TRUSTED ENTERPRISE SOLUTION

The One Stop, Interoperable Solution for all your Network and Data Security Needs

ST Engineering

The Asymmetrical Cyber Threat Landscape

The cyber threat landscape is asymmetrical. Cyber attackers are well funded, organised and resourced, giving them the edge over enterprises that are, as a starting point, already short on cyber security staff.

Aided by rapid technological advancements, deep behavioural insights and an expanding attack surface due to the Internet of Things, cyber attackers are delivering increasingly creative attack methods and destructive payloads that better target vulnerabilities in systems and individuals. Cyber hacks and data leaks are the new normal and will escalate in number, complexity and damage.

With the plethora of connected devices used for work, an intrusion into a single component can lead to the crippling of the entire electronic ecosystem that the company depends on. Every door into the enterprise needs to be secured.

Trusted Enterprise Solution

ST Engineering's Trusted Enterprise Solution is a comprehensive suite of hardware-defined cybersecurity products designed to fit seamlessly into any enterprise security architecture.

Headquarters

Data Centre

Secure Endpoint Cloud Management System

PhoneCrypt Centralised Management

NetCrypt U Series

Users on-the-move

Trusted Enterprise Segments

Designed to safeguard businesses against intrusions without compromising convenience and operational efficiency, Trusted Enterprise Solution enables people to secure and access sensitive information on the go, anytime, anywhere in a trusted working environment.

Secure Network - Encryptors

Secures the network and connects to multiple sites on public internet / private IP infrastructure. The customised encryption is ideal for different security requirements and applications.

NetCrypt

A series of IP encryptors that offers versatility and flexibility to the users by leveraging on public Ethernet/IP infrastructure to connect multiple sites in a secure manner.

EtherCrypt

High performance Layer 2 encryptors that protect the transmission of sensitive data over Ethernet and Metro-Ethernet networks.

COMMON CRITERIA

National IT Evaluation Scheme
BY CYBER SECURITY AGENCY OF SINGAPORE

Secure Endpoints - Mobile

Users can communicate and connect securely while on-the-go, anytime and anywhere with instant messaging, multimedia, attachment and voice features.

PhoneCrypt

A dedicated secure Voice over IP (VoIP) and Instant Messaging (IM) solution to ensure complete privacy for voice and IM communications for enterprise professional and organisations. It comprises of front-end clients and back-end VoIP/IM system which offers true End-to-End protection.

CES INNOVATION AWARDS 2020 HONOREE

Secure Endpoints - Storage

Enables users to store their information securely in a portable USB encrypting hard drive with two factor smartcard technology for authentication.

DiskCrypt

External hard drive with full disk encryption and smartcard based authentication to protect users' data.

DESIGN AWARD

COMMON CRITERIA

SINGAPORE GOOD DESIGN 2019

CES INNOVATION AWARDS 2019 HONOREE

Secure Endpoints - Workspace

A specialised endpoint that provides security at users' convenience through virtualisation to isolate the OS and strengthen security at the firmware level to guard against cyber exploitations. It is complemented by a cloud management system to empower IT administration capabilities.

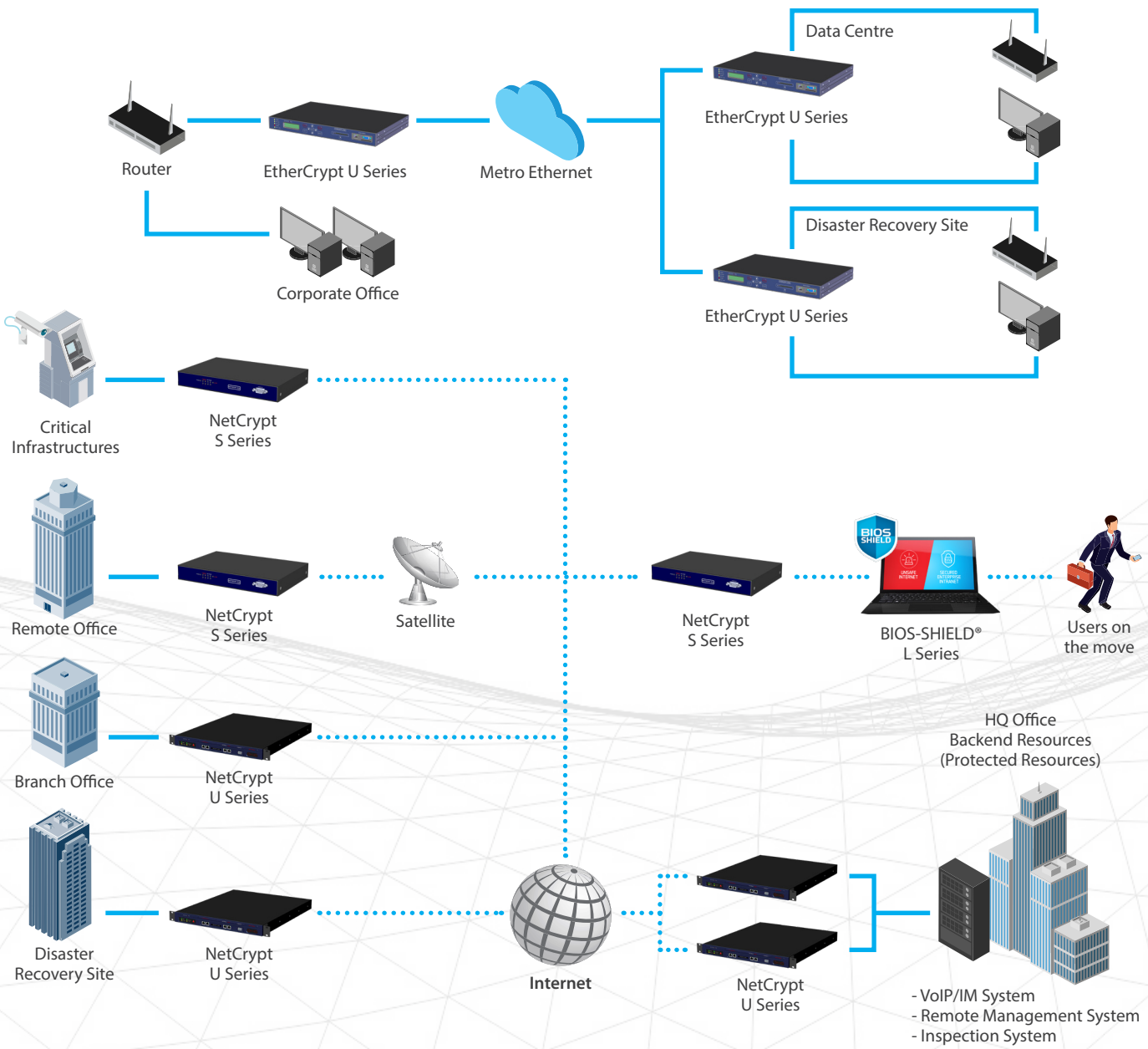
BIOS-SHIELD®

Provides security at your convenience; allows users and organisations to work in both trusted (Intranet) and untrusted (Internet) environments securely without compromising productivity. The secure browser enables users to freely search the internet and safely screen-shot and move graphics, photos and PDF files without the fear of importing malicious code.

Secure Networks
- Encryptors

NetCrypt Series is a range of IP encryptors that serve as a security gateway for office corporate LANs, site-to-site VPNs, mobile vehicles, rugged deployment and wireless inter-office connectivity. NetCrypt can be configured as a layer 3 or layer 2 encryption tunnelling device to accommodate the various infrastructure requirements desired, supporting point-to-multipoint (mesh, hub-and-spoke or hybrid) deployments.

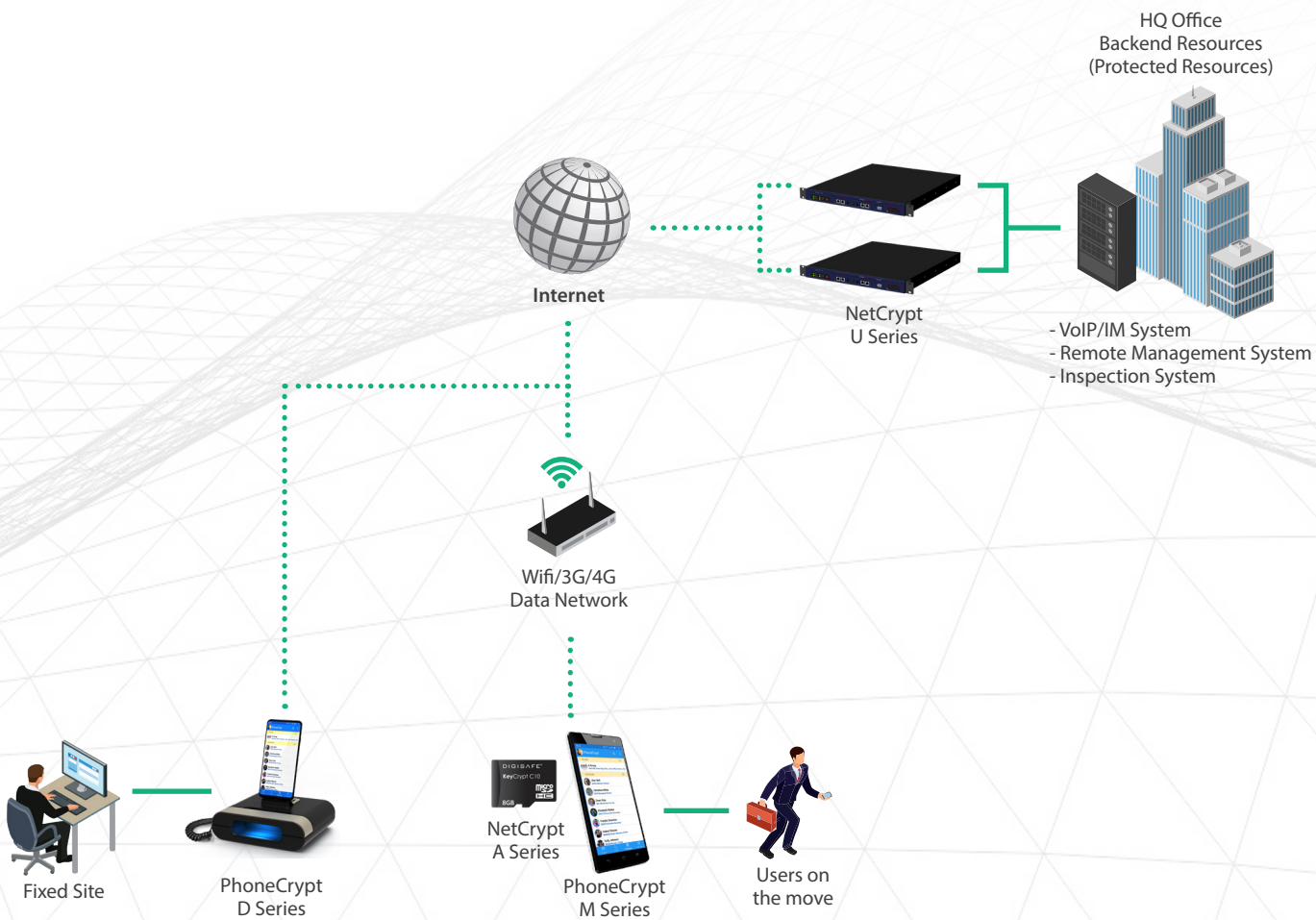
EtherCrypt Series comprises Layer 2 encryptors that protect the transmission of sensitive data over Ethernet and Metro-Ethernet networks. It is also suitable for point-to-point, point-to-multipoint and fully-meshed Ethernet networks.



Secure Endpoints - Mobile

Secure Phone Solution Suite is a dedicated Secure Voice over IP (VoIP) & Instant Messaging (IM) system that ensures complete privacy in communication for enterprise professional and organisation communications on-the-go anytime, anywhere. It consists of a front-end client solution and a backend VoIP & IM system to provide a trusted internal communication solution where users can embark on instant messaging, multimedia, attachment and voice features. From network to mobile handset secure technologies, we have developed strong hardware-based roots and trust in our mobile technology solutions.

PhoneCrypt D Series is designed for the office environment, connecting to backend secure VoIP system through RJ45 connection to the internet. PhoneCrypt M Series is designed for mobile users, connecting to the backend secure VoIP system through 3G/ 4G/ WiFi connection.



Secure Endpoints - Storage

In today's digital age, data has become one of the most crucial assets of enterprises, governments and individuals' privacy. Data compromise due to stealing, loss or repair of storage devices poses serious threats to both organisations and individuals, leading to serious operational, reputational damages and even financial losses.

DiskCrypt Series encrypts all data-at-rest (HDD/SSD or M.2 SSD) with two-factor authentication, requiring no software installation and operating independently of the operating system. The next gen ultra-slim credit card size version provides greater mobility, making it ideal for the convenience-conscious mobile workforce.

Users on the move

DiskCrypt M Series

BIOS-SHIELD® L Series

Fixed Site

DiskCrypt M Series

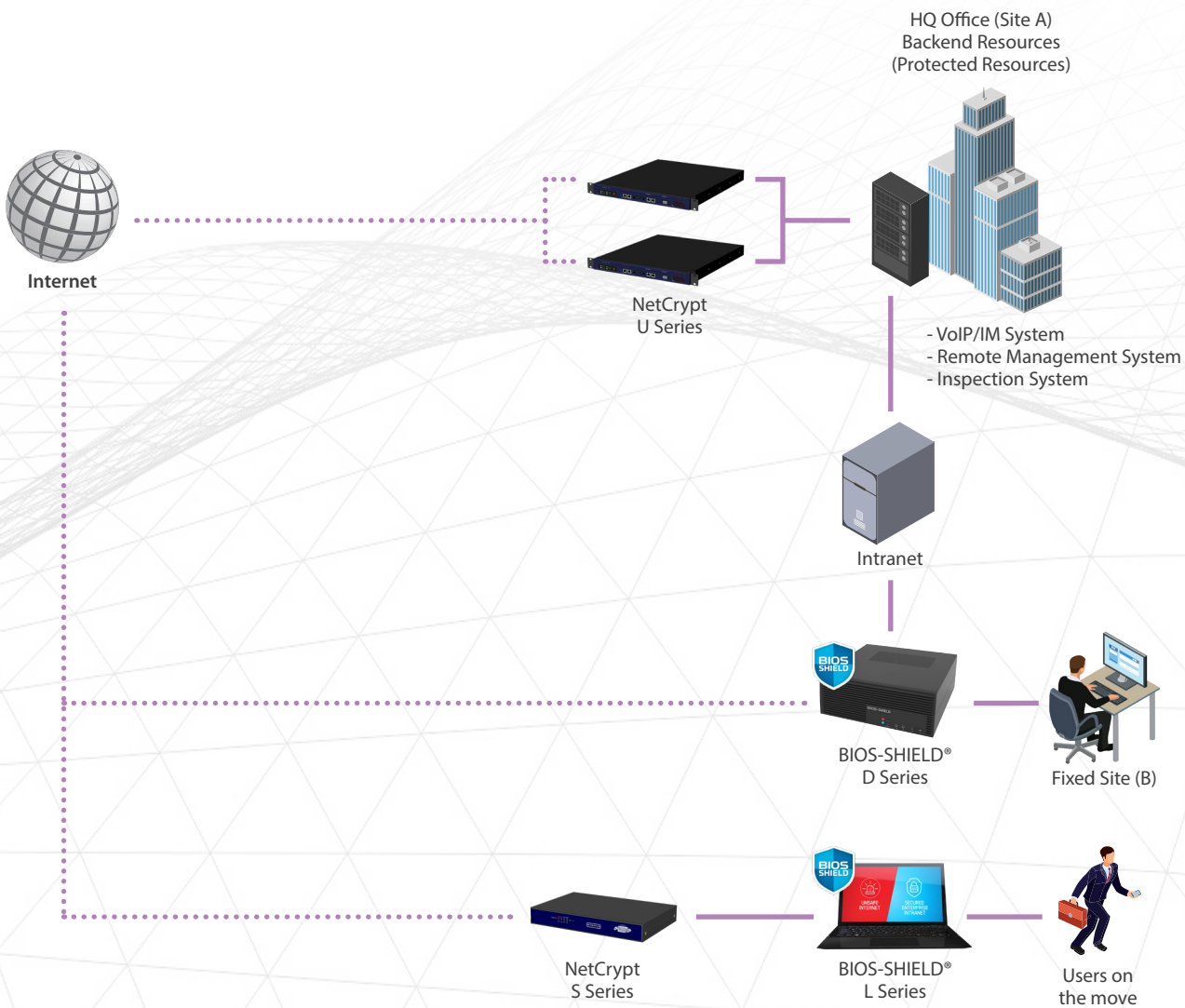
BIOS-SHIELD® D Series

Secure Endpoints
- Workspace

The following diagram provides an overview of how BIOS-SHIELD® Computers are implemented in organisations. Being stationed at a fixed site, BIOS-SHIELD® D Series allows users to access the backend resources of the HQ directly through the Intranet. At the same time, they can access the Internet freely and safely using the other workspace in a single computer.

BIOS-SHIELD® L Series is designed for users on-the-move, allowing users to connect to the HQ Office through an encrypted communication channel formed with a set of NetCrypt. With this encrypted channel, users can access the backend resources of HQ through the Internet. At the same time, they can access the Internet freely and safely using the other workspace on the same computer.

Remote Management System and Inspection System at the HQ Office provide remote administration and monitoring of all BIOS-SHIELD® Computers, including those stationed at a fixed site and those deployed to users on-the-move.

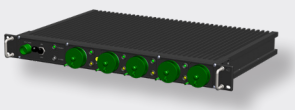


Encryptors Series

Secure Networks - Encryptors

NetCrypt S20

- IP encryptor with 100Mbps throughput aggregate
- Supports 50 concurrent IPSec tunnels
- Supports customised encryption algorithm
- Suitable for mobile vehicle deployment

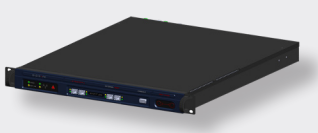


NetCrypt R100

- IP encryptor with 100Mbps throughput aggregate
- Supports 80 concurrent IPSec tunnels
- Supports customised encryption algorithm
- Operating temperature of up to 55°C
- Ruggedised and suitable for outdoor deployment

NetCrypt U1000

- IP encryptor with 500Mbps throughput aggregate
- Supports 300 concurrent IPSec tunnels
- Supports customised encryption algorithm
- Supports up to 3-factor authentication
- Path Redundancy Client High Availability

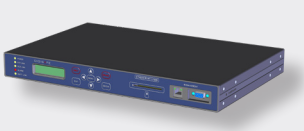


NetCrypt U2000

- IP encryptor with 1Gbps throughput aggregate
- Supports 800 concurrent IPSec tunnels
- Supports customised encryption algorithm
- Supports up to 3-factor authentication
- Path Redundancy Client High Availability

NetCrypt A10

- Application that provides secure connection with layer-3 VPN tunnel
- Roam capability
- Tunnel persistency
- 2-factor authentication



EtherCrypt U1000

- 1Gbps throughput Layer 2 encryptor
- Supports point-to-point, multipoint-to-multipoint
- Supports customised encryption algorithm
- FIPS 140-2 level 3 certified security module

EtherCrypt U2000

- Low overheads 10Gbps Layer 2 encryptor
- AES-GCM algorithm for data confidentiality, integrity and anti-replay
- Supports for Jumbo frames up to 8000 bytes
- Supports point-to-point, multipoint-to-multipoint
- Supports customised encryption algorithm

Secure Endpoints - Storage

DiskCrypt M100

- Disk encryption enclosure for data protection
- AES-256 XTS full disk encryption
- Supports 2-factor authentication
- FIPS 140-2 Level 3 and CC EAL5+ certified smartcard
- Operating System independent

DiskCrypt M10

- Data protection for M.2 SSD (2242)
- High performance USB 3.1 & SATA III interfaces
- AES-256 XTS full disk encryption
- Supports 2-factor authentication
- FIPS 140-2 Level 3 and CC EAL5+ certified smartcard
- Operating System independent

Secure Endpoints - Mobile

PhoneCrypt D200

- Secure voice conversation and instant messaging through backend PhoneCrypt system
- Layer 3 IPSec security for maximum security
- Supports AES algorithm for tighter data confidentiality
- Encrypted storage system for contacts and protects confidential data against unauthorised access

PhoneCrypt M100

- Trusted & seamless end-to-end solution
- Enhance security with NetCrypt A10 (with cryptographic MicroSD)
- Effective management system

Secure Endpoints - Workspace

BIOS-SHIELD® Firmware

- Loadable firmware version
- Suitable for most Intel 8th Gen CPU
- Performs internet separation with Secure browser
- Eliminates insider threats
- Time machine restoration by saving "snapshot" of their HDD
- Layered security approach
- Cloud management system
- USB device controls
- USB Encryption

BIOS-SHIELD® L100

- 8th Gen Laptop pre-loaded with BIOS-SHIELD® firmware
- Include all features of BIOS-SHIELD® firmware
- Suitable for on-the-move usage

BIOS-SHIELD® D100

- 8th Gen Desktop pre-loaded with BIOS-SHIELD® firmware
- Include all features of BIOS-SHIELD® firmware
- Suitable for office or fixed sites

Storage Series

Mobile Series

Workspace Series

www.stengg.com
cybersecurity@stengg.com

DOP 0620

www.stengg.com/cybersecurity