



The IT Directors Perspective: Maximizing the Value of HPE NonStop



CONTENTS

Introduction 2

Unlocking data to turn it into knowledge 3

Aligning mature core applications with changing expectations 5

Web service enablement in four easy steps. 7

Security as a first class citizen 8

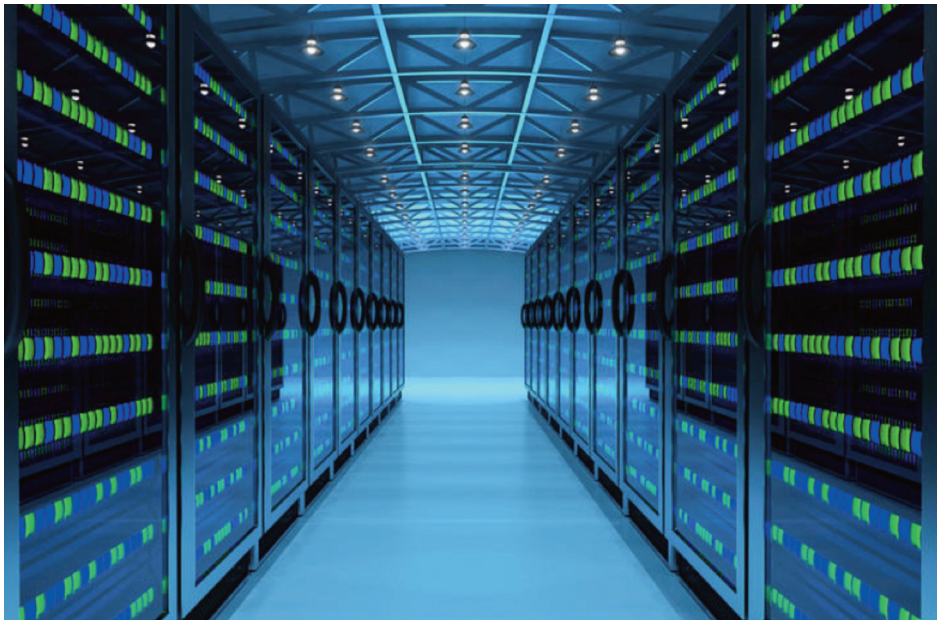
Achieving data protection with the innermost layer 10

Summary & Conclusion. 11

About the Author 12

Introduction

“You are traveling through another dimension, a dimension not only of sight and sound but of mind. A journey into a wondrous land whose boundaries are that of imagination.” Your next stop, the datacenter.



It is full of the latest and greatest technologies. Rows and rows of servers sit surrounded by flash disk arrays and enough fiber to reach to the moon and back. This is the new home for your software, the lifeblood of your company. You reflect proudly on what you have helped to create and then, doubt begins to cloud this wonderful vision. Is my software worthy of running on all of this shiny new technology? Can my software take advantage of all of these technologies? Is my software ready to run in the cloud?

Folks who run NonStop might take a slight pause while they ponder the cloud and wonder if they can fit their software into this new paradigm but upon reflection they will realize that Tandem was one of the first cloud providers. Back in 1976 they had envisioned applications being able to be run on independent CPUs with access to data hidden by a messaging system. You could add new hardware without having to change the application; if you needed more of a given resource you just added it. Sounds awfully like the definition of cloud computing, doesn't it?

CLOUD COMPUTING

The practice of storing regularly used computer data on multiple servers that can be accessed through the Internet –

Merriam-Webster

Unlocking data to turn it into knowledge

If you are reading this, you must be an IT professional. Information Technology, short and to the point, is two words: Information and Technology. The technology is the 'magic' that makes the information available to our users. Most users don't care about the technology, but the information they definitely do care about. Information is the life-blood of a company, without it the company cannot operate. There isn't a single major corporation that could survive if they suddenly lost all of their data. Data is one of the most important assets a company owns!

Providing access to our corporation's data has never been easier either. There are plenty of tools that allow our business partners to mine company data for the precious nuggets that will provide real value to our company unless (cough) that data is still stored in Enscribe files. It is the year 2017 and the last statistic about the NonStop customer base still has about 50% of the data stored on NonStop being stored in Enscribe files. Imagine the value that IT can provide to the company if they simply unlocked that data. Since IT organizations only exist to provide value to their company this should be at the top of everyone's wish list.

Enscribe is not a database, it is a set of files, most likely badly designed to save a few bytes on a disk. It has no tools to query it (NO! Enform isn't a user-friendly tool), to run what-if queries, to dynamically access it using whatever tools the user wants to use. Yet for some of us Enscribe is all we have. There are a few ways to deal with this Enscribe data: 1) Ignore it and pray it goes away 2) Throw it over the wall to the person in the next office 3) Nuke it all and start from scratch 4) Pick them off one-by-one. Option 1 is what most people seem to be doing, option 2 is great if you're not the guy in the next office, option 3 never works as the amount of risk vs. reward is too high, which leaves us with option 4 where we pick each file off one-by-one, sometimes referred to as the Tony Romo method. Option 4 is the best way to approach the task as you get immediate results with very little risk to your production environment.



DATA BECOMES KNOWLEDGE

There are hundreds of examples where 'random' bytes sitting on a computer's mass storage device have provided real, actionable information to corporations. One that comes to mind as the United States enters hurricane season is the ability to visualize a company's supply chain to see best how to deploy their assets to help the folks impacted by a hurricane.

Imagine a map of the US with all of the company's assets shown on it along with the path of the hurricane. The company had the data but it wasn't accessible to folks who needed it when it was locked in an Enscribe file, by moving it to a SQL database they were able to load it into a piece of software they purchased from a 3rd party. Once loaded it turned into a valuable tool.

Unlocking data to turn it into knowledge


It is relatively easy to convert Enscribe files to a modern SQL database using a tool such as comforte's Escort SQL; this incredible software product converts Enscribe applications and files to NonStop SQL without requiring any changes to existing programs (i.e. no source code changes). This allows an organization to focus on creating new applications that provide the business with new capabilities instead of spending time rewriting existing functionality.

According to Gartner, cloud computing has been among the top technology trends for six consecutive years. Cloud computing continues to experience major growth as companies of all sizes embrace it to reap the benefits of scalable, cost-saving applications

Many companies have used Escort to transform their Enscribe files, which were a mess, into eloquent SQL databases. Most Enscribe environments were designed, in what was typical for the time, as a single file that was then redefined depending upon different values stored in the record. In the late 1980s and early 1990s when the application was built, this was considered state of the art but it quickly became a problem when trying to build modern components. By using the Escort product, they are able to focus on the real task, which is to provide new functions to the business.

The conversion process couldn't be any easier and can be described as a two-phase process. First, the SQL database is designed. The Escort utility provides the user with the ability to convert the Enscribe files into normalized SQL tables. A single Enscribe file can be mapped to an unlimited number of SQL tables and data fields can be expanded, added, or eliminated. Once the database has been architected, the Escort utility creates the new SQL database and loads it using an ultra-quick parallel loader.

In phase two the application object files are 'prepared' using a provided utility to use the new SQL database. In this stage, a provided library is linked to your existing object. Once this has been done, your programs will now access the new SQL database using the existing Enscribe I/O calls.



Instead of developers spending their time writing reports they will be able to develop new functions and features. Hiring will be easier as most folks don't graduate from university knowing Enscribe and probably have no interest in learning it. And, perhaps most importantly, other groups will be able to access the data using industry standard techniques which has immense value for the company, adding a web front-end will take days instead of months.

Unlocking data to turn it into knowledge

That's it! Nothing else is required! From this point forward, your data is now housed in one of the best SQL databases in the industry and the developers can begin to build new applications that utilize SQL verbs (Select, Insert, Delete, ...) that co-exist with the existing applications that are using Enscribe calls (Read, Write, Writeread, Readupdate, ...).

Additionally, tools such as JDBC/ODBC, Tableau and QLIK can be used by the entire organization to access the previously unavailable data. You can also take advantage of all of the great features of the NonStop SQL engine including the ability to generate test data automatically.

Once you have converted your files to tables you have taken the first step on your journey towards the cloud. The next logical step is to start working on a strategy to move your applications and data into the cloud.



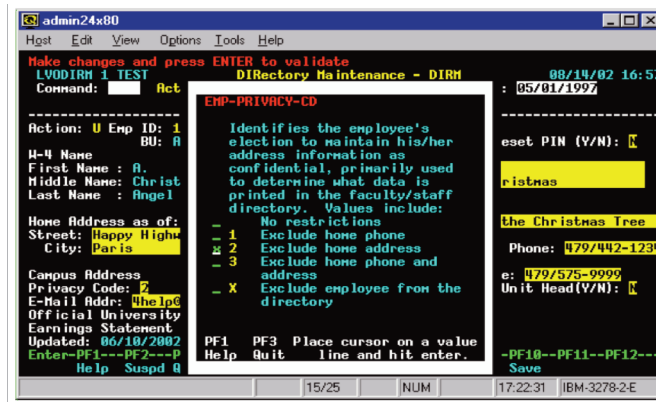
Aligning mature core applications with changing expectations

As 2017 begins to wind down most companies have a cloud strategy in place. All of the new features they produce are cloud native or at least cloud accessible. They have multiple offerings that their customers can access via the Internet, which allows them to be more competitive. Additionally, they are exploring the way to move more of their compute power into the cloud to allow them to focus on providing more features to their business partners. It's a great time to be an IT professional!

Aligning mature core applications with changing expectations

As you sit back and ponder the journey you, and your applications, have taken over the last few years you still get a bit uncomfortable when you think about your dreaded legacy application. It still provides lots of value to the company but most of that value is hidden behind legacy interfaces. Go to an airport and watch the gate crew change a seat assignment and you can't help but cringe as you notice them hitting the tab key 10 times in a row to move to the seat you would like using a terminal emulator that 'speaks' 3270. When you rent a car, you notice that the screen the agent is using is just a GUI slapped on an old green screen. Visit your financial advisor and I'll bet you'll notice the same thing.

Some people will tell you that the use of green screens is fine, that they'd rather build new features instead of rewriting them to use modern technologies – that they can't justify the expense of rewriting them. Of course, these people would be wrong, dead wrong!



A Typical Green Screen

Green screens aren't intuitive, meaning that companies spend a lot of money each year training folks on how to use them. In industries such as retail where the average turnover is 50% per year, training adds up quickly. If it takes a week to train a cashier and you have 100,000 cashiers that means you need to train 50,000 cashiers per year – without factoring in seasonal labor, which could double that number. That is 2,000,000 hours of paid time these new employees aren't being productive in and it doesn't even factor in the time of the folks that are working with them. At \$12 per hour that is \$24,000,000 a year that is wasted. Put that same person onto a modern interface and the training time drops to a single day since they will know how to use it. That is a savings of more than \$19,000,000 per year. The travel industry has the same economics. Now let's talk about how a CIO can't justify the money to rewrite them...

Web service enablement in four easy steps



As in all discussions of modernization, there are always numerous ways to do things. The best way is to use a tool that can leverage the existing data model so a company doesn't have to change the back-end immediately. This is probably the quickest path to getting something into production. During this phase, the software engineers should be working hand-in-hand with the user experience (UX) and business teams to ensure that the new system meets the needs of the users. Using a tool such as comForte's CSL, an existing Pathway server can easily be exposed as a REST or SOAP service. This allows the company to leverage the unparalleled reliability and scalability of their Non-Stop while exposing these services to new consumers without having to rewrite the application. Clients can be written in any language and run on any platform. CSL also provides the application with TLS security to ensure that your data stays private.

To create a RESTful or SOAP service using CSL Studio requires only four steps:

- 1. Import the applications DDLs**
- 2. Import the Pathway definitions**
- 3. Generate the REST wrappers and Doco or the SOAP WSDL**
- 4. Deploy the service to the NonStop**

All told, in about 15 minutes, a legacy Pathway server can be exposed as a running web service!

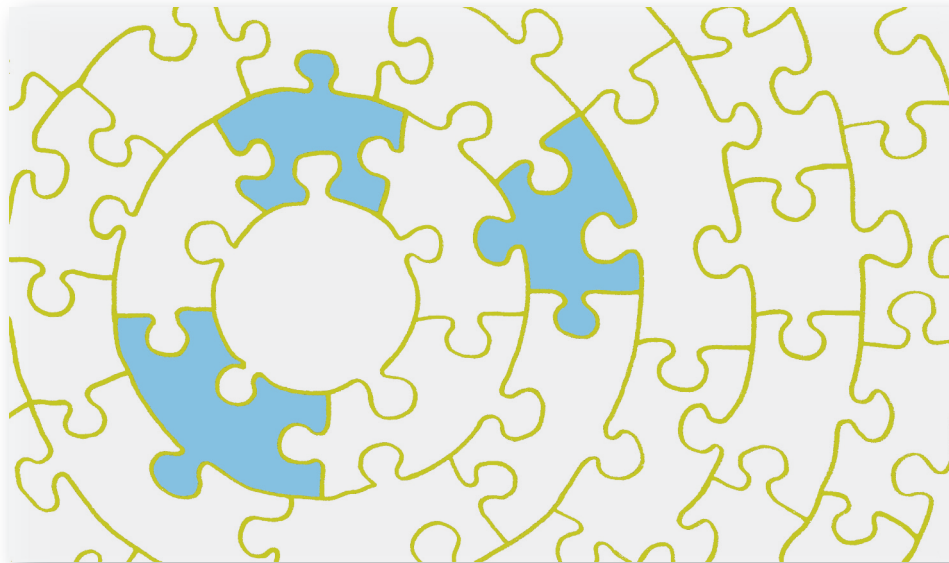
Web-enabling legacy applications isn't just for the replacement of green screens; any running Pathway service can be exposed in this manner. Once an enterprise's legacy services have been exposed one can argue that they are no longer legacy. The ROI for a tool such as CSL is amazing, no longer are company assets hidden behind a proprietary set of solutions, now third-party applications can be purchased that can access these services and create new, more powerful services. Creating a new feature can be as simple as writing a small workflow to call a few services in a totally new way. Testing can be automated using 3rd party tools. Running a stress test is as simple as pressing a button on an open source tool that is designed to generate data and send it to a web service.

Once a company has exposed their back-end services, they should start thinking about using the new Virtual NonStop capabilities. Imagine a world where a complete service can be deployed to an end-point location to ensure that it is always available. If the remote location goes offline it can still continue to operate without any impact to the users! Once a company moves into the virtual world the possibilities are virtually limitless. As a company's transaction rate increases the system would automatically expand to handle it without any user intervention. Gone forever are the days of buying enough hardware to handle the peak season and watching as it sits unused for 11 months out of the year.

Web service enablement in four easy steps



By using the Escort product, an Enterprise can make their data available via one of the best SQL engines, NonStop SQL. And with their applications being exposed using CSL, a company now has all of the building blocks to provide immense value for years to come. The last piece of the puzzle is to make sure that all of the IT assets are fully secured as no discussion of modernization can ignore such an important topic.



Security as a first-class citizen

Security, like everything else in IT, is a very straightforward topic; either you are secure or you are not. Lots of companies think that if they build a good perimeter defense (firewalls, VPNs, intrusion detection, etc.) that they are safe, but this couldn't be further from the truth. Defense only works when it is done in depth!

Security as a first-class citizen



Defense in depth is not a fancy new security concept; it dates back to medieval times. Back then, buildings were constructed to present as daunting a challenge to attackers as possible. They would be surrounded by water, or built on a hill, have a central enclosure of stone walls, and towers where people would watch for attacks, then one or more outer walls, also with towers. The height of the walls would increase towards the middle, enabling inner defenders to shoot over the defenders of the outer walls. Back then, when a breach occurred people died.

Luckily, today people don't die when a breach occurs, but the reputation of the company along with the trust they have built with their customers does. To prevent a catastrophic event like a breach from happening, IT organizations need to layer their security. Folks like to use an onion to describe good security: as you peel back the layers there is another one protecting the center. I typically separate good security into seven layers:

- 1) Well-defined policies and procedures that are understood by everyone in the organization. Things like data classifications, password strength, code reviews and usage policies
- 2) Physical security such as locks, ID badges, walls, and guards
- 3) Perimeters built with firewalls, denial of service prevention, network address translations, and message validation services
- 4) Network protection using encryption and identification services
- 5) Server and desktop protection via patching and malware detection
- 6) Application authentication, authorization, auditing, and secure coding practices including single sign on

Achieving data protection with the innermost layer

Layer seven; the innermost layer that protects the sensitive data that the 'bad guys' want has two very good standards to use when deciding what and how to do things. Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA). Both of these standards are constantly reviewed and enhanced to ensure that private data stays private. There are a few techniques that all organizations employ to protect their data. First, ensure that all (not some) communication is via a secure communications protocol such as TLS. If the attackers can read your communications, they can learn things that will help them attack your infrastructure such as a user name, password, or the address of a service. It should go without saying that the use of telnet and FTP should be banned (good security practices state they should be removed from the system). There is no reason for any communications to be in the clear. Second, all of the data should be encrypted or tokenized. Most security professionals agree that an organization should tokenize the super sensitive data (PII) and then encrypt it when it is in motion or at rest.

Adding TLS to an application is simple so there is no reason not to do it!

Of course, encryption has many flavors; it is recommended that all physical media have encryption turned on, which ensures that if a disk or tape is stolen, the data on it is useless. All modern operating systems have the ability to encrypt a disk or tape built-in. Encrypting all communications is pretty easy, all browsers support TLS 1.2, which should be used by anything using a web-like interface. ComForte's SSL-AT provides transparent TLS security to any application via an intercept library meaning that no application modification is required. Adding TLS to an application is simple so there is no reason not to do it. For those who want to have total control over their application, comforte has another product, SecurLib/SSL, which provides developers with complete control of their TLS implementation via simple to use APIs.

Tokenization is the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data.

Once you have enabled encryption on all of your communications and storage devices it is time to encrypt or tokenize your sensitive data (social security number, driver's license number, credit card number, PINs, bank account information, etc.). The approach most companies take is to encrypt or tokenize the data when it is written to a storage device. With tokenization, the sensitive data is replaced with a token, while with encryption the data is encoded and locked with an encryption key. In either case if the data is stolen it has no exploitable value.

Data security is no longer optional, bad actors are working 24/7 to hack into your systems. No matter how good you and your security team are, sooner or later one small mistake such as a missed patch of an obscure server and they are in. If your data is encrypted when in motion, and tokenized or encrypted when at rest, you have nothing to be concerned about.

Summary & Conclusion

As technologies advance and user expectations change, the NonStop platform must adapt. Just reliably supporting some of the most critical business functions in organizations worldwide is not quite enough anymore. Applications on the NonStop need to be seamlessly embedded into modern architectures and offer a modern user experience. At the same time, data security has to be treated as a first-class citizen, because of the additional exposure of business functions and data on the NonStop to other applications.

Therefore, there are three main elements to consider:

- Unlocking data by converting Enscribe files to SQL
- Unlocking business functions with web service enablement
- Securing sensitive data with tokenization or encryption

This might seem like a daunting task, but with the right partner at your side, you can unlock the full potential of your NonStop while minimizing effort and risk. comforte is a leading global provider of data security, connectivity, and application modernization solutions. comforte delivers best-in-class products and support for customers using HPE NonStop systems.

Building on over 30 years of experience on HPE NonStop systems, the strong bond between comforte and HPE began with a technology partnership in 2004, which eventually led to the inclusion of comforte-designed communication solutions in the NonStop operating system. Hundreds of organizations around the world, running mission critical applications, rely on comforte solutions every day to ensure their sensitive data is protected from possible data breaches, their data communications are secure, and their applications are easily accessible through modernization.

With a wide range of innovative and proven products, comforte solutions ensure customers gain immediate value from their investment, eliminate or reduce the need for additional software development costs, and experience as little downtime as possible. We are here to enable your success by providing expertise, an innovative technology suite and local support. To learn more, talk to your comforte representative today and visit www.comforte.com.



About the Author

Marty Edelman has been involved in the IT field for more than 30 years. As an independent consultant, he founded a small consultancy firm that specialized in developing high-volume mission-critical solutions for Fortune 500 companies. He and his team built the UPS Tracking System, the NYSE Consolidated Trade and Quote systems, and the S.W.I.F.T. next-generation computing platform.

While at The Home Depot, the world's leading home improvement retailer, he was the leader of the interconnected payments team and helped to introduce modern software development practices to the IT team which produces software used by over 300,000 associates and millions of customers. Furthermore, Marty was responsible for all aspects of payment processing (credit, debit, gift card, check, and PayPal) and accountable for ensuring that the organization's payment infrastructure was fully PCI compliant and secure.

