CYPHRE
a RigNet company

ENCRYPTION PROTECTS A TELECOM INDUSTRY IN TRANSFORMATION

As telecommunications service providers expand their service offerings to include everything from access to content, the cloud has become an increasingly strategic asset. With over-the-top players innovating at a rapid pace, many providers are transforming their networks deploying new virtualized technologies in their public and private data centers in order to lower costs and increase revenue.

With the breadth and depth of services offered to millions of service subscribers, the industry faces an almost boundless risk of cyberattacks that include endpoint vulnerabilities, insider threats that can wreak a spectrum of damage, credit card and identity theft to service interruption, forced internet outages, and much more.

Pervasive Vulnerabilities Persist at Many Levels

Cyber criminals use a variety of methods to take advantage of human beings, software, and hardware. The telecom sector is especially susceptible to Man-in-the-Middle attacks where hackers spoof wireless access points or insert a fake router in a network cabinet. Once in, cyber criminals have limitless access to the entire network, and likely beyond to other third parties. Even with existing security protocols, such as SSL or TLS, networks that have had their access compromised are just as vulnerable as unprotected networks.

Advanced Encryption Is Key to Preventing Massive Subscriber Data Theft

Proper diligence in tackling cyber security for telecom companies goes hand-in-hand with adopting a powerful, data-centric protection posture that provides the strongest defense against cyber threats.

Cyphre offers a full security solution that protects data in-transit, at-rest, and in-use. This uniquely powerful protection stretches across enterprise infrastructure, the Internet of Things, and private or hybrid clouds.

Our CyphreLink solution is particularly powerful for telecom service providers. As data is transferred over any network – fixed, wireless, cellular, and even satellite – CyphreLink provides the highest level of security for data in-transit by encapsulating it in an encrypted tunnel either point-to-point or in a mesh architecture.

Cypher's uniquely powerful solutions leverage hardware-based encryption that adds a crucial layer of protection not found with software-based encryption. By providing deeper and stronger data security than conventional methods, a service providers encryption keys and certificates are never exposed. Even if a hacker breaks into the network, the keys and certificates are protected and rendered unusable to the attacker.

Securing Heterogeneous Networks

Service providers are employing a mix of access and transport networks to move data from the Internet to the user equipment. While most of this network is considered secure and private, service providers have come to rely upon untrusted networks to extend coverage and capacity. These wireless (typically WiFi) networks are susceptible to MITM attacks. CyphreLink can be employed to establish a trust boundary between the service providers network and other authorized access points, limiting the damage that hacked WiFi access points can do to the network.

Non-compliance fees for GDPR are expected to be up to **€20 million Euro**

CYPHRE
a RigNet company

Securing the Internet of Things (IoT)

For telecommunications service providers, IoT represents a major revenue opportunity as the data must be aggregated at the edge of the network and moved securely to a final endpoint. Data originating from IoT devices will be communicated to microcellular or WiFi networks, and then backhauled through the core network over the provider's fiber or the public Internet. Each of these hops represents a very real threat to the data, the encryption keys protecting that data, as well as the certificates of the IoT devices themselves. CyphreLink secures the access and control mechanisms of these IoT devices end-to-end, giving service providers a significant differentiator when selling IoT data transport to enterprises and industrial customers.

Encryption Eases Compliance with GDPR

A major factor driving cybersecurity initiatives is the EU's General Data Protection Regulation (GDPR) to protect personally identifiable information (PII). The May 2018 deadline to be ready for this sweeping new regulatory mandate is fast approaching, and service providers and businesses are intensely focused on ensuring their ability to meet its requirements. With non-compliance fines expected to be up to €20 million Euro, the pressure is on telecommunications service providers to review, change and test new cybersecurity systems.

Preparing for GDPR requires understanding the cybersecurity risks and making wise investments in encrypted solutions. A no-nonsense approach includes encryption and key management from security experts like Cyphre, who understand exactly what organizations need to do to comply with GDPR requirements. Governance prescribed by GDPR makes it essential to associate cryptographic managed objects with encrypted information.

Cyphre's BlackTIE® Technology Is the Key

CyphreLink is powered by BlackTIE® Technology that extends unassailable protection for data, keys, and certificates from any end-point and across any access network. Hardware-based encryption technology leverages a specialized chipset with a dedicated security engine to offload cryptographic operations outside of host CPU and system memory - two of the most common entry points for cyber criminals. Key management controls offer total and exclusive control of the generation, exchange, storage, use, destruction, and replacement of encryption keys.

About Cyphre

Headquartered in Austin, Texas, Cyphre cloud encryption technology provides the highest level of security for cloud data. Period. Product offerings include Encrypted Cloud Storage and Enterprise Collaboration services, Secure IoT Integration and the Enterprise Cloud Encryption Gateway.

www.cyphre.com @getcyphre Cyphre /getcyphre