Hewlett Packard Enterprise

Brochure

Secure your HPE NonStop systems

HPE NonStop Security and PCI DSS compliance services

The need for security

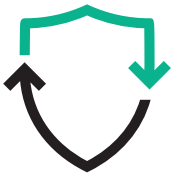
Securing systems and sensitive data are more important now than ever. Data breaches of large corporations are a regular occurrence these days and when they happen, they are extremely costly. Vigilance in establishing and maintaining the security of your HPE NonStop systems is essential for ensuring that your data remains safe.

HPE NonStop security is a specialized skill requiring continuously evolving knowledge and expertise. Our security specialists will give you the confidence that your security is optimally configured and that your customer and corporate data are safe.

A number of high profile multi-million dollar data breaches have occurred in organizations that believed that they were PCI DSS compliant at the time of the breach. Compliance does not guarantee security.

Best practices in security

Hewlett Packard Enterprise in collaboration with Knightcraft Technology offers you the services to help you not only comply with the Payment Card Industry Data Security Standards (PCI DSS) but also to make sure your systems are secure. Our services ensure that your security is in line with both industry best practices as well as your corporate security policies and practices.



HPE NonStop security review service

Identification and remediation of vulnerabilities
Despite best intentions, security gaps can open up in any system environment. Personnel knowledgeable in the security setup of the system move on, systems are upgraded without revisiting old configurations, changes are made to systems, application, and operating environments, as well as security technology and best practices change. It is only by regularly reviewing your system security that you can truly be certain that everything is optimally configured.

The HPE NonStop security review service provides a full analysis of all security-related subsystems such as Safeguard, open system services (OSS), SSL/SSH, XYGATE products, Pathway, TACL, NetBatch, ISV security software configuration, and so on. It will identify any areas where users could exploit the configuration to gain unauthorized access or privileges, and it will provide the steps required to remediate any gaps. It will also examine procedures around privileged user-id management, reporting and alerting, and the controls in place between production and development environments.

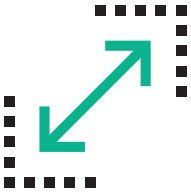
If desired, internal "hands-on" penetration testing can also be conducted on your HPE NonStop servers. The HPE NonStop security review service helps you secure your systems and sensitive data.

HPE NonStop security configuration

Best practice configuration for your security
Be it a need to implement and configure Safeguard, XYGATE modules, SSL/SSH, or other security-related software, the HPE NonStop security configuration service can help you out. This service will ensure that software you have either purchased or received as part of the operating system is configured in an optimal fashion. Your security subsystems will be configured to utilize all features that help achieve your security and compliance objectives, ensuring that there are no gaps that could be exploited to gain unauthorized privileged powers or access on the system.

HPE NonStop PCI DSS compliance

Ensure both security and compliance
Organizations that are subject to PCI DSS must not only achieve compliance for an assessment but must also continually maintain it. Unfortunately, the combination of the checklist and periodic nature of PCI assessments and, in some cases, lack of qualified security assessors' (QSA's) HPE NonStop expertise, are not a recipe for ongoing success.



The HPE NonStop PCI DSS compliance service can help you determine what you truly need to achieve and maintain compliance including how to use your existing security software to maximum effect. The service will help you achieve and maintain PCI DSS compliance in a practical way that takes into account your overall security requirements.

HPE NonStop PAN data discovery

Ensure that you know where all of your PAN data is located
One of the key aspects of a PCI DSS assessment is defining the scope of the cardholder data environment (CDE) for a QSA. Your PCI assessor would like to determine the locations where the primary account number (PAN) data are stored. The HPE NonStop PAN data discovery service provides an efficient and accurate way of achieving this.

Using automated PAN detection software, the system is scanned and any files or tables containing unencrypted or untokenized PAN data are identified and listed in PCI DSS compliance reports. The software identifies areas that you may know about such as the application database or transaction log files. It also locates areas you may not be aware of such as trace files, production data copied to test systems for problem troubleshooting, saveabend files, swap files and more. Without an automated PAN scanning tool, you cannot be certain that you really know where all cardholder data is located.

Make your HPE NonStop security the best it can be

Our security specialists will help keep your HPE NonStop systems secure and compliant.

System security is a never-ending story. Organizations must regularly review that what they have in place still satisfies their corporate and regulatory needs. From configuration to security reviews to PCI DSS, the HPE NonStop security and PCI DSS compliance suite of services will help you get your HPE NonStop security right.

Learn more at
hpe.com/info/nonstop

Our solution partner

Knightcraft Technology
Information Security Specialists

Sign up for updates

Hewlett Packard Enterprise

a00000623ENN, February 2017