FORNETIX

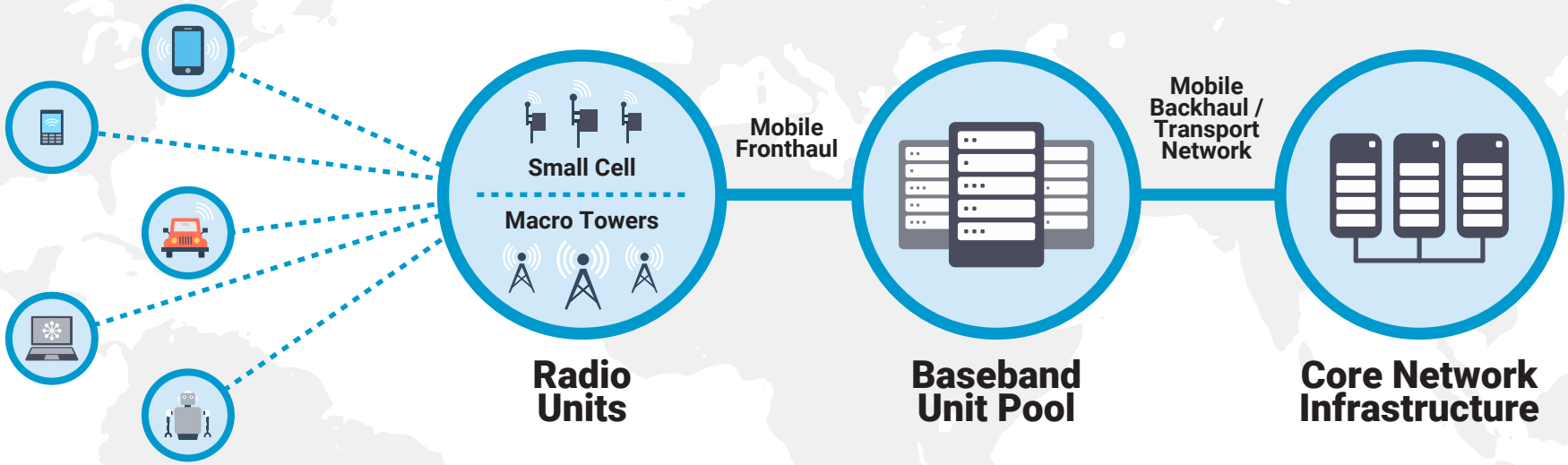
5G ARCHITECTURE

An Enterprise Data Security Risk?

Major Components
OF 5G ARCHITECTURE

SOURCE: Lewis, James. 2018. *"How Will 5G Shape Innovation and Security: A Primer." Center for Strategic & International Studies.*

User Equipment	Radio Access Network (RAN)	Core Network



Devices such as smart phones, computers, and Industrial Control Systems (ICS) generate data that is then transmitted to a base station, small cell, satellite, or Internet Exchange Points (IXP). Compromised devices may collect user data and impact local networks and systems, but are unlikely to impact the larger communications network.	RANs connect wireless or satellite subscriber devices to terrestrial telecommunication networks. Compromised systems may intercept or disrupt data flow and phone calls.	The core network is the backbone of the U.S. communications infrastructure that routes and transports data and connects the different parts of the access network. Compromised core devices may be used to disrupt data and services on a large scale, and impact customers who are interconnected by the access network.

Points of Vulnerability

1. SUPPLY CHAIN

» ISSUE

The 5G supply chain is susceptible to the malicious or inadvertent introduction of vulnerabilities such as malicious software and hardware, counterfeit components, poor designs, manufacturing processes, and maintenance procedures.

» IMPACT

5G hardware, software, and services provided by untrusted entities increase the risk of network asset compromise and affect data confidentiality, integrity, and availability. Even if a U.S. network is considered secure, data that travels overseas through untrusted telecommunication networks are potentially at greater risk of theft, manipulation, and detection.

Points of Vulnerability

2. DEPLOYMENT

» ISSUE

5G will utilize more information and communication technology components than previous generations of wireless networks, and municipalities, companies, and organizations may build their own local 5G networks, potentially increasing the attack surface for malicious actors.

» IMPACT

Despite security enhancements compared to previous generations of wireless network equipment and services, 5G networks will need to be properly configured and implemented for those enhancements to be effective. Improperly deployed, configured, or managed 5G equipment and networks may be vulnerable to disruption and manipulation.

Points of Vulnerability

3. NETWORK SECURITY

» **ISSUE**

5G builds upon previous generations of wireless networks and will initially be integrated with 4G LTE networks that contain some legacy vulnerabilities. Additionally, it is unknown what new vulnerabilities will be discovered on 5G networks.

» **IMPACT**

Some legacy vulnerabilities, whether accidental or maliciously inserted by untrusted suppliers, may affect 5G equipment and networks no matter how much additional security is built-in.

Points of Vulnerability

4. LOSS OF COMPETITION & CHOICE

» ISSUE

Despite the rise of standards to encourage interoperability, some companies build proprietary interfaces into their technologies, limiting equipment options.

» IMPACT

Customers who are locked into one technology or service provider may find themselves having to choose between continuing with an untrusted supplier or removing and replacing their existing equipment, which may be both expensive and time-consuming. Lack of interoperability may also make it difficult for trusted companies to compete, potentially limiting their ability to invest in R&D and eventually driving them out of the market.

Cybersecurity Risks With 5G

» 1. 5G Is a Software-Driven Network

- All cyber vulnerabilities in 5G are far-reaching and carry long-term ramifications.
- Standard IT risks are now applicable to the telecommunication infrastructure.

» 2. Network Security

- DSS involves sharing bandwidth between multiple streams of data, with each bandwidth slice having its own level of risk.
- Network slicing functions create more diverse communication paths that need to be secured.

» 3. Dramatic Bandwidth Expansion

- 5G bandwidth allows for greater amounts of information and types of information to be transported over networks.
- The capability of an enterprise's existing security solutions will be pushed well beyond its limits, rendering it inadequate.

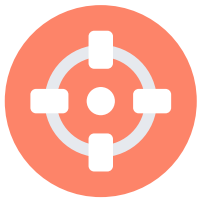
Cybersecurity Risks With 5G

» 4. OT/IoT-Based Cyber Threats

- With the flood of IoT devices comes new, yet undiscovered, backdoors for attackers to infiltrate business networks.
- If these systems are breached, they can become weapons in an attacker's hands that could inflict physical harm.

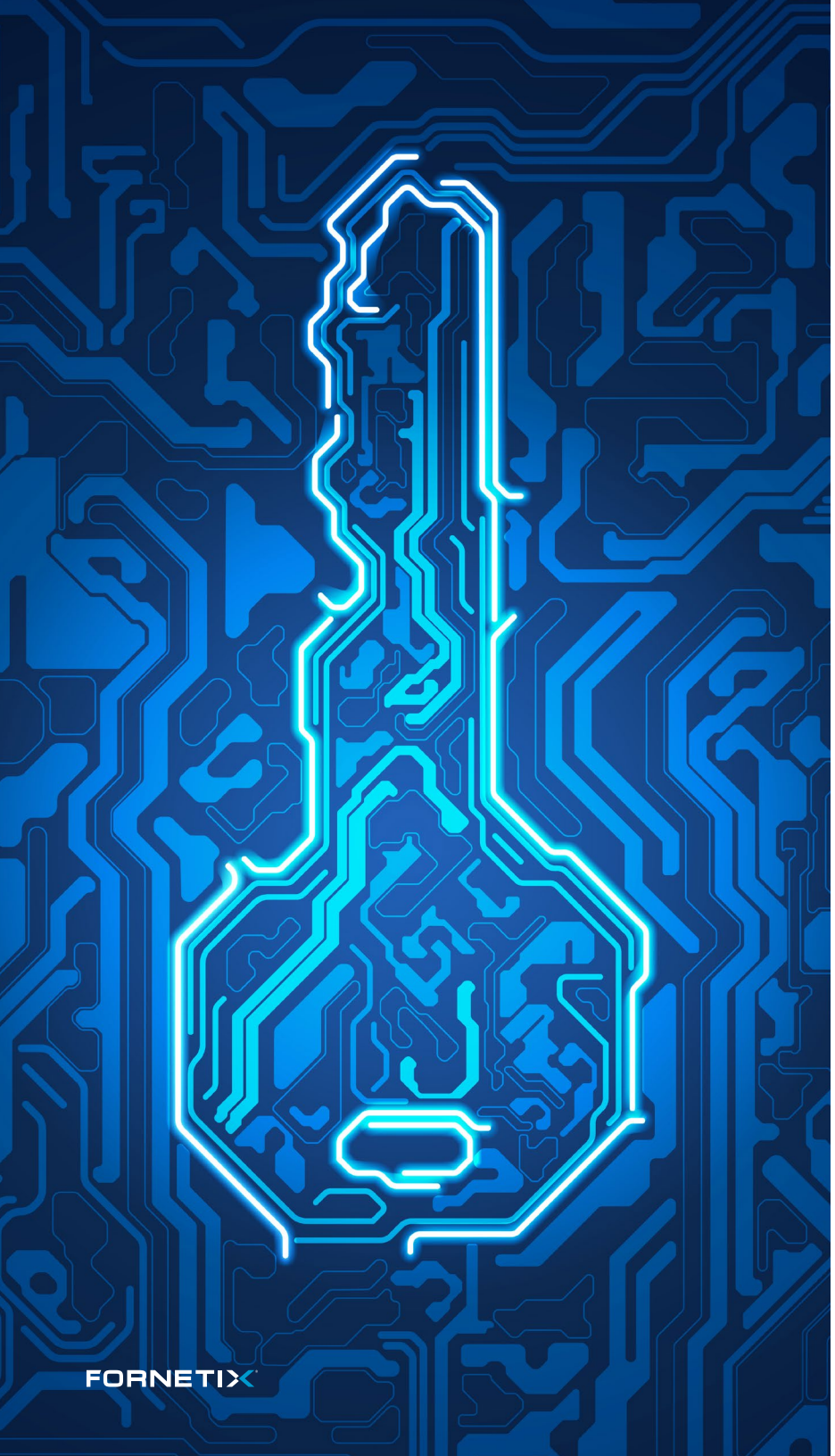
» 5. Distributed Routing

- Many factors play into routing 5G and where it's located in the network architecture.
- But in each scenario, there is the loss of benefits to having chokepoint control and inspection when enforcing security protocols.



» 6. Super Botnets

- As the internet expands into the tens of billions of devices, the scale and ferocity of these attacks are only bound to grow.



Mitigating the Risks

The speed and enormous volume of data 5G affords an enterprise to transfer is an exciting business opportunity, but with it comes great responsibility to ensure data remains safe.

Encryption is at the core of every security strategy and properly managing encryption keys plays a crucial role in mitigating the inherent risks associated with 5G.

VaultCore™ is a patented encryption key management solution with robust APIs that, when integrated with new or legacy systems, affords enterprises the ability to respond to the dynamic, service-centric 5G environment requirement of securing end-to-end communications.

With full automation of the encryption key lifecycle, centralized control of security, and simplified compliance policy enforcement across all devices, VaultCore safely delivers data across 5G to its endpoint protected and secure.

A Return on Your Security Investment

While VaultCore's positive value in the 5G network is the end-to-end secure communications on a mass scale, VaultCore's capability to integrate with existing products and services and communication infrastructures with zero network downtime directly supports cost savings. **Measuring the cost- effectiveness of VaultCore to justify spend is also a practice in calculating loss prevention.**

» COST BENEFITS

- Productivity and accuracy increased through automation
- Reduction in human error (responsible for 24% of breaches)
- A standardized process for disparate technologies
- Savings in preserving data security (average cost of a data breach in 2020 is $3.86 million)
- "Grow as you go," VaultCore is scalable to support over 100 million keys

IN CONCLUSION

5G Does Increase an Enterprise's Risk of Breach, But There Is a Cost-Effective and Simple Solution

We have a saying at Fornetix®, "if they can't get your encryption keys, they can't get your data." This holds true in almost every environment, whether your data is being stored, is in transit over a 5G network, in the cloud, or hybrid. Fornetix's commitment to industry standards, flexibility to address new technology risks, and interoperability advancements have allowed us to bring VaultCore, the most powerful encryption management solution, to virtually any device or technology.

From small businesses all the way to global enterprises with massive IoT infrastructure and an already heavy reliance on the new 5G network, there's a VaultCore deployment option that perfectly fits your unique needs to safeguard your data.

FORNETIX VAULTCORE

For more information, visit **www.fornetix.com**, call us at 844.549.6724, or email us at info@fornetix.com.