COST EFFECTIVE, EFFICIENT BRANCH LOCATION ENCRYPTION
CS SERIES
CS Series Encryptors

Scalable, efficient data encryption for high-speed network security without compromise.

It is often assumed that data networks are inherently safe. They are not. Data networks are vulnerable to security breaches. To be protected from a data network breach, cyber-attack or innocent routing error, your data must be encrypted. Only when encrypted can data be safe - rendering it useless to unauthorized parties.

SafeNet high-speed data network encryptors are internationally certified by independent testing authorities to protect your data while in motion. It’s why our encryptors are used by governments and defense forces in more than 25 countries!

THE CS SERIES

When high-performance, secure data transmission among “branch” locations is required, the CS series of low cost, high-efficiency encryptors is an optimal choice. Designed for more modest data transmission volumes and speeds, the CS series enables affordable solutions for less demanding requirements – without compromise.
SECURE BRANCH LOCATIONS

The CS Series Ethernet encryptors provides exceptional cost benefits to any organization needing to secure modest data volumes at speeds of 10 Mbps to 100 Mbps.

The choice of professional services organizations, such as law firms; health and government agencies and businesses with branch and remote locations; the low-cost CS series offers many of the benefits unique to our high-speed encryptors.

The CS Series makes defense-grade data security a practical solution for large, medium and small organizations.

ETHERNET SERVICES

Our CS Series platform provides secure, full line rate transparent encryption for data moving across Ethernet networks in point-to-point and multi-point environments.

Full interoperability with the CN and CS Series of encryptors means customers may standardize on one platform to secure data in motion across large networks between locations.

NETWORK AND MANAGEMENT

Each of the CS series encryptor products is configured and managed using CypherManager (CM7) – a purpose built software tool that makes managing your organization's encryption simple and safe.

The local (protected) and network (unprotected) 10/100 Base-T connections are made using CAT5 cables with RJ45 connectors. Support for Ethernet 802.3 and VLAN 802.1Q standards is provided. Command Line Interface and SNMPv3 management connections are via RJ45 connectors on the front panel.

CERTIFICATIONS*

Government and commercial customers benefit from the CS series independent testing authority certifications.

• Common Criteria
• FIPS

*Detailed certification information available upon request.
What makes SafeNet encryptors stand out?

Security Without Compromise

→ PERFORMANCE

The mix of “designed-in” outstanding performance capabilities makes our encryptors stand out. Our encryptors are world-leading and among them, hold all three major international, independent government testing authority certifications. These certifications are testament to our encryptors’ outstanding performance. They are ideally suited to the most demanding network environments. It’s why they are preferred by many of the world’s most secure organizations.

→ NEAR-ZERO LATENCY

SafeNet high-speed data encryptors are high-performance, operating in full-duplex mode at full speed without loss of packets. Latency is not affected by packet size and is approximately 4 microseconds per unit at 10 Gbps. Importantly, by using Field Programmable Gate Array (FPGA) technology, our encryptors’ outstanding latency performance is predictable and dependable. In summary, maximum throughput with zero protocol overhead.

→ FLEXIBILITY

Our encryptors enable maximum operational flexibility. This enables the encryptors to better meet customers’ specific and unique requirements and provide an optimized high-speed data encryption solution. The designed-in multi-purpose flexibility enables on-going operational simplicity, such as in-field upgradability as customers’ requirements change – protecting customers’ investment.

→ TRUSTED

Because SafeNet encryptors include the world’s only triple-certified products of their types, they are trusted by governments and defense forces around the world. This successful, exhaustive and rigorous testing over many years provides our government and commercial customers with maximum assurance. Certified CS encryptors provide the assurance of the leading international, independent government testing authorities: FIPS and Common Criteria.

→ COMPREHENSIVE RANGE

The CS range of Layer 2 encryptors provides the widest feature-set able to operate at 10 Mbps to 100 Mbps Ethernet protocols.
INTEROPERABILITY

Encryptors that support the same protocol are fully interoperable. For example, locations that have minimal needs may use CS encryptors, which can interoperate with a CN unit at a larger central site under the same CM7 platform.

EASY TO INSTALL

The ‘Bump in the Wire’ design of our encryptors makes them easy to install and highly effective. You simply place the encryptor at the access point to the public or private Layer 2 network and all data passing through the device is encrypted using an AES 256 bit encryption algorithm.

SIMPLICITY

Throughout the encryptor range, “set and forget” and transparency are underlying design themes. They help ensure simplicity of implementation, operation and management. Simplicity begins with ease of installation and continues with an intuitive user interface providing meaningful descriptive diagnostics – such as early warnings and simple fault-finding. The encryptors just sit and do their job – with minimal resource requirements.

LOW IMPACT

The low impact of our world-leading encryptor performance is not limited to network bandwidth and speed. It extends to network operations and management. Our encryptors simply “drop in” within the user network. They don’t require changes to other devices or network reorganization. Minimal network impact makes our encryptors a favorite among network engineers because the encryptors do not add load to the network operations or management.

RELIABILITY

SafeNet encryptors are designed, developed and manufactured to exacting standards. In addition to the high levels of security, the encryptors conform to international requirements for safety and environmental concerns, as well as providing high availability features with 99.999% uptime.

LOCAL OR CENTRALIZED MANAGEMENT

Configuration can be performed locally or remotely through our intuitive CM7 management software that also acts as the Certificate Authority in a network of encryptors by signing and distributing X.509 certificates.
CS Series Encryptors at-a-glance

<table>
<thead>
<tr>
<th>MODEL</th>
<th>CS10</th>
<th>CS100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Ethernet</td>
<td>Ethernet</td>
</tr>
<tr>
<td>Speed</td>
<td>10 Mbps</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>Protocol and application transparent</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Common Criteria certified</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>FIPS certified</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Support for external (X.509v3) CAs</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Robust AES encryption algorithm</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CRL and OCSP server support</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Automatic key management</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Flexible encryption policy engine</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Encrypts Unicast, Multicast and Broadcast traffic</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Policy based on MAC address or VLAN ID</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Self-healing key management in the event of network outages</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Per packet confidentiality and integrity with AES-GCM encryption*</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Store and forward architecture</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Smart network discovery and automatic connection establishment</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Centralized configuration and management using CM7</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Remote management using SNMPv3 (in-band and out-of-band)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tamper resistant and evident enclosure</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Fully interoperable with related CN models</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Your Assurance**
- Government and defense-grade assurance certified.
- Certified FIPS and Common Criteria
- No-compromise certified performance provides exceptional assurance, network performance and peace of mind.

**Why CS Series Encryptors?**
- No-compromise performance:
  - Near-zero latency
  - Maximum bandwidth
  - Minimum overhead
  - Scalable and flexible
  - Simple to manage
- Secure transmission of data through Layer 2 networks
- Defense-grade and ultra-reliable 99.999% up-time data network security
- Our high-speed encryptor technology is used by governments, defense forces and commercial organizations in more than 25 countries.

**Supported Networks**
- Ethernet II 802.3
- Ethernet over MPLS
- Carrier Ethernet
- VLAN/MPLS transparency

**CS10 Ethernet Encryptor**
- Designed as desktop systems that can be integrated into modern Ethernet networks.
- Encrypts the Layer 2 (Ethernet) protocol and can be configured for point-to-point or multipoint operation at speeds of up to 10 Mbps.

**CS100 Ethernet Encryptor**
- Designed as 1U high, 19” rack mounting systems that can be integrated into modern Ethernet networks.
- Configurable for point-to-point or multipoint operation at speeds of up to 100 Mbps.

*Pending firmware release*
Specifications

Cryptography
AES encryption algorithm
128 or 256 bit session keys
CFB or Counter mode
256 bit master keys
Optional algorithms (SEED, Aria, Camellia, custom)

Key Management
ATM Forum V1.1 specification
X.509 certificate authentication
RSA Public key Infrastructure
Periodic automatic key updates
KEK & DEK

Performance
Auto-negotiation of line speed
Speed of up to 100Mbps
CS10 - Latency 5 milliseconds (typical)
CS100 - Latency of 1 millisecond (typical)

Management
CM7 element manager
IPv4 and IPv6 support
Automatic encryptor discovery
SNMPv3 control, SNMPv1 monitoring
Out-of-band and In-band management
Alarm, Event, and Audit logs
SNMP traps and monitoring
RS232 local console (CLI)

Front Panel
CS10/100 - LED’s for interface, security, temperature, alarms, power.
CS100 - LCD status display, Power switch, RJ45 Local and Network connections, RJ45 Management connectors

Rear Panel
CS10 - RJ45 Local and Network connectors, RJ45 and DB9 Management connectors, Plug pack socket
CS100 - Power socket

All specifications are accurate as at the time of publishing and are subject to change without notice to meet the ongoing requirements of our customers.

Installation
0°/32°F to 40°C/104° operating temperature
0 to 80% RH at 40°C/104° operating
CS10 - Size: 185mm/7.3", 42mm/1.7", 160mm/6.3" (WxHxD)
Weight: 630 gram
CS100 - Size: 435mm/17.1", (19"), 44mm/1.7" (1U), 480mm/19" (WxHxD)
Weight: 6.8kg/15 lbs.

Shipping/Storage
CS10 - Size: 350mm/13.8", 180mm/7.1", 280mm/11", (WxHxD) – 2 units
Weight: 1.2kg/2.7 lbs. (1 unit) – 2.0kg/4.4 lbs. (2 units)
Max temperature: 40°C/104°F, 95% RH at 40°C/104°F
CS100 - Size: 580mm/22.8", 200mm/7.9", 580mm/22.8", (WxHxD)
Weight: 7.9kg/17.4 lbs.
Max temperature 40°C/104°F, 95% RH at 40°C/104°F

Physical Security
Tamper proof key storage (plus user password storage for CS10)
Tamper resistant/evident metal case
Anti-probing barriers

Power Requirements
CS10 - 90-240 VAC / 47-63 Hz Plug pack (7-20 VDC)
6 watts (20 watts maximum)
CS100 - 90- 240 VAC / 47-63 Hz
70 watts maximum
IEC 13 connector

Regulatory
Emissions – FCC Part 15 Class B
RoHS compliant
CE and N3912

Talk to Us
A brochure cannot provide all the information to determine the right encryptors for your data protection.
We have data security and network technical specialists who can help. We also work with data network providers and systems integrators to specify the best encryption solution for your needs.
Wherever you are, just contact us to discuss your needs. Or, if you prefer, your service provider can contact us on your behalf.
The optimal specification of encryptors for your data network is dependent upon many factors, including your IT and data network environments and business needs.