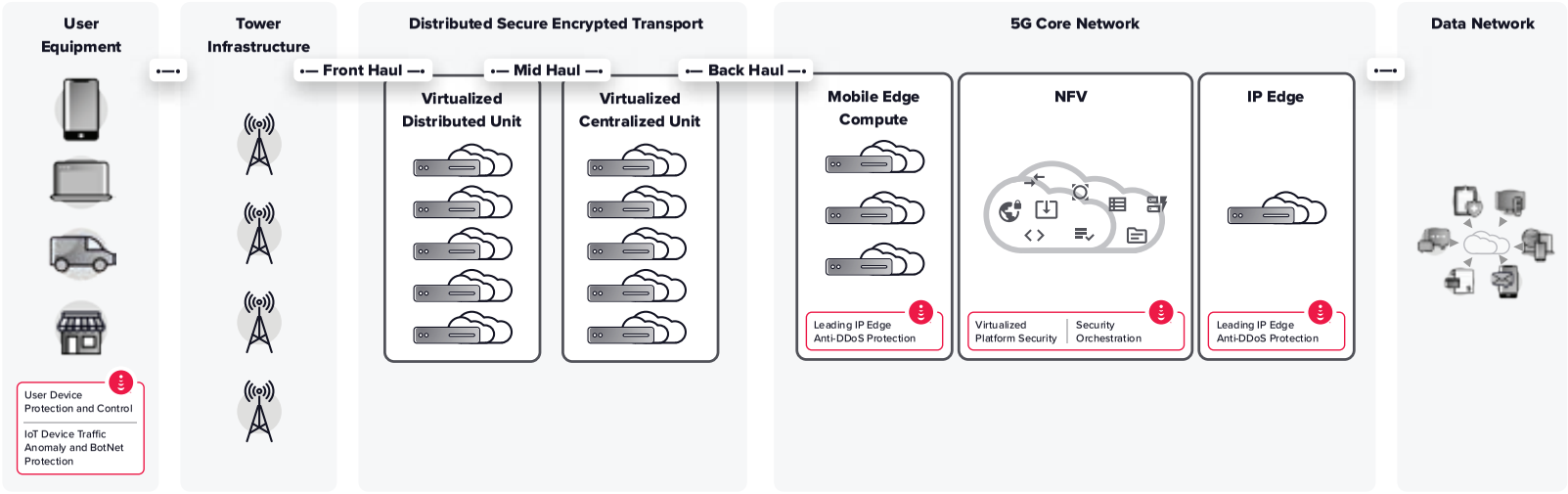
Based on Legacy Networks

- No Virtualization
- Basic Security Until Traffic Reaches IP Edge
- Lack of Secure Edge Compute
- Traffic Commingled
- Lack of Security Control for the Customer
- Not Enterprise-Ready



dish 5G

- High Virtualization
- Security Applied at Every Stage
- Secure Edge Compute
- Network Is Isolated Via Slicing
- Security Control Empowering the Customer
- Enterprise-Class Service
- Software-Defined and Software-Driven



The Challenges for Traditional Networks

Upgrading to 5G from existing 2G, 3G and 4G networks will not deliver the advantages offered by DISH 5G. The inherent limitations of 2G, 3G and 4G, over a diverse geographic landscape, become the burden of a traditional service provider.

Some of the challenges of retrofitting 5G over traditional networks include inadequate security protections, inflexible infrastructure and lack of customer control.

Traditional, one-size-fits-all networks cannot compare to the reliability, latency and flexibility of DISH 5G.

The DISH 5G Advantage

The new capabilities offered by DISH 5G give customers never-before-seen data protection, security and network reliability. New business models demand networks that adapt with the speed and needs of the customer. DISH 5G moves the processing of data out of the traditional data center to the edge of the network, delivering ultra-low latency required by new applications. The advantages of DISH 5G are clear: secure edge computing, hardware and chip-based security, unprecedented customer control and a first-of-its-kind, enterprise-grade wireless infrastructure.

DISH 5G's architecture provides end-to-end security, advanced threat visibility and secure function isolation. It is also elastic, providing bandwidth that dynamically adjusts both temporally and spatially as customers' needs change.

Through automation and orchestration, DISH 5G provides the highest level of security at the speed of system workloads, and the network allows for confidential computing at the edge. Customers have full security control from the outset, including flexible UPP, policy management and control with system-enabled self-healing, made possible by AI and ML tools.

DISH 5G supports customers that require control over selected components of the RAN and core network functions.

DISH 5G is also adopting measurable, state-of-the-art security standards beyond those currently found in the industry to provide a higher level of security for its customers.

Figure 2 on the following page shows how DISH 5G uses network slicing to offer end-to-end network services, delivering applications customized to the end-user. New verticals requiring massive connectivity, immersive experiences like VR/AR, machine-to-machine automation and more are made possible with DISH 5G, enabling higher performance, improved predictability, lower cost and greater control over the customer experience.

Figure 2

DISH 5G Network Slicing

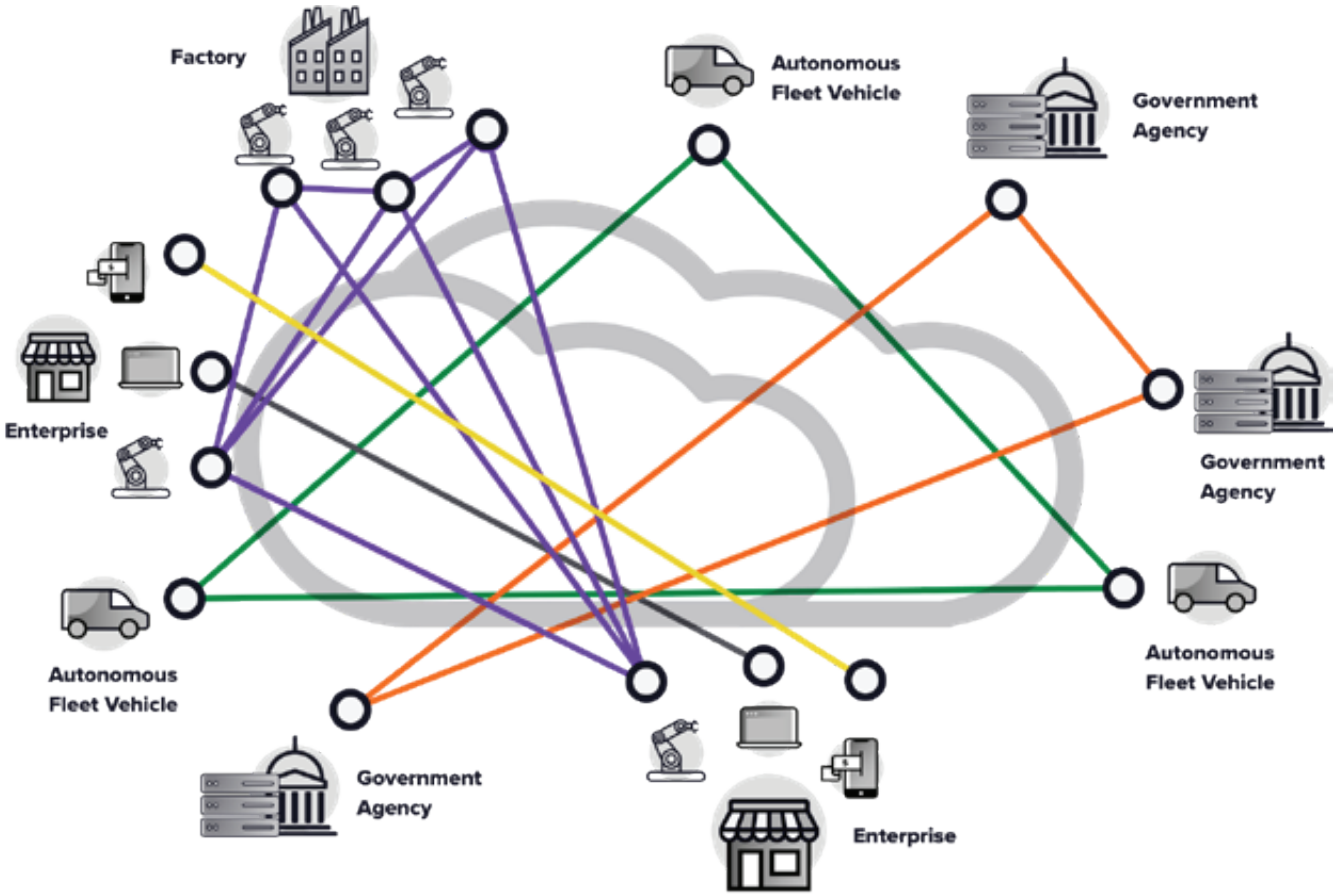
With fully virtualized network slicing, DISH offers end-to-end network services customized to the specific requirements of each client.

Retrofitted 5G, Based on Traditional Networks

Retrofitted legacy networks lack the flexibility to slice end-to-end, fully virtual network segments.

Greenfield 5G allows for cloud-native, fully virtualized networks, capable of dynamically supporting a multitude of applications and device types.

Retrofitted 5G simply cannot compete.



Foundational Security Strategy

To support DISH 5G, the company has partnered with an initial set of leading industry vendors to provide the highest level of security for its network and customers. The services provided by this set of foundational security partners include the following:

Firewall, Cloud and Container Security

DISH 5G utilizes 5G-native, next-generation containerized firewalls. These firewalls include real-time threat correlation, 5G slice security and dynamic security enforcement. They integrate a high degree of automation to manage security efficiently, and focus on controllable, scalable, “as-a-service” offerings.

With these services in place, DISH 5G is able to observe and control security across all network layers and locations, including the full stack of the containers and infrastructure, providing comprehensive protection. To manage vulnerabilities, ensure compliance and protect containers at runtime, DISH 5G leverages cloud workload protection capabilities, such as the Prisma Cloud Compute Edition.

DISH has chosen Palo Alto Networks, a cybersecurity leader, to deliver firewall innovation and enable the secure digital transformation of DISH 5G.

DDoS/UPP and Security as a Service

DISH 5G is leveraging tools that provide end-to-end UPP from cybersecurity threats for customers. These tools protect DISH 5G and off-network activities against all types of cyberattacks, such as malware, viruses, ransomware and phishing attacks. The solution allows customers to easily manage their cybersecurity policy and settings, creating a unified experience on all their devices. DISH 5G also provides customers with end-to-end user UPP from the device to the network and back. UPP ensures protection against even the most sophisticated, emerging DDoS and botnet attacks for both customer devices and the network.

DISH has partnered with Allot, a key provider of innovative network intelligence and security solutions, to support DISH 5G in this critical area.

Integration and Orchestration

While traditional networks are segmented into commingled environments with a shared fate, DISH 5G leverages secure, dedicated network slicing to enable a zero-trust security posture.

DISH has partnered with Nokia to help provide DISH 5G with end-to-end security and orchestration, from the physical hardware level to each application. Nokia is a leading technology and services company, supporting mobile networks, cloud platforms and other access technologies, and provides the tools and solutions needed to enable DISH 5G to manage security operations.

Conclusion

In an agile world, traditional wireless networks present significant roadblocks to meeting customers' future security requirements. A one-size-fits-all approach and a "trust me" model are things of the past. The changing business landscape demands new network technologies and security solutions that push computing to the edge of the network, provide support for new applications and offer end-users more control and visibility. These expectations are only being met by DISH 5G, as the network is not burdened by any traditional technologies, including 2G, 3G and 4G platforms.

DISH 5G secures its network for tomorrow's customers, providing intelligence and control beyond what is available today. DISH 5G customers are able to focus on their core business with assurance around security and privacy, while having the prerequisite visibility and network intelligence to rapidly respond to any threat.

DISH 5G customers are equipped to solve network and wireless challenges of the future. DISH 5G has surpassed the status quo by coupling powerful security solutions with unprecedented customer control.

In short, the benefits of DISH 5G are limitless, providing increased controls, 5G network slicing, unmatched threat visibility and more for network customers.

Acronyms

2G	2nd Generation
3G	3rd Generation
4G	4th Generation
5G	5th Generation
AI	Artificial Intelligence
API	Application Programming Interface
CI/CD	Continuous Integration/Continuous Delivery
DDoS	Distributed Denial of Service
IoT	Internet of Things
ML	Machine Learning
MVNO	Mobile Virtual Network Operator
NSA	Non-Standalone
O-RAN	Open Radio Access Network
RAN	Radio Access Network
SLA	Service Level Agreement
SMB	Small- and Medium-Sized Business
UPP	User Plane Protection
VPN	Virtual Private Network
VR/AR	Virtual Reality/Augmented Reality

About DISH

DISH Network Corporation is a connectivity company. Since 1980, it has served as a disruptive force, driving innovation and value on behalf of consumers. Through its subsidiaries, the company provides television entertainment and award-winning technology to millions of customers with its satellite DISH TV and streaming SLING TV services. In 2020, the company became a nationwide U.S. wireless carrier through the acquisition of Boost Mobile. DISH continues to innovate in wireless, building the nation's first, cloud-native, Open RAN-based 5G broadband network. DISH Network Corporation (NASDAQ: DISH) is a Fortune 250 company.