Hewlett Packard
Enterprise

Business white paper

Enhanced IT security and reliability

HPE IT Support Services for modern IT infrastructure

Table of contents

As companies make the transition to modern IT infrastructure that supports the new digital economy, it becomes increasingly important to ensure the security and reliability of their IT infrastructures. Several market factors are driving the need for additional focus on, and investment in, IT infrastructure. However, the costs to address them, combined with constrained IT budgets, present a major challenge. Creative approaches to reducing these costs are required so businesses can invest in modern IT infrastructure.

IT focus and investment areas

24x7 infrastructure

Most organizations rely on the Internet as a primary vehicle for customer interaction, and markets are increasingly global. Therefore, the infrastructure on which e-commerce depends must run 24x7, and service interruptions equate to lost orders and revenue—not just for the outage period, but for the long term if existing customers or potential new clients take their business elsewhere. The more "9s" of uptime required, the greater the cost.

IT availability: what do uptime levels mean?

- 99% = 87 hours annual downtime
- 99.9% = 8.7 hours annual downtime
- 99.99% = 52 minutes annual downtime

Key issues

- Global markets, competition
- 24/7 apps
- Security becoming #1 concern
- IT funding needed for cloud, Big Data, mobility, security
- Constrained IT budgets

Increased cyber crime

In a study of cyber crime costs in 2015, Ponemon Institute estimated the average total cost of cyber crime to companies in the United States at $15.42 million, an increase of 21.4% over the previous year.[1] The costs to companies participating in the study ranged from $1.9 million to $65 million, and while there are variations based on company size and the types of cyberattacks experienced, it's clear that the expense is high and that it's increasing rapidly.

New data privacy laws

In 2014, USA Today reported that 43% of companies experienced a data breach in the past year.[2] This growing threat and the need to comply with data privacy laws are a very real part of the focus and daily activity of every IT department. While the initial loss of revenue due to cyber crime is typically high, the long-term cost of analysis, corrective action, customer indemnification and legal liability can exceed five times the original loss.

Reducing the cost of downtime

Hewlett Packard Enterprise continues to invest in ways to help our customers retool their enterprises to take advantage of cloud, Big Data, and mobility. HPE Technology Services is committed to helping offset the rising costs and increased risk to core infrastructure by reducing the cost of downtime—which also entails enhancing security and increasing reliability.

[1] Ponemon Institute "Cost of Cyber Crime" 2015 Study: sponsored by HPE Security.

[2] **USA Today**, citing a report conducted by the Ponemon Institute, September 24, 2014

Goals

- Enhance security
- Increase reliability
- Reduce cost

Strategy

- Secure code
- Closed-loop parts management
- Predictive failure intervention

There are four key areas that contribute significantly to lowering the overall cost of downtime.

Secure code

In 2010, a zero day virus named Stuxnet introduced a new level of sophistication by not only attacking the operating system, but also infecting programmable logic controllers. Hewlett Packard Enterprise has taken action to help reduce the impact of these much more invasive and destructive threats by implementing new security measures to eliminate the possibility of complex logic code being compromised through unauthorized access. Firmware and other logic updates now reside behind a secure firewall, and users must verify their access authorization by identifying an active warranty record or HPE-branded service covering their products. (Safety and security updates remain available for download without verification.) This increased security ensures that customers can access HPE-certified updates without having to worry about the validity of the source and expending resources, time, and effort verifying downloads.

Closed-loop component management

Original Hewlett Packard Enterprise parts are a key to maintaining a secure, reliable environment. As previously noted, many subsystems contain embedded firmware on the logic cards; thus, Hewlett Packard Enterprise's parts management process is specifically designed to apply the latest code and electronic revisions and fully certify the part as an HPE original part. To be certified, each item must pass a unique identification process designed to eliminate counterfeit or non-HPE parts. This increased focus on component management is providing assurance that our customers and partners have a parts pipeline that is more secure than ever.

Predictive failure intervention

Prevention is pivotal in the quest to reduce or eliminate downtime. Hewlett Packard Enterprise focuses heavily on predictive failure analysis through instrumentation. Proprietary HPE tools and diagnostics are available to customers through HPE warranty, Care Pack, and HPE-branded service contracts. Remote support technology and other tools are now instrumental in identifying and preventing problems before they occur and in troubleshooting problems when a failure does occur.

Engineering enhancements and expertise

The key to increasing reliability is continuous quality improvement. The Hewlett Packard Enterprise Parts Logistics organization uses a closed-loop, continuous-improvement process that begins by building a supply pipeline of genuine HPE parts, which are kept in stocking locations around the world. When parts are consumed, a functioning part is installed in the customer's device and the failed unit is returned for evaluation and possible repair. Failed units undergo rigorous failure analysis to determine root cause, and when possible, engineering updates (including the latest firmware) are applied. In cases when there is a potential for increased risk in a customer's IT environment, the field engineer may request that the part be tagged and processed for failure analysis and notification of the results. Only HPE-certified repair parts benefit from this comprehensive level of engineering enhancements. Unauthorized Service Providers do not always use genuine HPE repair parts. The parts they use may be at older hardware revision levels and older levels of firmware, introducing potential incompatibilities and increasing customer risk.

Software updates (including firmware revisions) are written and maintained by Hewlett Packard Enterprise engineering experts. Our unique position as the originator of the hardware device enables efficient detection of software vulnerability or inoperability issues through proven processes for data collection and problem solving. From the field to the factory, Hewlett Packard Enterprise's engineering teams analyze, improve, and deploy software updates to help ensure reliable and secure customer IT environments.

Why HPE

HPE is dedicated to providing the most secure, trusted repair parts and firmware and software updates. By recently refining these processes further, Hewlett Packard Enterprise is providing our customers with even more security and reducing the risk of downtime. HPE-branded support, with secure access to the latest firmware and HPE-certified parts, helps ensure optimum performance and increased protection of the IT infrastructure.

Hewlett Packard Enterprise has a strong partner network backed by the HPE Partner Ready Program. To maintain superior quality, authorized delivery partners use the same certification training, repair parts, and engineering network used by our internal support organization.

Hewlett Packard Enterprise also offers a simplified portfolio of flexible service offerings designed to meet the needs of the most demanding IT environments. Industry best practices are integrated in each of these services.

- Datacenter Care offers highly customizable support for large, complex data center environments.
- Proactive Care provides access to support and engineering experts, proactive reports and consultation.
- Foundation Care offers an array of hardware installation and support services.

Only Hewlett Packard Enterprise and HPE Partner Ready Service Delivery have access to the engineering expertise, security processes, certified parts, proprietary tools and diagnostics described above. That's why only HPE and HPE Partner Ready Service Delivery should support[3] your Hewlett Packard Enterprise equipment.

Learn more at
hpe.com/services/support

[3] Customer is entitled to proprietary HPE firmware updates and replacement parts for each HPE product via HPE warranty, HPE Care Pack, or HPE-branded support contract delivered by HPE Technology Services or an HPE Authorized ServiceOne Delivery Partner.

Sign up for updates

Hewlett Packard
Enterprise

4AA5-7704ENA, March 2017, Rev. 2