Knightcraft Technology
Information Security Specialists

Untangling the labyrinth of security software
How to figure out what you really need

Greg Swedosh
NonStop Security & Compliance Specialist, Knightcraft Technology

Agenda

- Brief Introduction
- The security software labyrinth
- What functionality do I need to ensure secure HPE NonStop systems?
- Evaluating security software – things to test, questions to ask

Introduction

Greg Swedosh

- Owner and senior security consultant of Knightcraft Technology.
- Working on HPE NonStop systems since 1985 (Tandem Australia).
- Providing professional services to HPE NonStop customers.
  - Australia, New Zealand, UK, USA, Singapore, Japan, India, Indonesia, Malaysia
  - Banks and financial institutions, large retailers, telcos, governments
- HPE NonStop Security and PCI DSS Compliance Specialist.
- Hands on implementation expertise in Safeguard, XYGATE, comForte.
- Strong systems engineering experience.
- Performed PCI DSS assessments on behalf of a QSA.
- Regular presenter on security at HPE NonStop Advanced Technical Bootcamp.
- Author of "*PCI DSS Compliance for HPE NonStop Servers*" white paper.
- Knightcraft security and compliance services are available from HPE and comForte.

The Security Software Labyrinth

- What do we really need?
- How do we know the software will do what we require?
- Is it really as good as it sounds?
- What questions should we ask of the vendor?
- How do we know when our systems are secure?

- How should we go about evaluating it?
- How much security software is enough?
- How do we know when our systems are secure?
- Is the cost reasonable for what it does?
- How about support?
- Nice to have vs really needed?

Confession

- I have worked as a software distributor, so I have been involved directly in computer software sales. I work with a software vendor now as one of my many roles.
- I have had roles in sales, technical support, customer training, product design, software implementation and as the customer. Sometimes all of these roles at the same time!
- Some of my best friends are computer software vendors.
  (at least they were before this presentation)

Disclaimer

- I am not suggesting in this presentation that any of the NonStop vendors are in any way dishonest or deliberately misleading. They are not.
- What I am suggesting is that you should approach any software evaluation with a high level of critical thinking and don't take things at face value.
- More educated and demanding customers = better software = more secure systems.

Software Product Design

- Software companies will produce the best software that they can with the resources they have.
- Try to satisfy what they believe are customer requirements or needs.
  - Sometimes the need is obvious (e.g. tokenization/encryption of data to satisfy regulations).
  - Sometimes the needs of the customer are a guess.

But…

- Customer environments vary.
- Customer requirements can vary.
- Have your specific needs been catered for?
  - Don’t assume that they necessarily have.
  - One size does not necessarily fit all.

Websites and brochures can claim anything

- Marketing collateral will always put the company products in a shining light.
- It may put competitive products in a lesser light.
- The devil is in the detail. Look for what's missing as much as what's there.
- Don't assume that glossy brochures and websites necessarily mean better products.
- Use the marketing tools as a starting point for your questions.
- Don't be afraid to ask "too many" questions.
- Always evaluate a product. Don't just get a demo.

Exciting New Products

New Products

- Beware marketing spin.
- Don’t be seduced by industry buzzwords.
- Beware of vapourware.
- How long has it been on the market?
- Is it actually being run in production anywhere?
- Are there any reference customers?
- Do you really want to be an early adopter or a beta tester (code for “you QA the product!”) ?
- Because one product from a vendor is good, it doesn’t guarantee that all of them will be.

Should I take my software salesperson's word at face value?

What functionality do I need to ensure secure HPE NonStop systems?

To have truly secure systems…

A list of what HPE NonStop customers really need at a minimum (1)

- Safeguard optimally configured to prevent unauthorized access and to provide auditing of file access.
- OSS directories/files optimally secured (if used).
- Security aspects of all subsystems configured to prevent users gaining unauthorized privileged access (e.g. Pathway, Netbatch, TCP/IP, TACL, SCF, Expand etc.)
- Security events automatically sent off-box to a SIEM device. Reporting and alerting.
- NonStop SSL/SSH implemented to provide encrypted TACL/OSH/FTPS sessions.
- Mechanism to provide individual accountability to all user logons (e.g. force users to logon to personal userid before logon to super.super or other shared privileged userid).
- Separation of production and development environments.
- Multifactor authentication (PCI DSS requirement).

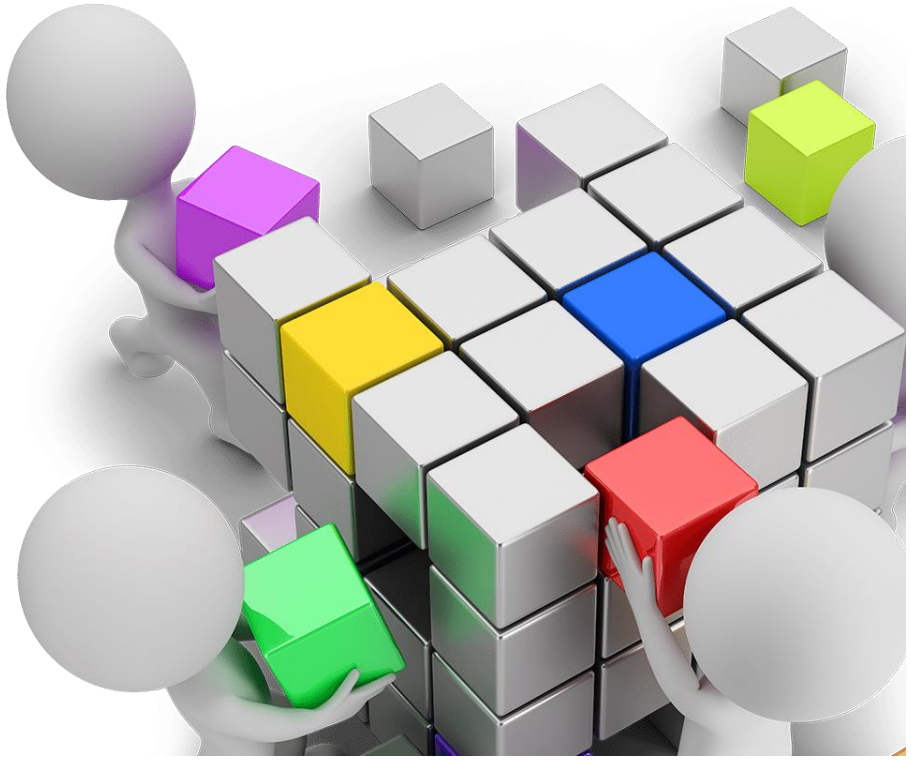
To have truly secure systems…

A list of what HPE NonStop customers really need at a minimum (2)

- Capture of all user sessions i.e. keystroke logging.
- File Integrity Monitoring (FIM) software to detect any changes to critical files (application objects, system configuration files, startup/shutdown files etc.).
- Encryption or tokenization of cardholder data. This can now be achieved without changes to the application or database using tokenization and intercept library based products.

To have truly secure systems…

- It's not just what software you have on the system, it's how it's configured!
- Just because it's installed and running, doesn't necessarily mean that everything is secure.
- It does not have magical powers.
- Make sure that it is configured optimally for your environment to achieve what it needs to achieve.

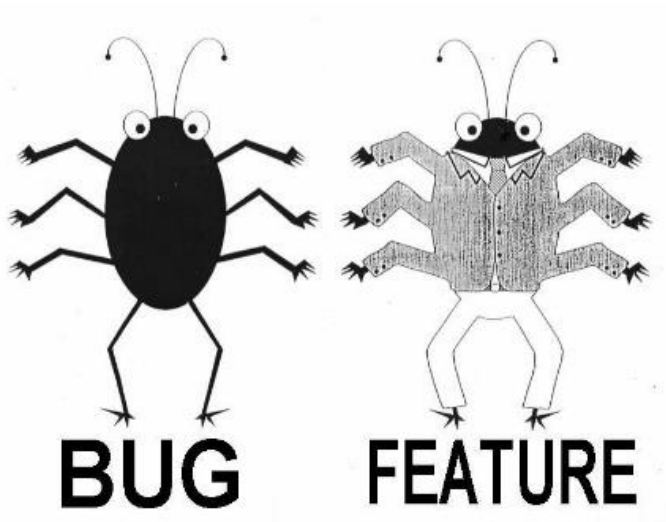


Evaluating Security Software

Things to test. Questions to ask.

Conducting a software evaluation

- Make sure you do evaluate the software.
- Go in with an open mind.
- Ensure that you focus on the actual requirements you are trying to address (Don’t get distracted by bells and whistles).
- Test the software in as much of a real life mode as possible.
- Try everything you can think of to “break” the software.
- Make sure that you log at least one fault call during the evaluation period. What is the company’s technical support like?
- Ask any questions via email to avoid any miscommunication and to make sure you cover everything off.
- Do also get a demo or assistance from the vendor in setting up your environment. You don’t want to miss the cool features.



Notes about the questions in the following slides…

- There are not necessarily right or wrong answers to these questions.
- These are a checklist of points for your consideration, to help you determine what exactly you need.
- Different answers will suit different customers.
- It is far from a complete list.
- Please send me your own suggestions for more questions to add to the list (greg.swedosh@Knightcraft.com).

General Questions (1)

- Does the software need to run as SUPER.SUPER or can any designated userid be used for running/managing the software?
- Is the software configured on the HPE NonStop host, via a client based GUI or via a web browser?
- How is the software configured? Have a look to see how complex the configuration files or configuration screens are.
- What authentication is required to manage the software configuration (if GUI or browser based)?
- Does the software use standard Guardian userids/aliases for authentication or does it have its own user database?
- How is the configuration protected from unauthorized access?

General Questions (2)

- Does the software have “NonStop” or restart capabilities?
- Does the software run as a Safeguard SEEP (Security Event Exit Process)?
- Are there special procedures required as part of an operating system upgrade?
- Does the software produce audit logs that include all required regulatory information?
- What performance impact is there in running the software?
- Does the software run in Guardian or OSS?
- Is there a requirement for other infrastructure such as web services to make the product work?
- Does the software require another machine to host its components (e.g. database) and if so:
  - How does it fit into your existing infrastructure?
  - Who will manage it?
  - Does it have appropriate security controls?

For Session Capture/Logging Software

- Does it operate fully in both Guardian and OSS (OSH) environments?
- What kind of sessions are captured (TACL, OSH, FTP… etc.)?
- Does it capture block mode sessions as well as conversational/command line sessions?
- Are passwords captured and displayed “in the clear” in the audit logs?
- Is it possible to “get around” the audit capabilities of the software ?
- Can the software capture the commands within a TACL macro and/or OBEY file?
- Is the origination of the event (i.e. IP address) captured for user sessions?
- Does an auto logoff feature exist where sessions terminate after a configurable period of inactivity?
- What overhead exists in capturing user sessions?
- What reporting tools can be used for viewing user sessions? Ask for sample reports to see how clear the presentation of user sessions is. Better still, evaluate and look at your own reports.

For Role Based Access Control Software

- Does it operate fully in both Guardian and OSS environments? If not, what restrictions exist?
- Does the software support use of aliases or does it require use of standard Guardian userids?
- Can user roles be allocated by group membership or does each user need to be configured individually?
- Can the software restrict access of privileged aliases separate from the underlying ID?
- Does the tool allow definition of a “role” and allow mapping one or multiple users to that “role”?
- Are all commands (input and output) fully audited?

For ALL Encryption Based Products

- Does it support strong protocols/encryption algorithms/cipher suites?
- Are the protocols/encryption algorithms/cipher suites configurable, allowing you to disable one individually in case a serious vulnerability is discovered without waiting for a patch to become available?
- How is the key management for encryption keys handled? Software or hardware based?
- Does the encryption solution interface with your existing HSMs?
- Are encryption keys stored unencrypted anywhere on disk?
- Are there performance figures or test tools that can assist in determining the processing overhead that will be added by encrypting the data?
- Does the implementation of the encryption add significant performance overhead?

For Data Encryption/Tokenization Products

- What modifications, if any, are required to the data file/table structure to implement field/column level encryption?
- What modifications, if any, are required to the application to enable the writing and reading of encrypted data?
- Which programming languages are supported? Are both native and TNS mode supported?
- Are both the Guardian and OSS environments supported?
- Are there programming examples in your required programming language provided to assist in implementation of the encryption solution?
- Does the solution allow for integration with applications on other computing platforms?

For File Integrity Monitoring (FIM)

- Does it use a secure fingerprinting technique such as SHA2 to establish if a file has changed?
- Does the software operate in real time or are collections run in batch (e.g. daily, weekly etc.)?
- What mechanisms exist to ensure that the software does not adversely impact the performance of the core application and system?
- Is the software controlled at the NonStop host, from a Windows workstation or both? If from a Windows workstation only, are there any firewall issues within your organization that need to be addressed? Is communication between the Windows workstation and NonStop server appropriately secured?
- Is a full history kept of when the files have been checked for changes and the results?
- Is every occurrence of a file being re-baselined audited?
- Is there a suitable security framework in place that prevents unauthorized changes of configuration?
- How are changes to the configuration audited?
- How flexible and user-friendly are the configuration and reporting?

For Session Encryption Software

- Is the product an SSL/SSH proxy? If so, can the audit logs link the “real” IP Address to each user session?
- If your organization is requiring session IP address for auditing or control purposes, you should ensure the interoperability of the session encryption software with your other security related software, as SSL proxies typically return an IP address of 127.0.0.1 (the loopback IP address) when interrogated by other processes.

For Audit Logging/Reporting/Alerting (1)
(which may be a feature of any software product)

- Do the audit logs contain all PCI required information (as per Requirement 10.3)?
  - User identification, Type of event, Date and time of event, Success or failure indication, Origination of the event (e.g. IP address. Note that NAT or use of SSL proxy may be an issue in the use of IP address to determine the origin of the event. See Session Encryption)
- Does the event include the identity or name of affected data, system component, or resource.
- What kind of event is generated when the software is shutdown or started?
- What kind of event is generated when the audit logs fill up or roll over?
- Can it be proven that the audit logs have not been tampered with (e.g. by use of audit record checksums such as SHA2)?
- Can audit records be sent “off box” to a centralized audit logging solution (e.g. to a SIEM device such as HPE Arcsight, SPLUNK etc)?
- Does the software allow configuration of alerting on selected events?
- How does the software function if audit records cannot be logged for some reason (e.g. if audit logging disk is full)? Does the software continue to function or does it stop all processing if audit cannot be captured? Is this configurable?

For Audit Logging/Reporting/Alerting (2)
(which may be a feature of any software product)

- Do audit logs automatically rollover when they are full?
- Do “old” audit logs get overwritten by new logs i.e. similar to Safeguard’s “Recycle Files”?
  - If so, what mechanism is in place to ensure that required files are not overwritten?
  - If “old” log files are not recycled or overwritten, is there an archive or cleanup mechanism to prevent disks from filling up with audit logs?
- Can reports be scheduled? If so, does the product have an inbuilt scheduler or does it use host based batch utilities such as Netbatch, Multibatch etc. or a workstation based utility such as Windows Scheduler?
- Are reports host based or PC based?
- Can reports be sent automatically to centralized locations e.g. network file server?
- How flexible/user-friendly/configurable are reporting and alerting?

How About Technical Support?
(You know you're going to need it!)

- What methods can you use to contact support? Phone/Email/Website?
- How responsive is support to your issues and questions?
- How technically competent do they appear?
- How helpful/friendly/personable?
- Does the company seem to have a good support process?
- Is support 7x24 if required and if so, is it available?
- What is the documentation like?
  - Suitably detailed?
  - Examples?
  - Easy to follow?
  - Covering everything?

Be Demanding!!!

- Vendors are keen to find something that differentiates their software. They may be open to suggestions for enhancements.
- Vendors want their products to be as strong and as good as possible. It's our job to help them.
- The more that is demanded of software products, the better they'll become.

Which all leads to BETTER SECURITY!!!

The Definitive Resource

PCI DSS Compliance for HPE NonStop Servers (Technical white paper)

– Details what a QSA will typically look for and what you need to do for EVERY requirement of PCI DSS.

– Independent of any software vendor. Highlights solutions from them all.

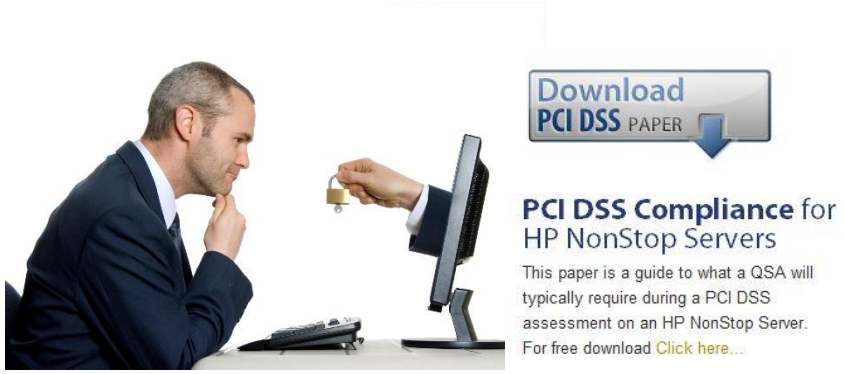
– Includes section on evaluating security software to meet your PCI compliance needs.

– Steps on preparation and how to approach a PCI DSS assessment.

– Information on cardholder data locations, privileged userids, security config etc.

– Download the latest version (PCI DSS 3.2) for free from www.knightcraft.com.

– HPE NonStop TBC presentation *You may be PCI DSS compliant but are you really secure?* (http://www.knightcraft.com/you-may-be-pci-dss-compliant-but-are-you-secure)



How Knightcraft Can Assist You

Knightcraft services can be procured from our partners

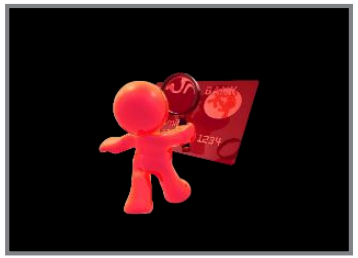
Hewlett Packard Enterprise

comforte

Security Review Service

Security Configuration

PCI DSS Compliance



PAN Data Discovery

For more information

- See the Knightcraft website www.knightcraft.com
- Email greg.swedosh@Knightcraft.com
- Talk to your HPE or comForte account team

Let Knightcraft Technology, the experts in HPE NonStop server security and PCI DSS compliance, help you to ensure that your systems are truly secure, as well as meeting your compliance requirements.

Knightcraft Technology
Information Security Specialists

Thank you

Greg.Swedosh@Knightcraft.com
www.Knightcraft.com