comforte

SecurDPS

The SecurDPS™ Product Suite – Powerful Data at Rest Protection on HPE NonStop

Introduction – *why should I care?*

Data breaches can cause severe damages to businesses processing sensitive data. To protect sensitive payment card holder data, PCI-DSS demands Primary Account Number (PAN) to be rendered unreadable anywhere it is stored. Other compliance rules and regulations like GDPR, HIPAA or local data protection laws require organizations to develop sound security strategies in order to protect their valuable data assets. However, instrumenting existing applications running on HPE NonStop servers with a compliant data-at-rest protection mechanism can be a daunting task.
The SecurDPS product suite provides the technology to protect any sensitive data with minimal efforts and without changing existing applications. SecurDPS allows organizations to take complete control of their sensitive data, lowering compliance costs and significantly reduce the risk of data breaches.

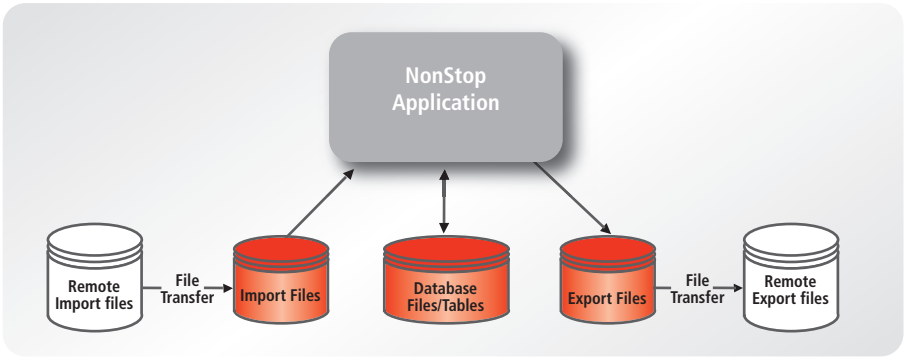
System Requirements

NonStop System:

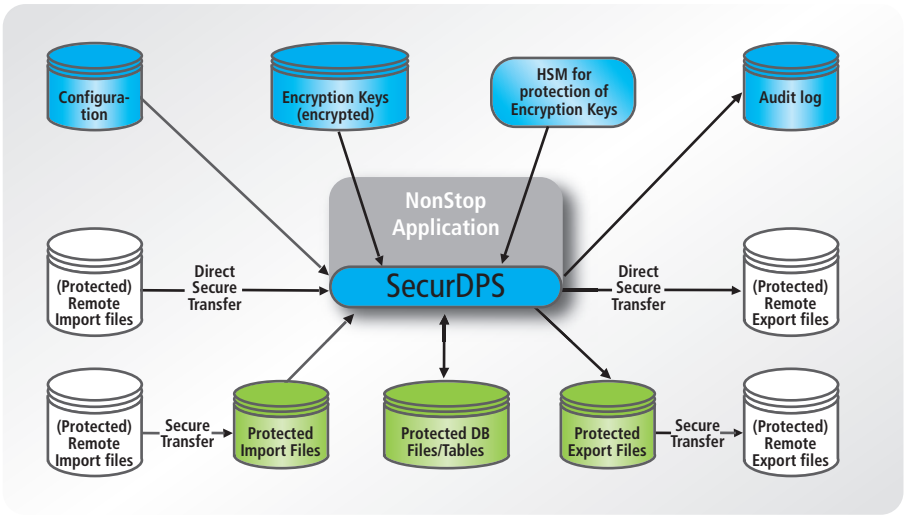
G06.27 or later
H06.07 or later
J06.04 or later
L15.02 or later

Architecture – *how does it work?*

The following diagram exemplifies a typical NonStop application storing sensitive data in database files or tables. It also exchanges files with sensitive data with remote systems which are intermediately stored on the NonStop system.



SecurDPS enables the protection of all sensitive data at rest without any application code changes, as depicted in the following diagram:



SecurDPS uses well-established I/O intercept technology to insert a protection layer into the application. Combined with advanced mechanisms for locating sensitive data in the I/O buffers for tokenization or encryption, SecurDPS operates completely transparently "under the hood" of the application.

Sensitive files exchanged with other systems can be protected by encryption; or the application can be instrumented to work directly with files on the partner systems via secure SFTP/SSH file transfer, eliminating any intermediate storage on the NonStop server. Optionally, remote files can also be protected using by encryption.

SecurDPS

Capabilities – *what does it do?*

- **Easy integration with your business applications**
  SecurDPS is the only solution in the marketplace that can integrate with your business applications without changing a single line of code.

- **Format-preserving field level protection**
  SecurDPS protects sensitive data while keeping the original format and characteristics of the data. This way, your applications and databases can simply continue to work with the data in a protected form.

- **Powerful Built-in Tokenization Engine**
  SecurDPS' patented tokenization scheme has been vetted by independent cryptologists. The stateless and vaultless architecture of the tokenization engine provides optimal performance with minimal system impact. SecurDPS is extremely flexible in terms of token formats and can address any business requirement.

- **Powerful Encryption**
  SecurDPS uses strong standards-based encryption algorithms to protect cryptographic material as well as sensitive application data.

- **On-the-fly PGP File Encryption**
  SecurDPS enables batch processes to work directly with encrypted files eliminating unprotected intermediate storage. Encrypted files can be easily exchanged with other systems supporting the OpenPGP standard.

- **Remote File Support**
  SecurDPS enables payment applications to import/export data directly from/to remote files via SFTP file transfer.

- **Comprehensive Key Management**
  SecurDPS is delivered with built-in key management capabilities. It can also be easily integrated with any preferred external key management system. Keys can optionally protected by a Hardware Security Module (HSM).

- **Granular Access Control and Auditing**
  SecurDPS controls which processes can access unprotected data based on object file, process name, user ids, creator ids, and numerous other attributes. It also provides an audit log of all authorized access to PANs in the clear.

- **Interacts seamlessly with Disaster Recovery solutions**
  SecurDPS is compatible with data replication tools including those which also employ intercept technology. The stateless token vault can be easily duplicated to backup systems supporting any disaster recovery architecture, including Active/Active.

- **Proven in production**
  SecurDPS is successfully running in several demanding production environments.

comforte 21 GmbH, Germany
phone +49 (0) 611 93199-00
sales@comforte.com

comforte, Inc., USA
phone +1-303 256 6257
ussales@comforte.com

comforte Asia Pte. Ltd., Singapore
phone +65 6818 9725
asiasales@comforte.com

comforte Pty Ltd, Australia
phone +61 2 8197 0272
aussales@comforte.com

www.comforte.com

comforte

For distribution partners in your region visit comforte's homepage www.comforte.com