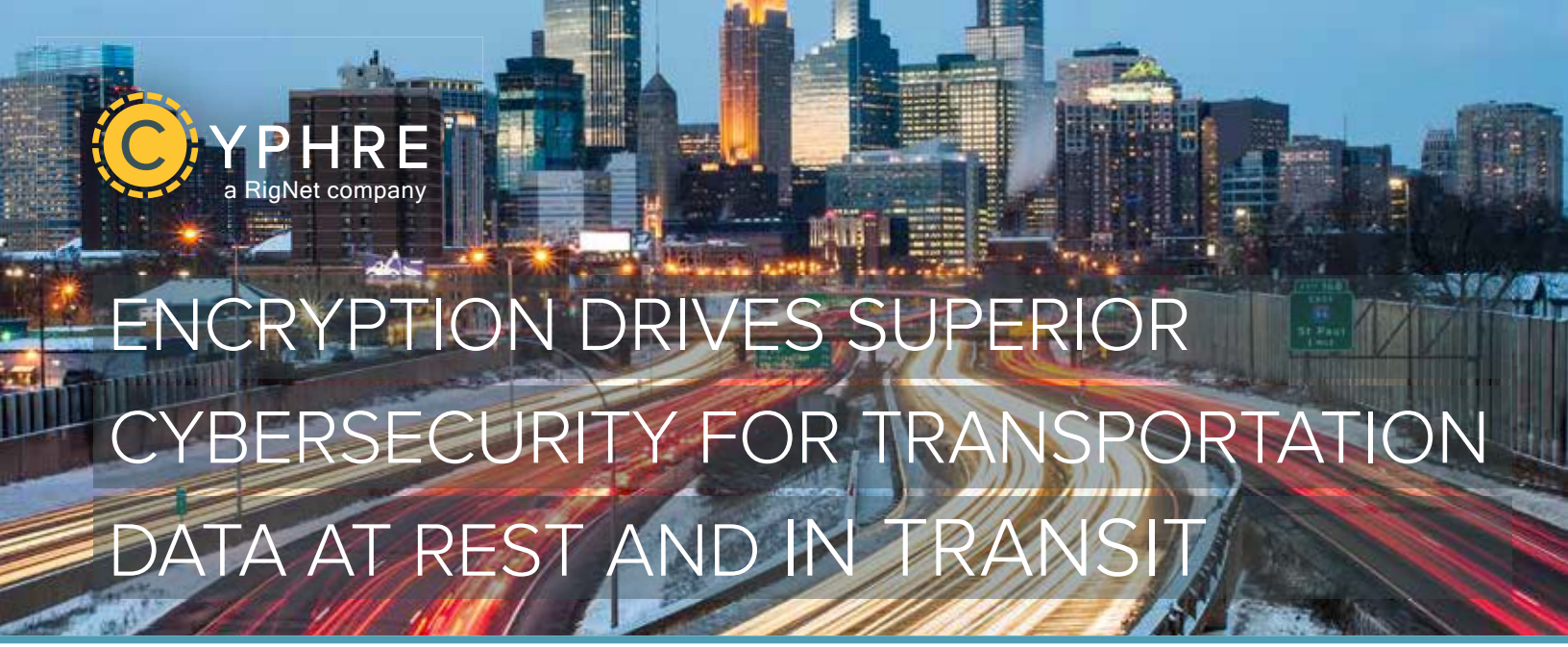


CYPHRE
a RigNet company

ENCRYPTION DRIVES SUPERIOR CYBERSECURITY FOR TRANSPORTATION DATA AT REST AND IN TRANSIT

Information is the Vehicle for Transportation Sector Success

The transportation industry is increasingly being targeted by hackers. Critical transportation infrastructure is coming under greater threat of catastrophic cyberattacks as cybercriminals target systems used to connect and control vehicles from trains to planes to trucks and autos. According to IBM, "Vulnerability flows from the growing reliance on cyber-based control, navigation, tracking, positioning and communications systems, as well as the ease with which malicious actors can exploit cyber systems serving transportation." Techniques employed by hackers—and the trouble they can cause—are evolving along with advancing transportation information technology.

Chinese firm Tencent recently bypassed a Tesla security mechanism implemented after a hack that occurred in 2016. These white hat hackers were able to remotely open the doors and trunk lids on Tesla vehicles, apply the brakes and flash the headlights. Firmware Over-The-Air patches have been applied to the Tesla motors to fix the vulnerability, but industry experts have pointed out that "the wider adoption of Connected and Autonomous Vehicles is likely to see cyber criminals finding increasingly more innovative ways to attack and exploit the technology and the data, from stealing vehicles remotely to stealing vast amounts of data and more sinister incidents."

Cars today have up to **100 Electronic Control Units (ECUs) and more than 100 million lines of code** — a massive attack surface.

Transportation systems manage large volumes of data, much of which can be valuable to cyber crooks. In fact, transportation now sits alongside healthcare, manufacturing, financial services and government as a high-value target. Today, a spectrum of cyber threats must be added to the many traditional risks facing critical transportation infrastructure (natural disasters, accidents, and so forth). Stolen data that could be used in terrorist attacks is a major concern for industry experts. Cyber terrorist attacks that disrupt transportation systems, damage infrastructure, or cause civilian injuries have terrible long-term sociological and economic consequences.

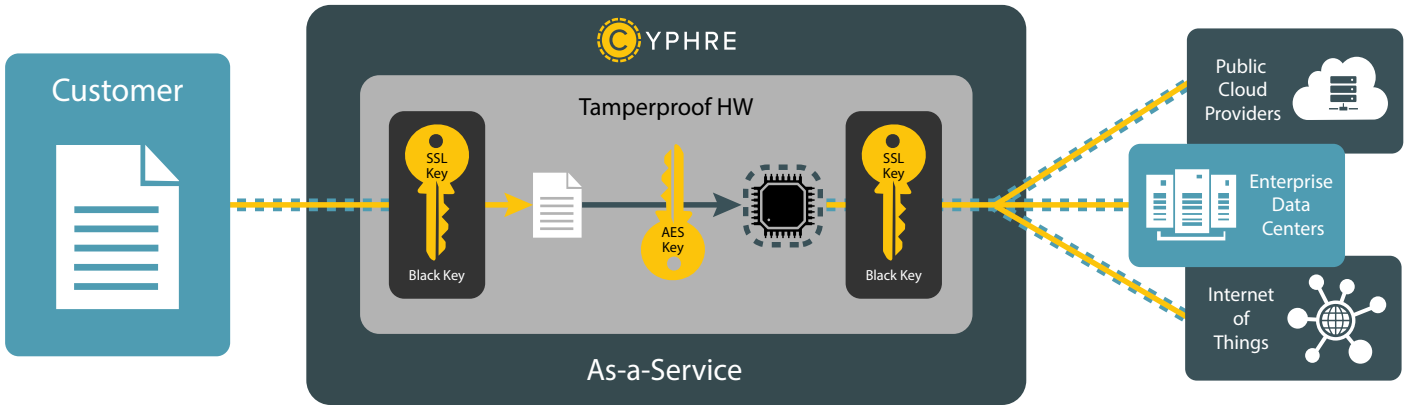
It is a fact of life that our complex, mission-critical transportation infrastructure is vulnerable to cyberattack by hostile global parties seeking to disrupt operations or steal information. Modern vehicles are filled with computers that have been proven to be hackable. Extrapolating this vulnerability to the coming widespread deployment of autonomous vehicles shines a spotlight on the real and growing concerns that must be addressed.

Delivering on the Commitment to Defuse Cyberattacks

Fortunately, proper application of robust encryption technology across the entire IT infrastructure can fully secure transportation information, both behind firewalls and during transfer over private intranets or the public Internet.

Whether at rest or in motion, data is best protected by encryption. Encryption provides the highest level of security, but the way encryption is achieved matters vitally. When single encryption software keys are memory resident in plaintext format on a host server, they are vulnerable to attack and data can be stolen. This presents a well-known vulnerability and major opportunity for hackers to exploit.

CYPHRE
a RigNet company



Cyphre's BlackTIE® technology augments vulnerable single encryption keys with hardware-encrypted Black Keys to nullify breaches, hacks, and other cybersecurity threats. Chip-resident Black Keys are completely isolated from hacker exposure. BlackTIE® assigns one key per file rather than one key for many files, establishing maximum protection for encrypted data at rest, limiting the 'blast radius' of any breach, and protecting traffic as it leaves the network. With authentication taking place on the hardware, no software installation is required on the host server. By offloading encryption activities from the host system Cyphre hardware increases encryption performance.

BlackTIE® also protects traffic as it leaves the network. Cyphre's automatic protection of information in transit requires no proactive action by the teams moving the data. This establishes a "zero knowledge" stance for employees, eliminating them as a possible point of exposure. Network administrators can easily monitor and control all file sharing activities within an organization, as well as integration with LDAP authentication systems.

Hardware-driven encryption from Cyphre protects enterprise data even if hackers break into the server, thus neutralizing a common breach technique that targets software-only security. Cyphre's crypto-hardware-based keys provide virtually unbreachable protection against common attacks such as cold boot attacks, malicious code, brute force attacks, and more.

In short, Cyphre's BlackTIE® encryption technology secures data in transit and at rest with a uniquely powerful encryption service solution that is invisible to end users, highly scalable, device-resident, and cost effective for medium and large scale environments.

About Cyphre

Cyphre, a RigNet company (NASDAQ:RNET), is a cybersecurity company deploying disruptive data protection innovations by enhancing industry standard encryption protocols with our patent pending BlackTIE® technology.

www.cyphre.com @getcyphre Cyphre /getcyphre