Hewlett Packard
Enterprise

DISCOVER, MONITOR AND PROTECT – A DATA-CENTRIC APPROACH TO NONSTOP SECURITY, COMPLIANCE AND TOKENIZATION

Sean Bicknell

4tech Software

DATA-CENTRIC SECURITY

- Security needs to be more than just tightening system access
- Putting up stronger walls is not enough
- Your data must pass through these walls for your company to function
- De-sensitising / de-valuing / de-identifying, your sensitive data mitigates all of the risk
- This must be done in a non-intrusive way
  - To reduce cost / time of implementation
  - To maintain application format
  - To leverage your current environment
- Regulatory Compliance

DATA DISCOVERY

- You can't protect what you don't know exists!
- Fast and efficient, real time data discovery is the first step
- PCI Version 4 adds new emphasis on the importance of scoping
  - 12.5.2 mandates that you must prove there is no sensitive data stored outside your CDE
- Understand the level of your risk
  - Today
  - Every day
- Reduce liability and exposure of your sensitive data
- Regulatory compliance
  - Achieved
  - Monitored
  - On-going compliance

DATA PROTECTION

- De-value your key data with industry standard tokenization
- Protect ANY sensitive data using format preserving techniques
- Implementation should be quick and straight forward
- Environment changes should be kept to a minimum
- High availability and scalability
- Application integration should be seamless and configurable
- On-box solution
  - Reduces exposure
  - Minimises cost
  - Speeds up deployment
- Value for money

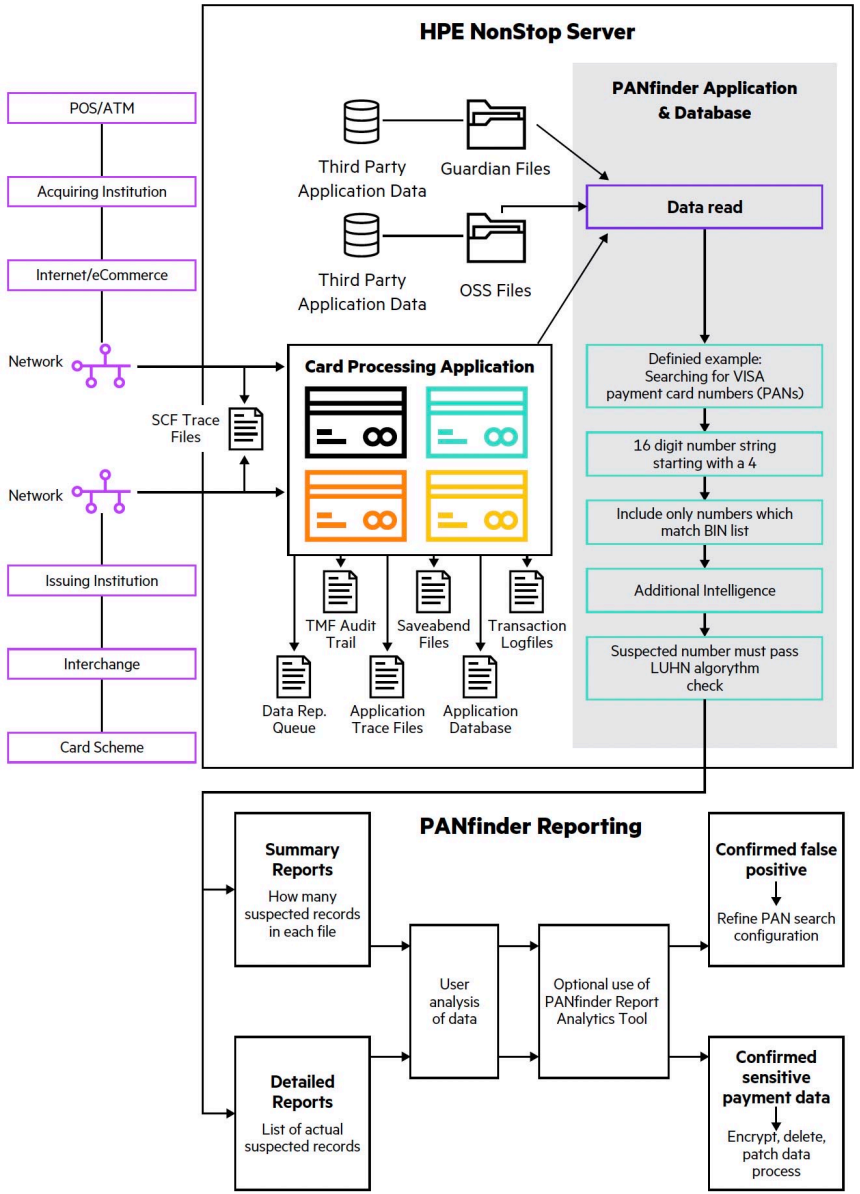
REAL TIME THREAT DETECTION

- Mitigating threats requires speedy detection to identify and properly neutralize any system vulnerabilities
  - Monitor all relevant activity in real time
  - Identify any malicious activity that could compromise your business
- This is true of both your data and your infrastructure
  - Continuous monitoring for unprotected sensitive data is key to regulatory compliance
  - Continuous, automated monitoring of the systems around your data, is a key factor in creating a Zero Trust environment
- Determine the appropriate response to the vulnerability with speed and confidence
- File Integrity monitoring is a PCI requirement

PANFINDER FROM HPE

PANfinder is a comprehensive payment card data discovery solution. It searches your HPE NonStop systems for hidden and unmasked payment card numbers and mag stripe data

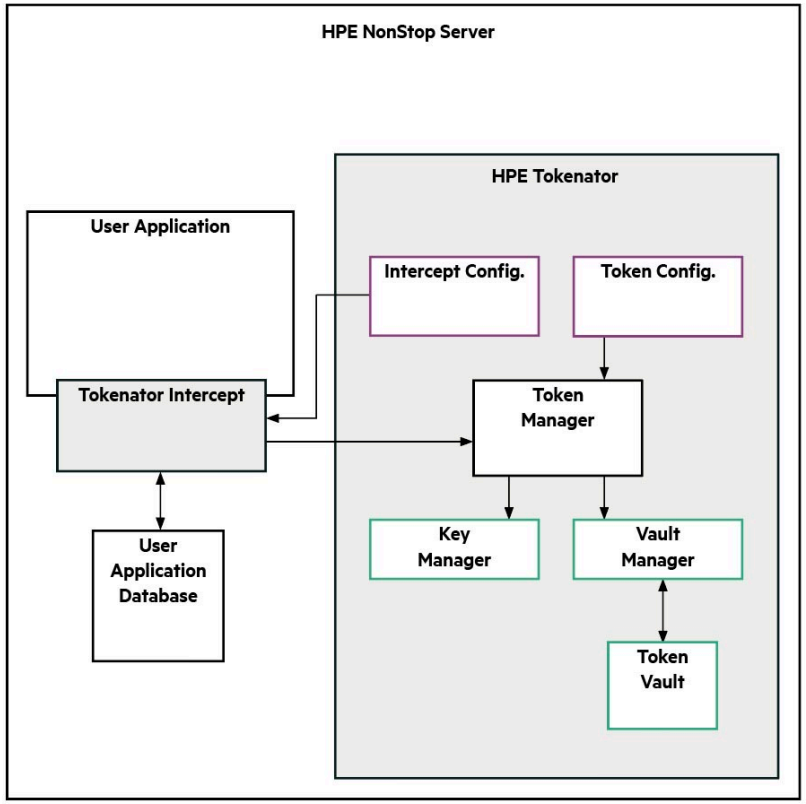
- Essential PCI-DSS scoping and compliance tool
- Industry leading, HPE NonStop specific data discovery solution
- Extremely accurate – Intelligent false-positive reduction
- Enterprise connectivity via SYSLOG to SIEMs
- Automated searches and comprehensive reporting
- QSA scan mode – identifies transaction data
- FASTSCAN gives multiple options to increase speed of data discovery
- Scanning of open and locked files



TOKENIZATION FROM HPE

Tokenator is a tokenization solution with format preserving functionality and Intercept based operability for the HPE NonStop

- Current features:
  - Vaulted Tokenization – AES256 protected
  - Intercept technology allows Integration without the need for user application changes.
  - Will support all future industry standard algorithms
  - Format preserved tokens
  - Enscribe file support
  - Sensitive data masking
  - Identifiable tokens
  - Configurable token structure
  - 100% NonStop based



TOKENIZATION FROM HPE

Tokenator is a tokenization solution with format preserving functionality and Intercept based operability for the HPE NonStop

- Fast and easy to implement:
  - Ten minute install
  - Bind the Tokenator library to any program
  - Test program
  - Documented examples

- Roadmap features – driven by HPE & customer demand:
  - SQL/MP support
  - SQL/MX support
  - Vaultless tokenization
  - HSM integration
  - File / table access auditing
  - Enterprise integration

INTEGRITY DETECTIVE FROM HPE

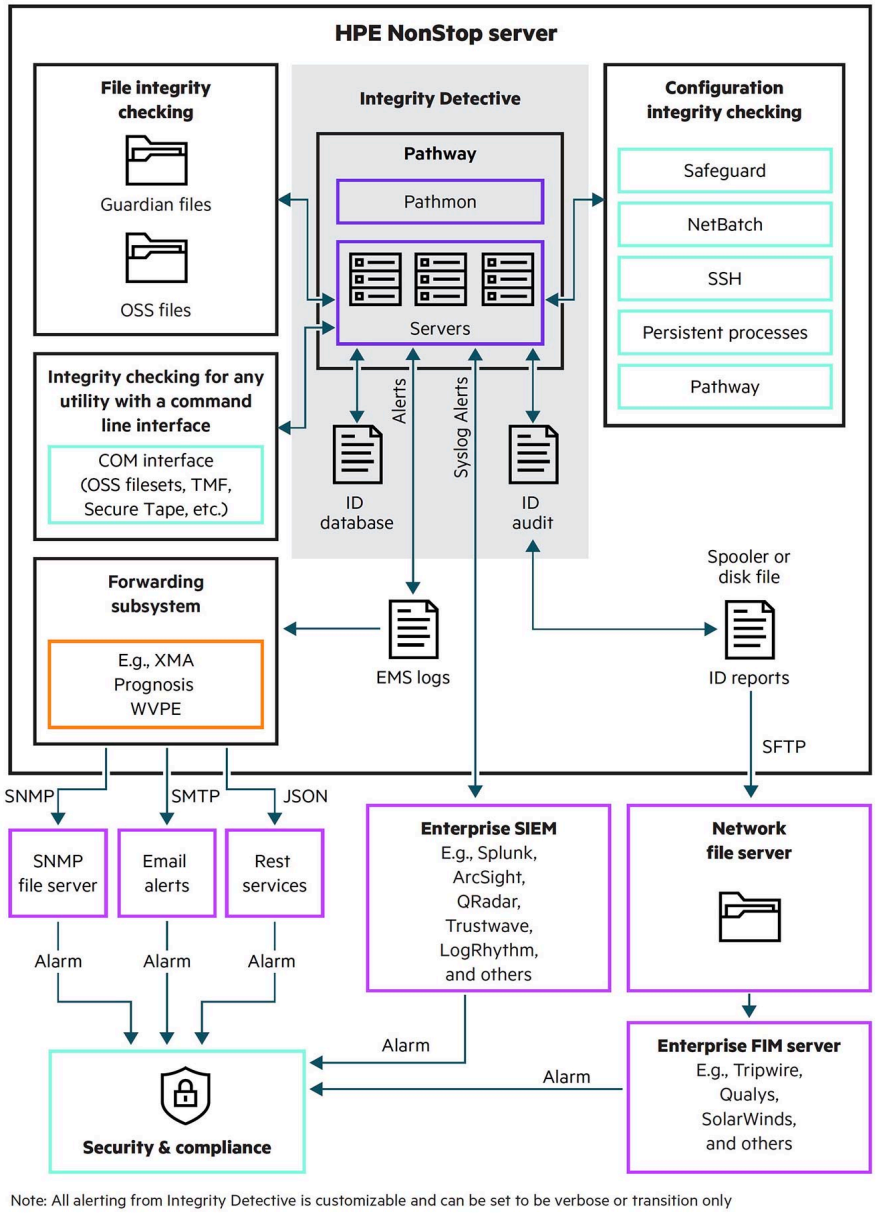
Integrity Detective is the most feature rich, real time, file & subsystem integrity monitoring solution available today on the HPE NonStop server.

Monitoring – Files and Subsystems

- Guardian and OSS files.
- Netbatch Jobs and Pathway.
- Folder watching: detect files added or deleted from watched subvolumes or subdirectories.
- Safeguard Objects.
  - Access Control Lists (ACLs) for discs, files, processes, devices, etc. Also Safeguard Groups, Object Types, SEEPs, and Globals.
- COM program output monitoring.
  - ID can monitor third party tools and subsystems
- CLIM configuration and status monitoring

Auditing

- Full auditing of all actions (baselining of files or subsystems, control parameter changes, state transitions). EMS alerts.



Note: All alerting from Integrity Detective is customizable and can be set to be verbose or transition only

INTEGRITY DETECTIVE FROM HPE

Security

- Inbuilt security defining what each user can see or do.
- Fully customizable user permissions.

Simple, cost-effective Infrastructure

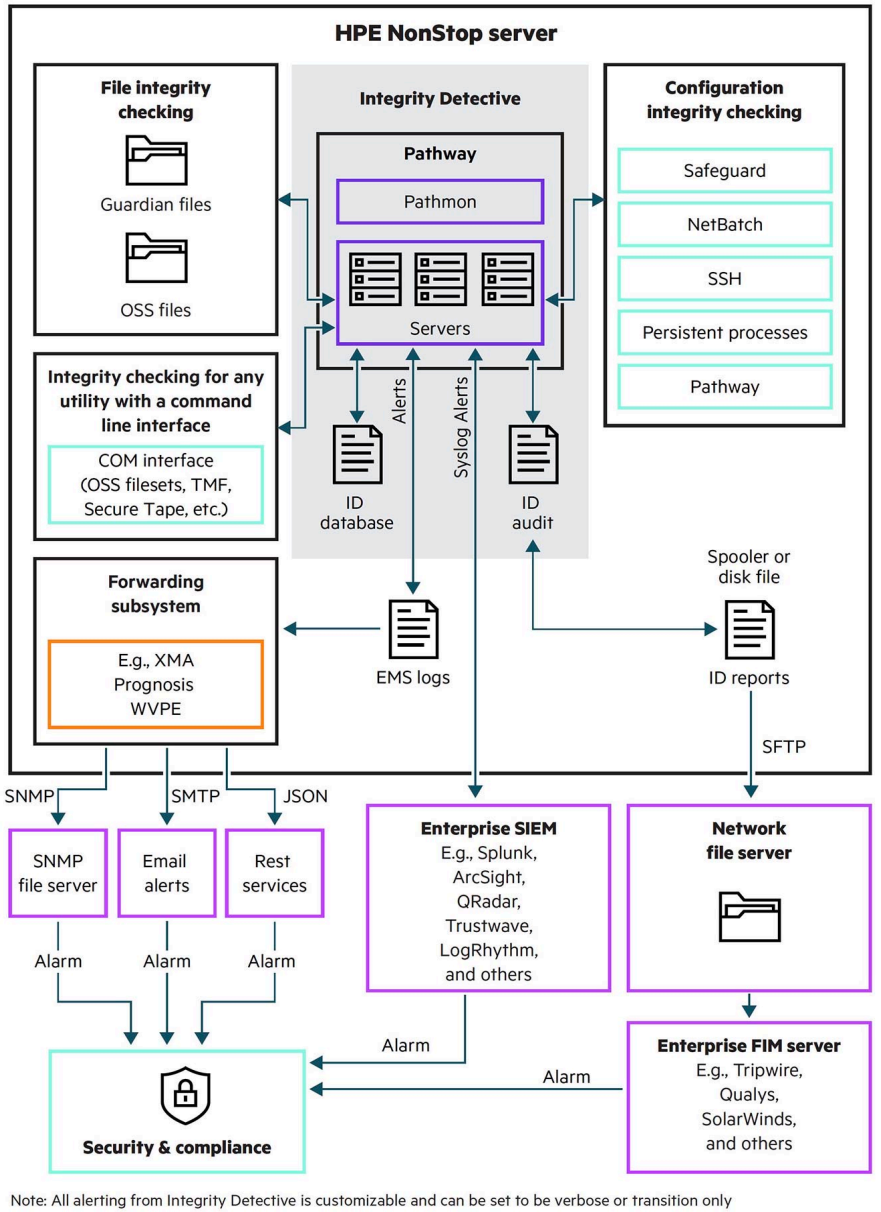
- No extra server hardware or technology required.

Change Detection

- **If a file (or subsystem param) is changed and then changed back again to its baselined value, ID raises an “amber” alert, indicating that something may be amiss and should be checked.**

Enterprise Alerting

- Continuous monitoring generates real time alerts. Instantly sends alerts to SIEM (via syslog), EMS, or both. Alerts will also be displayed in the GUI.
- Found Values. ID captures a mismatched value and displays it in the GUI. User can see immediately the ‘should-be’ and ‘actual’ values.
- All settings fully configurable.

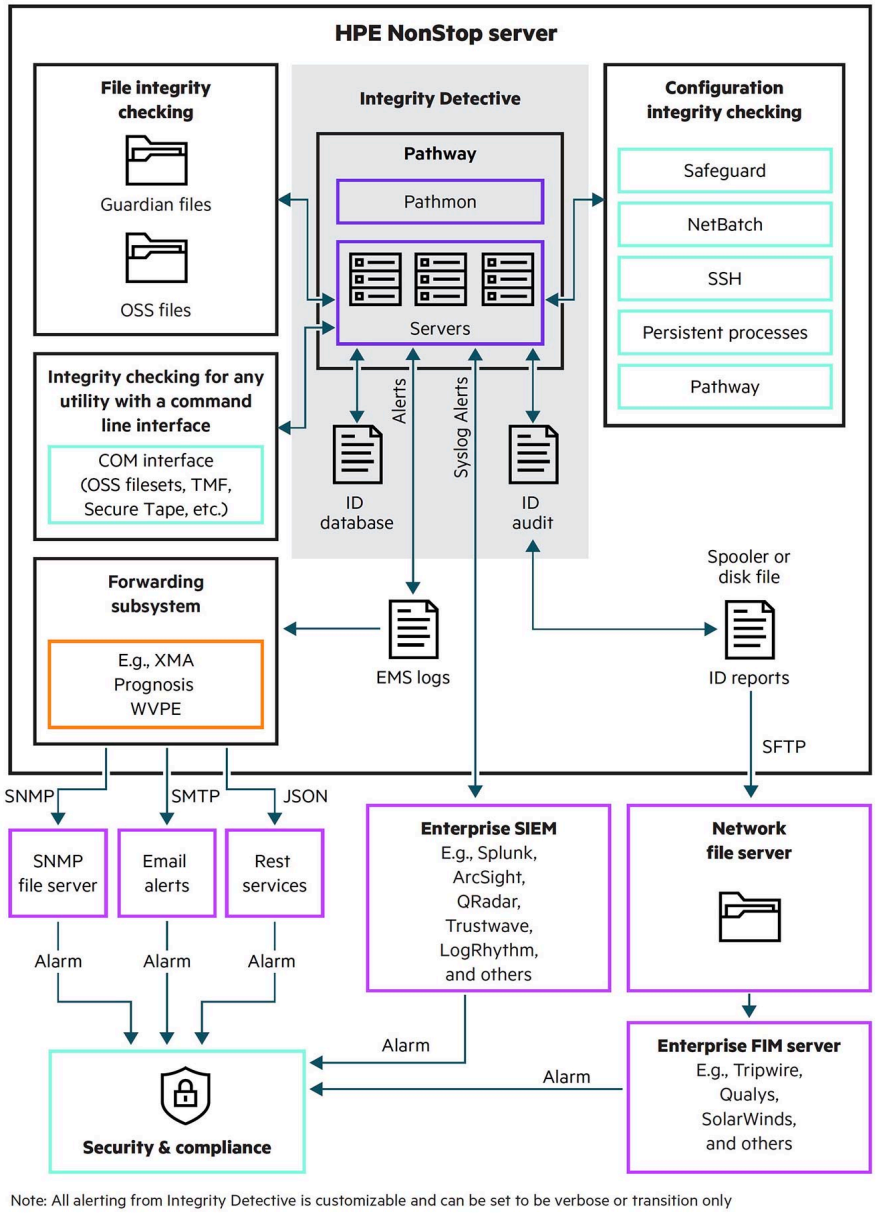


Note: All alerting from Integrity Detective is customizable and can be set to be verbose or transition only

INTEGRITY DETECTIVE FROM HPE

Useability

- Quick to set up, easy to configure.
- Can add multiple files from a subvol or multiple subvols simultaneously.
- Notes can be used to track changes and activity within ID.
  - Users can tag a note against each object monitored.
  - This allows a history to be built up over time showing what has happened to an object and what remedies were actioned.
  - This can reference change documents or trouble tickets so that auditors can see that the 'alleged' (documented) processes actually took place.
- Most screens have a built-in Print function. PDF ‘prints’ can be useful offline or as audit evidence.



Note: All alerting from Integrity Detective is customizable and can be set to be verbose or transition only

INTEGRITY DETECTIVE FROM HPE

The Integrity Detective walk through video has been removed to reduce the file size of this presentation file.

The video can be found on our YouTube channel here:

www.youtube.com/@4techsoftware663

IN CONCLUSION

- Regulatory compliance is not a once a year, tick in the checkbox task
- Prove where your data ‘is’ and ‘is not’
- Regulatory compliance doesn’t equal security
- Scoping and Data Discovery are a key requirement in achieving regulatory compliance
- Tokenization is the industry standard way to protect / devalue sensitive data
- Protecting the protection – ensuring that no changes to your environment go undetected

- Complex and critical functions performed with a simple, easy to mange solution

THANK YOU

CONTACT:

Sean Bicknell
E-Mail: Sean.Bicknell@4techsoftware.com
WWW: www.4techsoftware.com