Neutralize Data Breaches
Using data-centric security on NonStop

Prashanth Kamath U
Sr. Product Manager – NonStop Enterprise Division
Forward-looking statements
This is a rolling (up to three year) Roadmap and is subject to change without notice.

This document contains forward looking statements regarding future operations, product development, product capabilities and availability dates. This information is subject to substantial uncertainties and is subject to change at any time without prior notification. Statements contained in this document concerning these matters only reflect Hewlett Packard Enterprise's predictions and / or expectations as of the date of this document and actual results and future plans of Hewlett Packard Enterprise may differ significantly as a result of, among other things, changes in product strategy resulting from technological, internal corporate, market and other changes. This is not a commitment to deliver any material, code or functionality and should not be relied upon in making purchasing decisions.
HPE confidential information
This is a rolling (up to three year) roadmap and is subject to change without notice.

This Roadmap contains HPE Confidential Information.

If you have a valid Confidential Disclosure Agreement with HPE, disclosure of the Roadmap is subject to that CDA. If not, it is subject to the following terms: for a period of 3 years after the date of disclosure, you may use the Roadmap solely for the purpose of evaluating purchase decisions from HPE and use a reasonable standard of care to prevent disclosures. You will not disclose the contents of the Roadmap to any third party unless it becomes publically known, rightfully received by you from a third party without duty of confidentiality, or disclosed with HPE’s prior written approval.
Agenda

– Introduction to security on HPE NonStop
– HPE FPE and HPE SST – technology overview
– HPE SecureData and Companion Products
– Conclusion
– Q&A
Hewlett Packard Enterprise: Protect your digital enterprise

- Transform to a hybrid infrastructure
- Enable workplace productivity
- Empower the data-driven organization
- Protect your digital enterprise

Proactively protect the interactions between users, applications and data across any location or device.
HPE security strategy and focus

Provide capabilities to protect and secure:

– Your NonStop installation
– Communication between your NonStop servers and other systems and devices
– Data stored on your NonStop servers and backup media

Help you monitor and demonstrate compliance
Respond to reported security vulnerabilities
Integrate with HPE enterprise security products

Enable you to implement modern and industry standard security policies and practices for your NonStop infrastructure
Security is at the very top

Security and compliance

Primary Datacenter Challenges for 2015 and Beyond

Q: Thinking now about your datacenter operations, what do you see as the primary challenges your IT organization will face in the next 12 months?

- Security and compliance
- Cost/constrained capital budgets
- IT staff productivity, headcount, and skills
- Technology refresh [server and storage upgrades]
- Making effective use of cloud
- Data migration
- Disaster recovery/high-availability capabilities
- Datacenter automation
- Controlling power and cooling costs
- Datacenter consolidations/increasing density

n = 772
HPE NonStop security product portfolio

On platform
Users must be authenticated
Resource access is controlled

Guardian security
Safeguard
OSS security
ITP WebServer
XYGATE User Authentication
XYGATE Access Control

Network security
Sensitive data is encrypted
Incoming traffic can be filtered

NonStop SSL and add-ons
- cF SSL-LIB
- cF SSL-AT
NonStop SSH and add-ons
- cF SSH-LIB
- SFTP API
IPSec (IP CLIM)
Iptables / ip6tables (IP CLIM)

Data Security
Stored data and sensitive customer information is protected on disk or tape

HPE SecureData
XYGATE Data Protection (XDP)
cF Data Security*
Volume Level Encryption (VLE) with Enterprise Secure Key Manager (HPE ESKM)
OSM Data Sanitization
BackBox Virtual Tape Controller (VTC)
cF Secure Tape *
Secure Virtual Tape System (VTS)

Audit /compliance
Security events are audited
Security policies can be verified and compliance proven

XYGATE Compliance PRO
XYGATE Merged Audit and add-ons
- ArcSight Integration
- Plug-in for ACI BASE24
- Plug-in for ACI BASE24 eps
- Plug-in for HP HLR
- Plug-in for AJB-RTS

* Available soon

This is a rolling (up to three year) Statement of Direction and is subject to change without notice.
Data Security requirement for NonStop systems

What does PCI DSS say?

3.3 Mask the PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed)

3.4 Render the PAN, at a minimum, unreadable anywhere it is stored

3.6 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.

- Until recently, customers had two choices to encrypt PAN data
- Explicitly tokenize or encrypt in the application code
- Use Volume Level Encryption (VLE) to protect the data on media
- For ISV applications that customers use, VLE along with compensating controls was sometimes accepted by auditors
- With transparent tokenization available on NonStop, auditors are likely to insist on a tokenization based solution in the future
EU’s General Data Protection Regulation

– Pan EU regulation on how personal information of individuals in the EU is collected, shared and used globally
– Demands stringent data protection policies and practices
– To be implemented by April 2018
– Severe business impact due to data breaches
  – Notification to data protection authorities within 72 hours of an incident
  – Steep fines – up to € 20 M or 4% of world-wide revenue, whichever is higher
Data-centric Security
## Data-centric Security for end to end protection

<table>
<thead>
<tr>
<th>Threats to Data</th>
<th>Traditional IT Infrastructure Security</th>
<th>Data Ecosystem</th>
<th>Security Gaps</th>
<th>HPE SecureData Data-centric Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Compromise</td>
<td>Authentication Management</td>
<td>Data &amp; Applications</td>
<td>Security gap</td>
<td></td>
</tr>
<tr>
<td>Traffic Interceptors</td>
<td>SSL/TLS/firewalls</td>
<td>Middleware/Network</td>
<td>Security gap</td>
<td></td>
</tr>
<tr>
<td>SQL injection, Malware</td>
<td>Database encryption</td>
<td>Databases</td>
<td>Security gap</td>
<td></td>
</tr>
<tr>
<td>Malware, Insiders</td>
<td>SSL/TLS/firewalls</td>
<td>File Systems</td>
<td>Security gap</td>
<td></td>
</tr>
<tr>
<td>Malware, Insiders</td>
<td>Disk encryption</td>
<td>Storage</td>
<td>Security gap</td>
<td></td>
</tr>
</tbody>
</table>
HPE Format-Preserving Encryption (FPE)

- Supports data of any format: name, address, dates, numbers, etc.
- Preserves referential integrity
- Only applications that need the original value need change
- Used for production protection and data masking

<table>
<thead>
<tr>
<th>FPE</th>
<th>253-67-2356</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>8juYE%Uks&amp;dDFa2345^WFLERG</td>
</tr>
</tbody>
</table>

First Name: Gunther Last Name: Robertson
SSN: 934-72-2356
DOB: 08-07-1966

First Name: Uywjlqo Last Name: Muwruwwbp
SSN: 253-67-2356
DOB: 01-02-1972
Tokenization

- PCI DSS QSAs recommend tokenization to protect cardholder data at rest
- PCI scope reduction simplifies compliance and reduces costs

- Traditional tokenization technologies
  - Utilize database based “token vaults”
  - Can have issues with scalability, performance and disaster recovery
  - Introduce token collisions
  - Require backup per transaction
HPE Secure Stateless Tokenization (SST)

<table>
<thead>
<tr>
<th>SST</th>
<th>8736 5533 4678 9453</th>
<th>347-98-8309</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partial SST</td>
<td>1234 5633 4678 4321</td>
<td>347-98-2356</td>
</tr>
<tr>
<td>Obvious SST</td>
<td>1234 56AZ UYTZ 4321</td>
<td>AZS-UX-2356</td>
</tr>
</tbody>
</table>

- Replaces token database with a smaller token mapping table
- Token values mapped using random numbers
- Lower costs
  - No database hardware, software, replication problems, etc.
HPE SecureData Enterprise
HPE SecureData — Data Security Platform

HPE SecureData Management Console

HPE SecureData (Virtual Appliance)

Authentication & authorization sources (e.g. active directory)

HSM

Policy controlled data protection and masking services & clients

Business applications, data stores and processes

Payment terminals

SaaS & PaaS cloud apps

Partner integrations

HPE SecureData z/Protect, z/FPE

HPE SecureData Native UDFs

HPE SecureData Web Services API

HPE SecureData Command Lines & Automated File Parsers (C, Java, C#, .NET)

HPE SecureData native APIs

HPE SecureData File Processor

HPE Nonstop Applications & Databases

Mainframe applications & databases

Network Interceptors

Web/cloud applications (AWS, Azure)

3rd party SaaS gateways

ETL & data integration suites

3rd party applications

Teradata, Hadoop & Vertica

Business applications, data stores and processes

Volumes and storage

Enterprise applications

Production databases

Payment systems

HPE SecureData

Volume Key Management

iOS and Android devices

HPE SecureData Web Services API

HPE SecureData Command Lines & Automated File Parsers (C, Java, C#, .NET)

HPE SecureData native APIs

HPE SecureData File Processor

HPE SecureData z/Protect, z/FPE

HPE SecureData Native UDFs

Partner integrations

SaaS & PaaS cloud apps

Payment terminals

Policy controlled data protection and masking services & clients
HPE SecureData platform tools

Protected Data Environment

<table>
<thead>
<tr>
<th>Name</th>
<th>SS#</th>
<th>Credit Card #</th>
<th>Street Address</th>
<th>Customer ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kwfdiv Cqykgk</td>
<td>161-82-1292</td>
<td>3712 3486 3545 1001</td>
<td>2890 Ykzbpoi Clppn</td>
<td>S7202483</td>
</tr>
<tr>
<td>Veks Iounrfo</td>
<td>200-79-7127</td>
<td>5587 0855 7634 0139</td>
<td>406 Cmxt4 Osfaln</td>
<td>B0928254</td>
</tr>
<tr>
<td>Pdmme Whtob</td>
<td>095-52-6883</td>
<td>5348 9209 2367 2829</td>
<td>1498 Zeqjtbx Pqkg</td>
<td>G7265029</td>
</tr>
<tr>
<td>Eswf Gzqlyv</td>
<td>178-17-8353</td>
<td>4929 4333 0934 4379</td>
<td>8261 Sainbmeayqw Yotv</td>
<td>G3951257</td>
</tr>
<tr>
<td>Jsfk Tbluhm</td>
<td>525-25-2125</td>
<td>4556 2545 6223 1830</td>
<td>8412 Wbbhalhs Ueyzg</td>
<td>B6625294</td>
</tr>
</tbody>
</table>

Native APIs
- Enable encryption in custom apps
- C/C++/C#/Java
- Distributed and mainframe platforms

Command Line Tools
- Bulk encryption and tokenization
- Files and databases
- Variety of distributed and mainframe platforms

Web Services APIs
- Any web services enabled platform
- Additional layer of masking
- Offload processing on HPE SecureData Server

HPE SecureData File Processor
- Converged HPE SST and HPE FPE client solution in Java
- Handles different record types within the same file
- Efficient multi-field, multi-threading architecture
HPE SecureData on NonStop

Available for NonStop X and NonStop i systems

Two options

– Simple API
  – Called by applications to tokenize data or unstructured files
  – Uses structured (HPE FPE) and unstructured (“IBSE”) encryption
  – Supported on OSS

– Host SDK
  – Supports both HPE FPE and HPE SST
  – Also supports Voltage Payments Transaction Decrypt
  – Supported on Guardian (native only) and OSS

Work with HPE Stateless Key Management

– Secure SSL/TLS for key and policy fetch
– Stateless, resilient, proven.
– Smart caching so APIs can operate offline
– In turn connects to AD, LDAP if required for external authentication
HPE SecureData Companion Products on NonStop

What are they?
- XYGATE Data Protection (XDP)
- cF Data Security (cFDS)*

How do they help?
- Tokenize/encrypt your data without modifying the application code (OSS, Enscribe, SQL/MP)
  - Easily configure the solution to locate the data in your files/db to be protected
- SDK to simplify the implementation on NonStop should you prefer changing application code
- “Deep port” to the NonStop architecture and security model (e.g. scalability, audit logging)

* Quotable now, available soon
XYGATE Data Protection (XDP) High-level Architecture

SDK option:
- Lightweight API that can embed directly into NonStop application
- Ease and speed of implementation; deep port out of the box
- Enables non-native applications to utilize HPE SecureData
- Non-blocking access for multi-threaded applications
- Offload encryption to pathway server classes for scalability and throughput advantages

Intercept Library option (SDK + Enscribe + SQL/MP):
- No application changes required
- Overlays system’s I/O procedures with additional functionality to encrypt/tokenize on the fly
- Allows integration with other platforms via HPE SecureData enterprise support
- All sensitive data is protected in the database
- XDP configuration files control behavior (such as which files or fields to access and protect)
NonStop cF Data Security

- **Base module**
  - Application transparent integration for Enscribe databases
  - NonStop API wrappers for HPE SecureData for tighter control of the implementation
  - cF Data Security Manager controls access to the HPE SecureData platform, locates sensitive data, and audits access

- **SQL/MP add-on**

- **Advanced add-on**
  - Locate and protect data in complex structures, including ISO8583 messages and custom formats.
  - Tools for automatic, no-downtime data migration
  - Integrating with data transfer tools such as SFTP, FTP, IBM Connect Direct for on the fly protection/deprotection/translation at the interface
  - Transparent audit logging for access to sensitive data by applications

- **File protection add-on**
  - Protect structured file record areas (e.g. binary blobs) or unstructured sensitive files (e.g. private keys, password files)
  - Additional protection layers for sensitive files (e.g. HSM protection, split knowledge dual control mechanisms with secure unattended startup)
PCI Compliance Benefits

- HPE SecureData can protect customers from PCI risks by demonstrating data protection that avoids PCI fines and audit failures.
- HPE tokenization can reduce PCI audit scope reducing the audit footprint and decreasing compliance costs by up to 95%.
- Tokenization allows customers to move beyond just compliance to full data security for all types of businesses including:

  - Payment Capture
  - Retail and Online Apps
  - Payment Processing & Apps
  - Authorization Gateways
  - Issuing & Merchant Banks
Summary

– Threat of data breaches is real; effectively securing your sensitive data is the need of the hour
– HPE SecureData can help you to mitigate the risk
– Benefits of HPE SecureData and companion products on NonStop
  – Easily protect your sensitive data by implementing a data-centric security model
  – Offer you a choice – with or without modifying the application
  – Reduce the compliance cost through PCI scope reduction
  – Have a unified data protection solution across your enterprise
  – Get support from your familiar HPE support organization - GNSC
For more information

- HPE NonStop Security
- HPE Software Data Security
- Collaterals
  - HPE SecureData on NonStop Solution Brief
  - HPE SecureData Enterprise Data Sheet
  - Data Protection and PCI Scope Reduction for Today’s Businesses
Thank You
p.kamath@hpe.com