Cyphre
a RigNet company

Cyphre BTX

Security without Compromise

The Need for Fast, Secure Networks

The adoption of cloud computing, digital transformation, and analytics into enterprise networks has enabled companies to gain the intelligence needed to improve decision-making and the performance of their core assets and systems. These new technologies are impacting critical infrastructure industries, including energy, healthcare, finance, manufacturing, and the government sectors, where the number of connected devices has soared into the billions.

At the same time, cybersecurity breaches continue to increase by attacking the many vulnerabilities in traditional security solutions that expose unencrypted data in system memory, the CPU, network and storage. There is an urgent need for secure communications that can be trusted to withstand persistent, sophisticated, and costly cyber threats without compromising performance or the flexibility of the ever-changing network landscape.

Protecting Networks and Legacy Systems

The vast majority of enterprise networks are more than ten years old. These legacy networks are built on infrastructure that can be costly to upgrade and patch, making them vulnerable to side channel, memory, man-in-the middle (MITM), and an ever-growing number of increasingly sophisticated attacks.

While organizations segment their networks and depend on encrypted virtual private networks (VPNs), such as IPsec and TLS, highly sensitive information and credentials are often communicated in plaintext or stored insecurely. VPNs are only as secure as the devices and methods used to encrypt and decrypt the network traffic. Malicious actors often target system vulnerabilities that allow them to:

- Steal private encryption keys that are broadcast in plaintext
- Decrypt VPN tunnels
- Impersonate devices with stolen credentials
- Compromise data, availability and plant safety

Application Performance

A large enterprise may be running hundreds of applications across its enterprise WAN and production networks. Optimizing application performance while protecting information privacy and confidentiality is difficult due to:

- Chatty application protocols over high-latency networks
- High IP VPN overhead over low-bandwidth links
- Slow firewall performance due to CPU demands for encryption
- Slow encryption key generation for high-frequency transactions

VPNs, even with next generation optimization technologies like SD-WAN, can be difficult to manage and are prone to performance challenges. Networks with high-performance needs or limited bandwidth, such as IoT, VSAT, financial trading, and mobile networks cannot support the performance impacts of chatty protocols like IPsec.

Complex Integrations

As the network expands to support cloud, edge and collaboration applications, implementing more security controls frequently comes with integration and compatibility concerns, such as:

- Complex configuration and tuning of IPsec and GRE tunnels
- Application layer protocols that are impacted by IPsec and GRE
- Changes to end user behavior required by software-based VPNs
- Adhering to security and compliance policies

Cyphre BTX Security Appliance

Cyphre's BTX delivers a patented and FIPS 140-2 validated hardware-based platform for protecting data and ensuring secure communications that is easy to implement – delivering the security without compromise that your enterprise demands.

How does Cyphre BTX work?

Cyphre BTX is a hardware-based network encryption solution for site-to-site communications that is delivered as an appliance. Deployed at each site, BTX appliances leverage Cyphre's patented BlackTIE® security engine that offloads encryption operations to hardware in a way that protects plaintext encryption keys from ever being exposed in the CPU or system memory.

The BTX is a turnkey solution comprised of:

- CyphreLink BTX Security Appliances available in multiple form factors for data center or edge deployment
- Cyphre BlackTIE Technology, hardware-based Security Engine that is integrated with the BTX appliance
- CyphreLink Application secure site-to-site encryption solution that leverages BlackTIE.

Cyphre BTX Benefits

Security

- Never exposes private keys and encryption keys to the CPU or memory
- Resistance to side-channel, cache memory and MITM attacks
- Avoids using insecure, software-based random number generation
- Encryption keys are generated with a SEED value from the security engine's hardware-based true random number generator

Performance

- Better application performance over high latency, low bandwidth links
- Reduction of typical IP VPN packet overhead by more than 50%
- High-performance encryption and decryption
- Offload of crypto operations to hardware to reduce CPU load for encryption and decryption

Ease of Use

- Simplification of integration and compliance
- Configuration and tunnels
- Agnostic to applications
- Flexibility to support both edge and data center deployments

FIPS VALIDATED 140-2 DELL GSA IT Schedule 70

Technical Specifications

CyphreLink BTx Security Appliances

Host Appliance	Dell PowerEdge XR2
Form Factor	Rack (1U) Height: 42.8mm (1.69") Width: 482.0mm (18.98") Depth: 808.5mm (31.8") Weight: 21.9kg (48.3 lbs.)
Network Interfaces	2x RJ45 1G (10/100/1000) 2x SFP+ 10G (10/100/1000/10000) Expandable Interfaces (Optional)
Management	1x RJ45 iDRAC (IPMI, SOL) 1x DB9 Serial Console 2x USB 3.0
Hardware Security Engine	Cyphre BlackTIE Crypto Core Module
Power Supply	Redundant hot swappable 550W power supplies
Operating Conditions	Temperature operating range: -15º C to 55º C; Shock resistance: 40G

Cyphre BlackTIE Security Engine

Certifications	FIPS 140-2 Validated (Certificate #3619 Design Patent (Pat. No. 10,623,382)
Platform	NXP Security Crypto Coprocessor Family
Random Number Generation (RNG)	Hardware-based True RNG sources true entropy for random and unpredictable key generation (NIST SP 800-90A)
Secure Boot	Crypto signed/validated firmware prevents side-channel attacks
Crypto Algorithms Supported	ECDHE, RSA, AES-128 bit or 256 bit, SHA, TLS 1.2 (AEAD - ECDHE-RSA-AES256-GCM-SHA384 and ECDHE-RSA-AES128-GCM-SHA384)
Key Protection	Patented key protections ensure true plaintext keys never exposed to root system OS, CPU, or memory
Trust Architecture	Trust keys generated in non-readable enclave using a unique One Time Programmable Master Key (OTPMK) fused to every system

CyphreLink VPN Application

User Interface	CyphreLink UI v3.X - Web-based user interface for simple yet powerful system and network encryption configuration and management
Performance	Up to 1 Gbps Ultra-low latency <1ms 50% Less VPN Overhead* * when compared to IPsec
Networks Supported	All Layer 4 networks VLAN, VRF, QOS, TOS
Encryption Algorithms	AES-GCM-128, AES-GCM-256, AES-CBC-256 DHKE 2048/4096

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

For more information
visit our website www.**cyphre.com**
or contact us at info@**cyphre.com**

Cyphre™
a RigNet company

Enabling Intelligence. Delivering Results.