Hewlett Packard Enterprise

VMS Software

Objective
Update robust business OS with support for new and legacy hardware systems

Approach
Engage with HPE to obtain Integrity systems for test environment configurations to address any possible customer migration path

IT Matters
- Delivers decades of systems uptime for manufacturing, finance, governments

- Reduces security risk by up to 81x with a superior vulnerability profile

- Drives down system maintenance with 50x fewer software patches annually

Business Matters
- Lowers TCO by 25% over industry-leading enterprise OS vendors

- Saves approximately $30,000 per year, per system with reduced maintenance

- Extends the life of critical investments with proven upgrade path

VMS Software: Rebooting OpenVMS with HPE

Driving massive public and private organizations with an OS that was different from the start

A million every minute

Although technology trends like Big Data and Cloud are hot topics in IT circles these days, there are few concepts as compelling business continuity. It might not be a fashionable topic in the journals, but if your enterprise processes or manufactures on a massive scale, there's a very real possibility that downtime is costing you a million dollars every minute you can't do business.

When the idea of mission-critical systems first emerged, there were only a few big players in the operating system space, and VMS was one of the early leaders. Originally written by Digital Equipment Corporation in 1977, the OS offered high availability through clustering and the ability to distribute the system over multiple physical machines for disaster tolerance.

Over the years, the system was upgraded, renamed OpenVMS and ported to Alpha systems before the OS was acquired by HPE for its Intel Itanium-based Integrity Business Critical Systems.

Case study
VMS Software

Industry
Technology/Software
Development

Page 2

> "We've never thought of security as an add-on or an afterthought, and it shows—just by running OpenVMS on HPE hardware, you're reducing your security risk by between 61x and 81x due to the reduced number of OS vulnerabilities."
>
> — Eddie Orcutt, Vice President of Software Engineering, VMS Software, Inc.

Legendary performance

After all these years, the OS still has a stronghold among finance, government, and manufacturing giants. The reason? Legendary performance. There have been reports of enterprises experiencing in excess of 10 years of continuous uptime with OpenVMS. "It's not widely reported, but that level of availability, uptime, and security are why 90% of manufacturing today in Taiwan happens on HPE NonStop and OpenVMS," explains Eddie Orcutt, vice president of software engineering at VMS Software, Inc. "We have customers that are incredibly loyal to OpenVMS and have been for 38 years, so our job is to continue that business as far into the future as the need allows."

Today, VMS Software, Inc. finds itself playing a highly unlikely role in the technological universe: startup company. For the past few years the VMS Software team has been operating as an independent business, updating and improving its code and facing new challenges. "Many of our customers would like to continue running our OS on newer hardware, which for us is wonderful," Orcutt relates.

But the typical OpenVMS customer isn't the typical IT consumer. "Our customers tend to run higher spec hardware and run it for much longer—they're not on a 3-year refresh cycle," Orcutt explains.

What's old is new again

Even so, when systems remain static for long enough without the ability to upgrade or integrate popular open systems, customers can become antsy. "Before we launched as an independent company, we were facing an uncertain future," Orcutt recalls. "Our customers were wondering if they were ever going to be able to upgrade to the latest Integrity systems, and some of them were considering leaving the OS and the platform to go all in on x86."

It was a prospect OpenVMS customers didn't really want to undertake. "They would have to rewrite millions of lines of application code to make the migration," Orcutt says. "What they really wanted was an upgrade path for our OS that would carry their business well into the future."

Case study
VMS Software

Industry
Technology/Software
Development

Page 3

So Orcutt and team set out to deliver that solution to the market. One step at a time, the team began to qualify OpenVMS on newer versions of HPE Integrity Servers, eventually bringing the OS to its i2 and i4-based models.

The sentiment from the OpenVMS community changed almost overnight. "There was a real sense of excitement that our OS was moving into the future," Orcutt recalls. "Our customers were reassured that OpenVMS would run on the next version of their hardware, and the one after that."

Reliability reintroduced

To deliver its rock-solid OS to existing and new customers therefore presents its own challenges. "When we bought the code and launched VMS Software as a startup, we bought all iterations of the OS going back to versions that run on some pretty obscure hardware," Orcutt explains. "And even our newest version of the code requires specific hardware models which may not be in current production."

So VMS Software teamed up with HPE, the maker of business-critical Integrity Servers, and the one-time owner of the OpenVMS code. "We know who our customers are, and we know the kind of stability and availability they need to drive these massive enterprises," relates Sue Skonetski, vice president of customer advocacy at VMS Software. "So we approached HPE to get access to the systems we needed."

Modernizing migration paths

Through HPE, VMS Software can purchase and configure its own testing environments to make sure its OS delivers out in the field, no matter what hardware its customers are using. "We have customers who still run OpenVMS on VAX and want to migrate to Alpha, we have users who are on Alpha and need to migrate to Integrity, so we have to be able to support all of them," Skonetski explains.

Although VMS Software itself is not in the business of hardware, it will recommend certain server models and architectures to its customers. "It's a very close business relationship between VMS Software and HPE," Skonetski says. "Our customers buy a lot of hardware from HPE, and HPE sells OpenVMS."

Some of those customers are household names, such as a certain European furniture manufacturing giant, some operate entire federal governments, and some generate massive amounts of electricity for major metropolitan areas. Although its customers are often reluctant to be referenced due to security concerns, they are fiercely loyal.

Secure from the start

Security, it turns out, is another major reason customers stay with OpenVMS once they've discovered it. "From day one, security was programmed directly into the OpenVMS operating system," explains Orcutt. "We've never thought of security as an add-on or an afterthought, and it shows—just by running OpenVMS on HPE hardware, you're reducing your security risk by between 61x and 81x due to the reduced number of OS vulnerabilities."

Customer at a glance

Hardware

• HPE Integrity BL860 i2 Server Blades

• HPE Integrity BL860 i4 Server Blades

• HPE Integrity rx2800 i2 Server

• HPE Integrity rx2800 i4 Server

Software

• OpenVMS

On any given day, competitors' operating systems have anywhere between 3.7 and 4.5 vulnerabilities present compared to just .056 vulnerabilities in OpenVMS. The effort, hours, and cost it takes to patch those vulnerabilities presents its own business challenges for the enterprise. That translates into around 50 patching events per system for the dominant OS vendors' products vs. 1 patching event each year on OpenVMS. And the cost to perform those patches averages $30,000 per year per system on Microsoft Windows or Red Hat Linux-based servers, clients, and databases vs. just over a thousand dollars per year for OpenVMS.

Reducing TCO by 25%

"There are a couple ways to view the patching piece," Orcutt says. "You can spend the time to run test environments to see what the patches will actually do to your production environment, or you can patch and pray each time a new update is issued. If you spend the time to test, it's going to cost you more money each time you patch. If you 'patch and pray,' it's going to cost you more money when the patch does something unexpected to your business."

The same kinds of benefits hold true for operating and staffing costs. Over a typical five-year lifecycle, OpenVMS averages ownership costs of about $850,000 for 40 application servers and 10 database servers vs. more than $3.3 million for the same size environment on the market leading operating systems.

The future is open wide

"It's funny, because we hear constantly that Windows and Linux are cheaper because they run on x86 hardware," Orcutt says. "And that's true from an upfront purchase price standpoint, but when you look at the amount of money you need to spend to actually run your business on a given OS, you're going to spend a lot more on the Windows and Linux side."

That's not to say OpenVMS doesn't have its eye on the x86 platform. In fact, even with the massive amount of legacy hardware support it offers, the team sees great potential in emerging markets and bringing the OS to new platforms. "We're in the process of porting OpenVMS to Superdome X, at which point we'll support x86 in addition to all the modern and legacy Integrity systems."

Sometimes what's old is new again.

f 𝕏 in ✉

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise