Making Sure that Your Data Centre Provider’s Foundations are Green
Free Migrations Break the Stalemate Between Inertia and Modernization
SD-WAN: As Simple or as Complex as Needed
Case Study: Fileturn – streamlining the accounts process
Delivering Evidence from the Dark Web when Data Breaches Go to Court

Use Existing Banking Technology for API-led Strategies to Attract fintechs
Use Existing Banking Technology for API-led Strategies to Attract fintechs

Banks can adopt several strategies when working with fintechs. Those most commonly discussed range from programmes to instill an entrepreneurial agile culture within banks, building and engaging extensively with developer communities, and building internal developer capacity. In this article the author will look at three key areas on how banks can capitalize more on the API technology layer and support the open banking technology infrastructure they have already invested in to attract and fast-track collaboration with fintechs. Adopting such approaches will help banks establish stronger differentiators to ensure that the best developers and most promising third-party service providers (TPPs) will work with them. Similarly, these approaches can also help attract partnerships with other banks with complementary goals.

In Data Centre and Virtualization ...

Making Sure that Your Data Centre Provider’s Foundations are Green

The data centre industry continues to grow rapidly as more of our lives become digitally led. But, whilst digital technology is powering, some say revolutionizing, the way we work and live, the millions of data centres which store and process the digital data we create are purging metric tons of hardware, draining country-sized amounts of electricity, and generating carbon emissions as big as the global airline industry. In this article, the author explains that there are many shades of ‘green’ in the data centre industry and why it is more important than ever to ensure that your data centre provider’s foundations are in fact green.
Editorial

The future is bright – the light of hope is shining ahead for all of us
As we move forward into 2021 – despite the latest lockdowns we are all facing – we have a chance to take with us the new working practices developed last year, honing them even further to create our new agile working practices for the future.

RESEARCH PAPERS

Technology and Innovation

Use Existing Banking Technology for API-led Strategies to Attract fintechs
Vidura Gamini Abhaya, Senior Director – Solutions Architecture, WSO2
Creating an agile culture within banks to engage with developer communities and build internal developer capacity is not easy. But there are three key areas on how banks can capitalize more on the API technology layer and support the open banking technology infrastructure they have already invested in to attract and fast-track collaboration with fintechs.
Keywords: Financial Services, API, Open Banking, Authentication, Enterprise integration, Ecosystems, Technology infrastructure

Free Migrations Break the Stalemate Between Inertia and Modernization
Stanley Zaffos, Senior Vice President of Product Marketing, Infinidat
Data migrations are a lot like a toothache. You can delay going to the dentist for a while, but eventually, you are going. The desire to postpone data migrations is understandable. Migrations consume scarce staff resources; they are time-consuming, create financial and operational risks, and complicate vendor relations.
Keywords: (Data storage, Hybrid cloud, Data migrations, Service Level Agreements (SLA), Cloud storage

E-KYC in the Era of Rising Digital Crime
James Roche, Senior Consultant for Authentication, Identity and Scams, FICO
Compliance teams face huge challenges in balancing KYC with customer satisfaction when consumers move their financial lives online. Digital on-boarding is often impeded by regulations, legacy systems and a disjointed approach to customer due diligence (CDD) in app environments.
Keywords: Electronic Know Your Customer (e-KYC), Anti-money laundering (AML), Identity validation, Identity verification, Authentication

Data Centre and Virtualization

Making Sure that Your Data Centre Provider’s Foundations are Green
David Watkins, Solutions Director, VIRTUS Data Centres
The data centre industry continues to grow rapidly as more of our lives become digitally led. But, whilst digital technology is powering, the millions of data centres which store and process the digital data we create are purging metric tons of hardware, draining country-sized amounts of electricity, and generating carbon emissions it is more important than ever to ensure that your data centre provider’s foundations are in fact green.
Keywords: Data centre, Sustainability, Digital transformation, Carbon emissions, Green energy, Efficiency
IT Security

31 Modern Bank Heist: From Smash and Grab to Hostage Situation as Cyberthieves Evolve  
Tom Kellerman, Chief Cybersecurity Officer, VMware Carbon Black  
Modern cybercriminals are evolving and new tactics, techniques and procedures (TTPs) are emerging, so defenders need to keep pace. The financial sector is not a new target for criminals, the bank heist has evolved significantly over the years – from stickups to cyberspace – but the fundamental motivation behind the attacks has remained the same: money.  
Keywords: Cybersecurity, Endpoint protection, Financial services, Cloud-native, Security, Cyberattacks  

35 Expert Witness: Delivering Evidence from the Dark Web when Data Breaches Go to Court  
Austin Berglas, Global Head of Professional Services, BlueVoyant  
With personal data being easily purchased from the dark web. Many criminals are undertaking this data to commit identity theft but BlueVoyant professionals can evaluate and explain to courts how personal data is sourced by cybercriminals and used to commit fraud. In this article the author discusses how the impact of stolen data can become a legal issue in terms of class action lawsuits.  
Keywords: Cybersecurity, Data breach, Risk, Expert witness, Legal, Personally Identifiable Information (PII)

In Conversation with ...

39 In Conversation with Eric Newcomer  
We talk to Eric Newcomer, the new Chief Technology Officer at WSO2 about his new role and why he has such a forward-thinking approach to life.

Case Studies

45 Case Studies – Introduction

46 Fileturn – streamlining the accounts process  
YourDMS

48 Café Zupas Extends WatchGuard Simplicity and Protection from the Network to the Endpoint  
WatchGuard Technologies

50 MM Manufacturing – eliminating the waiting game  
Taulia
The future is bright – the light of hope is shining ahead for all of us

Happy New Year, and here’s to a healthier New Year for us all.

What a horrendous year 2020 was, but as vaccines continue to be developed and rolled out there is the ray of hope shining bright at the end of the tunnel.

As we move forward into 2021 – despite the latest lockdowns we are all facing – we have a chance to take with us the new working practices developed last year, honing them even further to create our new agile working practices for the future.

For many, COVID-19 has become the catalyst propelling business digital transformation. Technology is making it possible for more people to work from home (WFH) than ever before.

As organizations reimagine their work and the role of the office in creating safe and productive jobs where collaboration between employees was easy given the densification, open-office designs, research by McKinsey reveals that adoption of new working practices developed with WFH is proving both productive and highly collaborative for employees.

During the pandemic, many were surprised by how quickly and effectively technologies for videoconferencing and other forms of digital collaboration were adopted – and for many, McKinsey say, the results have been better than anyone could have imagined.

In the McKinsey research, over 40% report that they are as productive, or more productive WFH compared to working in an office, and 80% say they feel that being liberated from long travel journeys gives them greater flexibility in balancing their personal and professional lives.

In addition, WFH has given many organizations access to new pools of talent, allowing them to adopt innovation processes to boost productivity, building their corporate culture without the constraints normally associated with locational and property costs.
While technology is seen as a key enabler in achieving this, it is still going to take a mindset shift to ensure that teams can work effectively together in a seamless manner regardless of where they are located.

Leadership of course is paramount. The COVID-19 crisis has reminded business leaders that it is the capabilities and mindsets of an organization’s workforce which provide the foundation for creating more resilient companies.

The rise of online learning is set to revolutionize upskilling the workforce. In the virtual world, online learning using real business problems or competitive simulations can continue to operate as they would do in-person environments. Not only will this build staff learning, but it will also achieve the behavioural change that comes from the day-to-day application of new learning and skills helping to create a more productive workforce.

Tuning in to webinars and virtual conferences it is heart-warming to watch suppliers, analysts, consultants, trainers, academics and industry experts pulling together to tackle new challenges, sharing advice and information, and creating an inspiring ethos which we can all adopt.

Of course, it is more vital than ever to track performance and wellbeing, adjusting learning so that employees can gather and deploy the right skills. This will enable staff, managers and leaders to maintain focus, build productivity and nourish resilience over the next few weeks and months as businesses adapt to the new ‘norm’, challenges of new markets, and new processes associated with leaving the European Union.

As I look ahead optimistically to 2021, we all have the chance to be more knowledgeable and better organized.

Journeying together we walk alongside you helping to build the skillsets, mindsets and resilience you need to reenergize your employees and create the agile organization of the future – now let’s enjoy that bright journey together.
Use Existing Banking Technology for API-led Strategies to Attract fintechs
Vidura Gamini Abhaya

Abstract
Banks can adopt several strategies when working with fintechs. Those most commonly discussed range from programmes to instill an entrepreneurial agile culture within banks, building and engaging extensively with developer communities, and building internal developer capacity. In this article the author will look at three key areas on how banks can capitalize more on the API technology layer and support the open banking technology infrastructure they have already invested in to attract and fast-track collaboration with fintechs. Adopting such approaches will help banks establish stronger differentiators to ensure that the best developers and most promising third-party service providers (TPPs) will work with them. Similarly, these approaches can also help attract partnerships with other banks with complementary goals.

Introduction – The power of collaboration and proactive differentiation
Many banks are looking to collaborate more proactively with fintechs who possess the consumer-centric, agile culture required to rapidly prototype and bring to market innovative new solutions that deliver value to today’s savvy consumers.
Putting regulatory compliance to one side, banks are starting to buy into the necessity for genuinely “doing open banking”. Yet strategies to capitalize on already available technology to achieve this doesn’t receive the same attention as operational and community engagement. Open banking APIs enable the secure sharing of customer data (with customer consent), and consumer products built around this will soon become the norm as seen with the popularity of open banking-based credit alternatives like Creditspring and personal finance management apps like Cleo.

In every regulated open banking ecosystem, all banks will eventually have the same mandated APIs. Even in non-regulated countries, market forces mean that most banks will end up using open banking-style standardized APIs. However, standard open banking APIs will not really benefit the bank in the long run because they only deliver minimal benefits for consumers and third-party providers (TPPs).

So, how can banks look to benefit more from this new ecosystem with their existing technology capabilities?

**Ensuring fintechs do less when they work with you**
With open banking, banks have the capability to share, receive, and produce data using the same interfaces. For instance, a bank may already have a credit scoring system internally. With the API aggregation capabilities of their open banking platform, the bank can now receive and make use of account, transaction, and credit data from other banks as inputs to fine-tune and produce more accurate outputs using their own credit scoring system.

Third parties developing either B2B or B2C apps for providing consumers new avenues to access personal loans, property rentals, long-term vehicle hires, and leasing services would find this data extremely useful. Previously, their developers
would have to collect, correlate and calculate creditworthiness by themselves. Even where credit scoring is done by a third-party service, this still requires additional work such as collating the information and integrating with another system to submit this information and obtain the credit score. Passing data to different systems requires app developers to follow additional security practices, privacy regulations, and other regulatory requirements. All this is time-consuming and expensive.

Now, developers can access highly refined credit ratings via a simple one-time API integration, delivering considerable savings and much faster time-to-market. Offering such APIs would help the bank to differentiate and build long-term strategic relationships with TPPs.

While the bank can make this API available for free to all users, it will need to be enforced with rate-limiting policies to ensure fair usage. A premium monetized version of the same API can also be made available.

From a technical perspective, the bank can use an integration product such as an enterprise service bus (ESB) to integrate with other banks, for example, to share and view accounts and payment information and credit scores.

Providing higher-quality enriched data
Aside from mandatory information being made available under regulated open banking APIs, banks can enrich the data offered and monetize it through additional APIs. This enrichment can be achieved by using additional information from other internal systems at the bank, or by collaborating with external services.

For example, a bank could integrate with an external service that uses AI and natural language processing (NLP) techniques to calculate credit scores. The bank submits information to this service and the processed output provided by the
service is used by the bank in its own credit-worthiness checks. This is an
enrichment to the bank’s own credit check and this data can be shared with
external app developers through a monetized premium API. The bank can create a
new API product through which consumers could obtain standard credit scores as
well as the AI-enriched credit scores. Usage of this new API can be monetized and
charged back to the consumer per usage or absorbed by the third-party developer.

Taking open banking functionality to other industries “as-a-service”
The new technical capabilities banks acquire as part of an open banking platform
could be provided “as a service” to organizations that do not want to invest heavily
in deploying, maintaining, and updating such systems.

An example is strong customer authentication capabilities and consumer consent
management. Banks can extend these capabilities as a service to third-party app
developers who can integrate with the bank’s identity and access management
service for authentication and pay per number of users. Customers, including
incumbent businesses and startups, benefit from not having to invest in a product
and maintaining it on their own and by the knock-on effect of the trust consumers
already place in the bank’s brand.

Similarly, together with authentication features, consent management could be
used by businesses where they require customer consent to share information with
third parties. Hypothetically, a medical clinic with customer medical records in
partnership with an insurance provider could use consent management features
offered as a service by a bank to share those records, subject to consumer consent,
with the insurance provider. The consent management system at the bank would
only need to maintain an identifier to the customer record at the medical clinic (data
holder) and a reference to the insurance policy (data recipient). The bank’s system
does not need to store any personally identifiable information about the customer
giving consent. The insurance app needs to redirect to the bank’s consent
management system when it requires to grab consent and verify from the user, just
as with open banking scenarios. This service would come inbuilt with the same
consent management flows that allow consumers to manage their consent
preferences.

In conclusion
I have outlined three API-led strategies that deliver value to consumers by utilizing
existing capabilities of open banking solutions. These strategies are set against the
reality that APIs are already a baseline requirement in banking. To stand out,
proactive experimentation and building the technical capabilities along with the right
partnerships are core elements for delivering personalized and timely value to
consumers, which in turn builds a bank’s competitive growth strategy in today’s fast-
paced digital world.
Free Migrations Break the Stalemate Between Inertia and Modernization
Stanley Zaffos

Abstract
Data migrations are a lot like a toothache. You can delay going to the dentist for a while, but eventually, you are going. The desire to postpone data migrations is understandable. Migrations consume scarce staff resources; they are time-consuming, create financial and operational risks, and complicate vendor relations. As the author of this article explains, it’s why Infinidat offers free data migrations for new customers done by experienced teams of professionals equipped with procedures, automation, and tools that transparently move data onto InfiniBox systems and guarantees regarding performance and schedule.

Introduction
Free migrations are the easiest and safest way to bound the risks and costs of changing storage vendors. Requiring the vendors bidding for your storage business to include the data migration effort enables “like for like” comparisons between incumbent and nonincumbent vendor bids.

Outsourcing to the storage vendors also provides insight into the vendors’ internal skills and ease of use — if the bids are transparent. Transparency is critical because it makes it difficult for vendors to move money between hardware, software, maintenance, and consulting services that distort ease of use perceptions.
Why are data migrations painful?
Data migrations are inherently complex, and when poorly done, affect the ability of IT to meet Service Level Agreements (SLAs). They touch backup/recovery, Disaster Recovery (DR) schemes, business continuity plans, policies procedures, and asset/vendor management.

Ironically, if IT meets its service level objectives, the best that infrastructure and operations (I&O) Leaders can hope for is that data migrations complete on schedule and don’t create operational problems.

If SLAs are not being met, these leaders face additional scheduling pressure because customers want their problems fixed asap. With the dangers of migrations understood (or experienced), the minimal set of prerequisites to successful data migrations are creating comprehensive planning, testing, implementing, and validating that data migrations were successful. Migrations can be resource-intensive, time-consuming, and risky to other SLAs such as performance and availability.

Of interest to senior management are: Did it solve the problem? How much did it cost? Did the migration complete on time? With more immediate risk than upside, migrations are a pain!

Why does Infinidat offer free data migrations to new customers?
In many sales situations our biggest competitor is inertia, and we are very good at doing seamless migrations. Removing or mitigating the costs and risks of data migrations makes it easier for prospects to put us on their shortlist and it takes away the biggest excuse or reason for doing nothing.

So, for Infinidat getting on a prospects shortlist is a strategic imperative because it often leads to I&O leaders assessing their satisfaction with existing storage solutions: something we encourage because, in competitive situations, we mostly win.

Free migrations, or even their discussion, provides Infinidat with an opportunity to showcase our deep technical competency and InfiniBox’s performance, ease of use, and desirability as a consolidation platform. It also allows us to build relationships with prospective new customers and insights into their workloads.
Free migrations enable IT organizations with skills shortages, no recent migration experience, or limited budgets to augment their staff at no cost and benefit from working with teams experienced in doing data migrations. These benefits extend beyond meeting migration schedules to include skills transfers and visibility into the methodologies and automation and migration tools. New customers consolidating their storage infrastructures also benefit from InfiniBox’s higher availability and simplified D/R schemes.

**How can Infinidat afford to offer new customers free migrations?**

Infinidat can offer free data migrations to new customers because we have driven much of the cost out of migrating onto InfiniBox. The cost reductions derive from InfiniBox Neural Cache algorithms and robust local and remote replication facilities, our selling large storage systems, and an experienced, competent staff equipped with the tools it needs to provide a consistent migration experience.
Another consideration is the success of our customers. Since most of our customers do significant upgrades within two years of becoming Infinidat customers, and our primary business is selling storage solutions, migrations only have to pay for themselves.

**What are the “gotchas”?**
The initial purchase and/or forecasted growth rates have to be large enough to justify committing a migration team to the project. The good news is that driving down the cost of the migrating data onto InfiniBox systems lowers the threshold of deal size acceptability, and it does not take a lot of effort to get a yeah or nay answer from an account team.

Another is that the organization has to commit staff resources to work with their Infinidat migration team. However, compared to taking on the migration project alone, free migrations increase the probability of success, shrink the inhouse resources needed by augmenting in-house skills, and shorten the calendar time required to complete the project.

**Let’s talk**
Infinidat’s success in the most competitive segment of the storage market, Fortune 2000 accounts; our creating a multi-PB storage solution with unbeatable ease of use, sub-msec response times, and an extensive ecosystem, superb support, and disruptively better economics are matters of the historical record. Now with free migrations, what do you have to lose? If you can’t answer that question or if this article has raised unanswered questions, it is time to talk with Infinidat.
E-KYC in the Era of Rising Digital Crime
James Roche

Abstract

Even before COVID-19, the risks of online fraud were being highlighted by industry professionals. Earlier this year Cifas, the UK’s fraud prevention service, reported that in 2019 over 364,000 cases were recorded to its database – the highest ever recorded. Online retail saw one of the most significant rises in cases – with a 100% increase. Technology was identified as playing a key role in facilitating fraudulent conduct, with 87% of identity fraud in 2019 occurring through online channels. And in a separate study by Cifas, three quarters of fraud prevention professionals said COVID-19 will have a ‘significant’ impact on fraud, and more than 90% warned of fraud spikes in 2020 and 2021.

Against this backdrop compliance teams face huge challenges in balancing KYC with customer satisfaction. When consumers move their financial lives online, they expect a simple streamlined process and less paperwork. Digital on-boarding is, however, impeded by regulations, legacy systems and a disjointed approach to customer due diligence (CDD), also known as KYC in online or in-app environments. In this article, the author examines how compliance teams can adapt for a digital environment.

Introduction

The regulations say customers need to prove their identity online using official documents and authoritative data records. Customer Due Diligence (CDD) / Know Your Customer (KYC) also asks a provider to understand the affairs of the applicant to a sufficient degree in order to set expectations for how they will make use of a
service, especially a financial one. At each stage of the process, the applicant wants to know that the business values them and their time, and that their personal information is safe. This is likely to frustrate existing customers who would have previously been asked for and provided this information, and many may find the need to confirm details throughout the process tiresome.

There are, however, serious concerns associated with removing all friction. If a fraudster can take over an account and apply for a product without all the necessary checks, the real customer may be harmed. If lax KYC processes allow money laundering to occur, the bank can face massive fines and loss of reputation. Therefore, having some customer friction in the process can bring a positive benefit: awareness that security is going on behind the scenes provides customers with peace of mind.

**Compliance can alleviate costs**

The choice of identity verification solution often lies with those tasked with providing excellent customer service. Customers are directly involved with proving their identity, making it vital that this process is not so difficult or time-consuming that they abandon their application. That said, if the identity proofing put in place is not adequate to meet the regulatory requirements for KYC, then customer friction downstream is inevitable as compliance teams reach out to the customer for additional proofs of identity. Compliance is too often seen as a cost of doing
business, but done right it protects the organization from loss of reputation and substantial fines – involving compliance teams in the design and choice of identity proofing solutions is vital.

**The applicant’s identity and data should drive the process**

The applicant, their identity and data are the key to understanding the process and therefore businesses which architect their procedures around their customers will see better conversion rates and lower risk.

Applicants appear from many different routes. In some cases, the business may have no information, little information, an identifier in an existing customer database, or a complete set of data. The on-boarding process must therefore be flexible enough to cope with these different situations.

An applicant-focused on-boarding process should be designed to request only the necessary information at the right time. The functions of “identity proofing” and “credit and affordability” within financial institutions can overlap much more than they already do to reduce customer friction and improve efficiencies.

A consistent journey through the application procedure builds customer confidence and results in the capture of higher quality data. At the same time, as the applicant moves through the process, the business builds up confidence in their identity and information. In some cases, analysis of the flow may develop a better order to prompt the user for data or identify another source where data can simply be looked up.
The key steps to e-KYC

1. **Basic** – The on-boarding process for a regulated entity which must perform customer due diligence or KYC, fraud prevention for a new customer starts with basic data – contact information, including email address.

2. **Identity validation** – The next step is to gather any identity evidence necessary – for example passport number or official name – and check the identity against public lists of politically exposed persons (PEPs) and companies or individuals subject to sanctions.

3. **Identity verification** – Having proved the claimed identity exists, the next stage is to prove that it belongs to the applicant. Matching the person to identity evidence, for example using facial matching to the photo in a passport, establishes the official identity of the application.

4. **‘Liveness checks’** – Criminals that attempt to open accounts using a stolen identity try to break through the integrity of digital onboarding with recordings or a photograph of the legitimate identity holder. The key to detecting these is to identify when a recording or photograph is in use; this is known as a ‘liveness’ check. Liveness detection in digital channels generally falls into three categories:

   5. **Passive** – Often using machine learning, an assessment of the applicant for signs that it is a photograph or recording.

   6. **Active** – The system asks the applicant to carry out certain activities such as look up and down, blink etc.

   7. **Live video link to an operator** – less scalable, more expensive and adds friction to the customer experience but a regulatory requirement in some countries.

Depending on the level of risk and regulatory requirements, organizations can use one or more of these techniques. For example, a passive liveness check could form a ‘first pass’ with any borderline decisions resulting in stepping up the check to active liveness detection or video contact with an operator.

**Data matching**

Fraudsters operating at scale cannot have a completely unique data set for each fraudulent application, so some data elements are re-used across applications or re-used with only minor variations. For example, the same mobile phone number might be used across multiple applications or names reused with slightly different spellings. Data matching and analytics will help to spot similarities across applications and reveal any links between them.

**Compromised account checks**

Any system relying on people can never be totally secure. Customers store their login details unencrypted, re-use passwords and lose mobile phones and security
tokens. Techniques must be used to spot signs of a compromised account, and these techniques include geolocation, device identification and behavioural data.

**Source of wealth and funds**
One way to look for money laundering is to gain an understanding of applicants’ source of funds. It is important to explain why these questions are asked.

**Re-authentication in future transactions**
The last step before opening the account is to determine how a customer will be re-authenticated in future interactions. Existing customers may already have methods in place, but it is good practice to allow them to update authentication factors to increase security, or to update a biometric which might change over time.

**In conclusion – the applicant should be central focus for each business discipline**
During the on-boarding process is it vital to obtain good, accurate data from applicants. Data which the business already holds could be verified if it might have changed, but applicants may ask why they are being prompted again for static data. It is only as the applicant makes their way through the on-boarding process that the questions and data required become apparent. It is important to build a flexible process which can adapt to each applicant’s particular circumstances.
Through this approach, the applicant becomes the point of focus for the internal disciplines of the business:

- The customer experience group is tasked with ensuring positive customer outcomes in a streamlined manner.
- Compliance ensures legal obligations and regulations are met efficiently.
- IT security is concerned about session, application and endpoint security and resilience.
- Software engineering must ensure systems are robust, secure and maintainable.
- Fraud management is focused on balancing losses and liability against preventative measures.
- Business owners are focused on increasing cost-effective generation and protection of revenue.

Only once these skills are brought together, with an emphasis on improving the customer journey, can a business build smart on-boarding processes and benefit from happy customers, reduced risk, compliant procedures and increased revenue.
Making Sure that Your Data Centre Provider’s Foundations are Green
David Watkins

Abstract
The data centre industry continues to grow rapidly as more of our lives become digitally led. But, whilst digital technology is powering, some say revolutionizing, the way we work and live, the millions of data centres which store and process the digital data we create are purging metric tons of hardware, draining country-sized amounts of electricity, and generating carbon emissions as big as the global airline industry. In this article, the author explains that there are many shades of ‘green’ in the data centre industry and why it is more important than ever to ensure that your data centre provider’s foundations are in fact green.

Introduction
Data centres are power hungry, it must be recognized that the industry has made huge leaps in efficiencies from the legacy data centres of years past. These positive changes are being driven at many levels: society is demanding that everyone takes responsibility for their own actions which could be detrimental to the environment; many governments are demanding more efficient, sustainable, environmentally considerate data centres; the data centre industry itself is changing from within; and customers are demanding that their providers are committed to sustainability and green energy solutions.
Today, there are technical solutions and tools that enable data centres to operate more efficiently, using less energy, without compromising the reliability of facilities.

What data centre customers should look out for
Many of today’s customers have exacting Corporate and Social Responsibility targets and these include the outsourced data centre power consumption and carbon emissions in calculations of their own carbon footprint. However, demanding more sustainable data centre solutions is one thing, but how can a business determine whether a facility is actually “green”, and how “green” it is?

Many data centres will claim green credentials, but there are many different shades of green, for example, carbon neutral is not as sustainable as carbon zero.

1. Design and build
When designing large-scale sustainable data centres, there needs to be a balance between making it green without compromising its operations and reliability. Building a sustainable data centre means building facilities that don’t have a lasting, detrimental impact on the planet. It also means considering the recyclable content of materials that have been used, minimizing waste to landfill, considering the recycling of waste heat generated, whilst ensuring facilities are well maintained.
The data centre industry has certainly evolved, especially in recent years, but although the basic data centre design hasn’t changed much, some aspects have greatly improved. Reports show that infrastructure efficiency has improved by 16% since 2014\(^1\) demonstrating that where steps are taken to improve issues like heating and cooling, cost savings can also be made.

When it comes to building facilities, BREEAM (Building Research Establishment Environmental Assessment Method) standards look at the green credentials of commercial buildings, verifying their performance and comparing them against sustainability benchmarks. BREEAM measures sustainable value in a series of categories, ranging from energy to ecology. Each of these categories addresses the most influential factors, including low impact design and carbon emissions reduction; design durability and resilience; adaption to climate change; and ecological value and biodiversity protection. As well as the commitment to meeting BREEAM specifications, many providers also employ a modular build methodology to deploy capacity as and when required. This drives up utilization, and maximizes efficiency (both from an operational and cost perspective).

2. **Powering the data centre**
   Arguably one of the most difficult areas to account for is the energy consumed (and heat generated) by data centres. The constantly processing computers
and servers which make life online possible and so ubiquitous have long been seen as significantly detrimental to the environment. Reports suggest that data centres globally currently use between 200 and 500 terawatt hours (TWh) of electricity per year\(^2\). Even at the lower end of this estimation, this accounts for 1% of the global electricity demand – more than the energy consumption of some entire countries – and surpassing that of energy hungry industries.

Customers want to know if data centres are powered by renewable energy sources. It is in the use of renewable energy where being environmentally conscious is helping to better meet customer demand. Periods of electricity price surge or downtime associated with traditional energy sources can challenge providers to maintain service at the level that their users expect – renewables are already demonstrating increased reliability. Furthermore, fixed pricing in renewable energy can help manage budget volatility – again important in managing and meeting customer demand.

Today, renewable energy is often less expensive than brown power. As technologies develop, demand is driving down price, and it’s now not just more affordable to be environmentally aware, but potentially fiscally beneficial too. Buyers can negotiate long-term fixed-prices or stable-price contracts for renewable energy and in recent years the cost of hydrogen fuel cells has plummeted, to the point where they are an economically viable alternative for standby generation.

More widely, the cost of renewable power is increasingly cheaper than any new electricity capacity based on fossil fuels\(^3\). Indeed, on average, new solar photovoltaic (PV) and onshore wind power costs less than keeping many existing coal plants in operation, and auction results show this trend accelerating – reinforcing the case to phase-out coal entirely.
3. **Using the very latest techniques**
   In legacy data centres, for every kilowatt of power a server used, it generally requires another kilowatt of thermal energy to cool it down. Nowadays, using modern cooling techniques, accepting higher server “air on” temperatures and deploying hot or cold aisle containment, facilities can be cooled for a tenth of the power used by a server.

Examining plant management, there are now many technologies and methodologies which can be deployed to drive efficiency and produce less carbon emissions. In addition, there doesn’t need to be as much engineering infrastructure in place to achieve acceptable environmental conditions:

- Highly efficient servers, mean that one rack can replace six older versions, placing more emphasis on air management, cooling and containment systems. UPS (Uninterrupted Power Supply), means that unused capacity can ‘hibernate’ to reduce electrical losses;

- CRAC (Computer Room Air Conditioner) units are typically equipped with variable speed fans, which will regulate in line with demand to reduce energy consumption;

- Pumps are now equipped with variable speed drives, which again will regulate in line with demand to reduce consumption;

- Chillers often have “free cooling” functionality, where within certain temperature ranges cooling can be provided at a much lower cost;

- Ground and air source heat pumps are being deployed, along with local energy generation all making use of clean, naturally available resources.

**In conclusion**
Energy improvements in data centre construction and management ensures that the world’s increasing data use does not necessarily mean spiraling energy consumption, and the associated environmental impact.

Every data centre operator in the world should feel an obligation to minimize the impact they have on the environment and surrounding communities. Being a responsible operator with a demonstrated commitment to sustainability is not just the right thing to do, it is increasingly what customers are demanding and can actually deliver commercial benefits – continuing the journey to greater energy efficiency and sustainability is more vital than ever.

---

**Reference**
SD-WAN: As Simple or as Complex as Needed
Duane Henigin

Abstract
More cost-effective and flexible than legacy router-centric multiprotocol label switching (MPLS) WANs, software-defined wide-area network (SD-WAN) offers superior responsiveness, enhanced application performance, more robust security, and improved visibility that gives greater reliability and consistency to enable organizations to advance their cloud and digital transformation initiatives. But despite all this, says the author of this article, too many organizations are still failing to take full advantage of the new generation of SD-WAN technology.

Introduction
For many enterprises today, it is likely that their wide area network (WAN) has grown in complexity over time, or the company has inherited a network with its own challenges. Indeed, mergers, acquisitions, consolidations, closures, new applications and new business needs make designing and managing an enterprise WAN a never ending and complicated task – a task that some say requires the ability to read minds and predict the future.

Add to that the reality that most businesses are constantly faced with finding a balance between dependability and performance with cost, and they have just scratched the surface of architecting and managing a modern enterprise WAN.
Businesses must find a new way to look at their WAN architecture – one that focuses on the desired business outcome and not just how the ‘ones and zeros’ get from point A to point B. This often points to networking architecture, such as software-defined WAN (SD-WAN) technology.

However, when building an enterprise WAN, it is critical to keep it as simple as possible. In fact, there are a number of valid reasons for a network to grow in complexity without over engineering it from the start.

While SD-WAN may seem daunting, it can provide an enormous opportunity to build a modern network with a solid foundation that will grow with the changing needs of a business.

For a product to be both simple to deploy yet address complex requirements, businesses must choose a vendor that has both maturity and focus. However, as well as the vendor having a solid foundation in enterprise WANs, the technology itself needs to be ready to hit the ground running. It must be simple to configure and deploy, but also advanced enough to handle the complexity and scale of an enterprise network – and there are only a handful of solutions that are capable of this.

source: Silver Peak
So, what should businesses look out for when it comes to SD-WAN?
An SD-WAN should have a solid foundation based on application acceleration and steering traffic over any combination of WAN transport reliably using virtual private networks (VPNs). In addition, with capabilities such as zero touch provisioning (ZTP) and zero touch configuration (ZTC), companies can deploy hundreds or thousands of sites or more in just a few days or weeks. This capability has been particularly critical during the COVID-19 pandemic, where companies have had to adapt to supporting the workforce as employees transitioned to working remotely.

Many enterprises will also need an SD-WAN that is capable of protecting their voice over internet protocol (VoIP) traffic. For example, a company might have two or three critical applications that have to be up at all times, they might need to prioritize certain traffic, as well as have the ability to securely segment traffic from the rest of the network. While some businesses believe that there is no way of doing this over the internet, once they start making VoIP phone calls across an SD-WAN fabric and start disconnecting circuits without negatively impacting the call in any way, they will realise that this is the reality of enterprise WANs today.
While being able to protect VoIP traffic with multiple circuits has become a standard feature of most SD-WANs, it is important that businesses look at more advanced capabilities. It should be able to protect VoIP traffic, as well as protect all other application traffic without using up available bandwidth. As such, the SD-WAN technology must be customisable and be able to adapt as business and application requirements change.

In addition to this, it must also be able to address complex configurations, such as dynamic routing, load balancing and failover criteria, security segmentation, application prioritisation, local internet breakout, application performance and high availability.

**In conclusion**

To navigate the complexities of enterprise networks today, particularly amid the COVID-19 pandemic, it is important that their networking architecture provides them with freedom of choice. It should be up to the business to decide how simple or complex their SD-WAN deployment should be – they should be able to choose what best-of-breed wireless, switching, security and solutions they use. Here, interoperability is key.

In addition to this, businesses should also be able to choose to stay with local applications or hosted applications, as well as keep their data centres or migrate to the cloud. This will enable businesses to correct all those annoying little “snowflakes” that exist in their network that continue to make network engineers lives hard.

Whether they chose to keep multiprotocol label switching (MPLS), move to all internet, or even run both, an SD-WAN should provide businesses with the choice. While it can be as simple or as complex as needed, the journey to SD-WAN can be made simple.
Modern Bank Heist: From Smash and Grab to Hostage Situation as Cyberthieves Evolve
Tom Kellerman

Abstract
VMware Carbon Black has just published the third edition of its Modern Bank Heists report, which takes an annual pulse of some of the financial industry’s top CISOs and security leaders. But as the author of this article explains, the report offers more than just data. Carbon Black uses the information gleaned from this report to educate the market on how modern cybercriminals are evolving; what tactics, techniques and procedures (TTPs) are emerging; and how defenders can keep pace. The financial sector is not a new target for criminals, the bank heist has evolved significantly over the years – from stickups to cyberspace – but the fundamental motivation behind the attacks has remained the same: money.

Introduction
The financial sector is historically one of the most secure industries in the world. It needs to earn trust and convince customers that their hard-earned money is safe. Nevertheless, the fact that banks are guardians of the one thing cyber criminals typically desire most (money), means security teams are under relentless pressure. Attackers are prepared to invest time, resources and collaborate to develop new and more effective ways to reach the digital vault and make off with money. Our third Modern Bank Heist report\(^1\) collected the views of 25 security
leaders and found that attackers are evolving and getting more sophisticated as they aim to secure long-term illicit access to banking systems – and they are capitalizing on the disruption of COVID-19 to help. So, what can we learn from the data revealed in the report, and how can we combat the emerging threats?

COVID-19 surge hits financial sector

Among the CISOs we surveyed, 80% said they had experienced an increase in cyberattacks over the past 12 months, up 13% compared with a year ago. Some of this is attributable to the COVID-19 surge – separate VMware Carbon Black data showed there has been an increase in attacks on finance sector targets of 238% from February to April 2020, and we saw ransomware attacks on the sector increase by a multiple of 9 during the same period. Closer analysis shows that notable alerts observed in VMware Carbon Black data spiked in correlation with significant moments in the COVID-19 news cycle, indicating that attackers are capitalizing on disruption to attack while the world looks the other way.

The majority (82%) of our CISOs noted an increase in attack sophistication over the past year, and the ways attacks are developing gives us a valuable insight into attacker behaviours that should inform our response. Overall, we are seeing attackers moving past inelegant “smash and grab” tactics, and towards more of a “hostage situation” where their motivation is to gain and retain footholds in target networks for long-term campaigns.

The Kryptik trojan and Emotet malware continue to feature among the top attack types experienced, our research has found (see figure 1), and these are often used in longer, complex campaigns aimed at leveraging native operating systems tools to remain undetected or gain a base to island hop to a larger and more lucrative target.

![Figure 1: The most prevalent threats affecting the finance sector from March 2019 to February 2020](Source: Carbon Black, Modern Bank Heist 3.0)
Another indication that attackers are operating for the long-term is the fact that the most prevalent MITRE threat ID affecting the finance sector over the past year is T1507 – Process Discovery (comprising 64% of attacks). This shows attackers are investing in increasing their knowledge of policies and procedures in financial institutions, the better to work out how to infiltrate them undetected. They are also ramping up their awareness of incident response tactics and seeking blind spots that they can exploit to remain invisible.

Island hopping experienced by one third
Over 30% (33%) of the CISOs surveyed reported experiencing island hopping, where supply chains and partners have been unwitting vectors for attacks. The most common type of attack is network-to-network, but one fifth reported suffering watering hole type attacks, where hackers target a website frequently visited by customers of the target and attempt to gain access credentials, or the site of the financial institution itself to launch malware into visitors’ browsers.

Island hopping-as-a-service is also on the rise. In 2019 our analysts uncovered a secondary component in a well-known cryptomining campaign that was designed to exfiltrate system access information that was destined for sale on the dark web. This is a significant change in behaviour that defenders need to keep on the radar as what looks like one type of attack may be cover for another.

“Virtual invasions” on the rise
Almost two thirds (64%) of those surveyed said that they had seen increased attempts at wire fraud transfer, up 17% compared with 2019. These attacks rely on attackers’ knowledge of business process gaps in the verification process, or on direct social engineering of customers or customer service representatives.

Counter-incident response up as attackers evade detection
Almost a quarter (24%) of our surveyed CISOs had witnessed counter-incident response as attackers prioritize persistence and seek to retain their foothold in the financial institution’s network. This is something we expect to see escalate in the coming year.

Tactics such as log deletion, manipulation of time stamps and disabling of security controls will all feature as attackers cover their tracks. Related to this are destructive wiper attacks designed to “burn the evidence” of infiltration and prevent defenders conducting forensic analysis to stop the same vectors being used in future. This has major implications for incident response: we need to get more clandestine.

Greg Foss, our Senior Threat Researcher at WMware Carbon Black has five tips for incident response to avoid alerting adversaries:

1. **Stand up a secondary line of secure communications** – This is vital to discuss the ongoing incident. Assume all internal communications are compromised and visible to the adversary.
2. **Assume adversaries have multiple entry points** – Shutting off one entry point may not remove the attacker and may have the opposite effect by notifying the attacker you are aware of their presence.

3. **Watch and wait** – Don’t immediately start blocking malware activity and access or terminating the C2. You need to monitor closely to assess the scope of the intrusion to work out exactly what to do to fully remove the adversary.

4. **Deploy agents in monitor-only mode** – If you begin blocking or otherwise impending activities, they will realize and change tactics, possibly leaving you in the dark.

5. **Deploy honey tokens or deception grids** – Particularly on attack paths that cannot be hardened.

**In conclusion**
The financial sector is facing a threat that evolves as fast as it can adapt. To combat the tactics adversaries are developing, we need to understand more about their behaviour. That means that kneejerk shutting down of attacks must be exchanged for a more clandestine and nuanced approach that allows us to learn, combined with our own collaborations across the cybersecurity and financial sector.

The digital vault is hostage to persistent, resilient attackers who have strategic plans for getting into and remaining in the network, so defenders need to think strategically too, if we are to stand a chance of mounting a successful counterinsurgency.

---

**Reference**

Expert Witness: Delivering Evidence from the Dark Web when Data Breaches Go to Court
Austin Berglas

Abstract
With personal data being easily purchased from the dark web. Many criminals are undertaking this data to commit identity theft but BlueVoyant professions can evaluate and explain to courts how personal data is sourced by cybercriminals and used to commit fraud. In this article the author discusses how the impact of stolen data can become a legal issue in terms of class action lawsuits.

Introduction
The well-publicized implementation of privacy legislation, including the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR), has raised public awareness considerably regarding the value of personal data and the implications of its loss or theft. The fear that a malicious actor might use stolen Personally Identifiable Information (PII) or other personal data to commit fraud via identity theft is a real and understandable concern for individuals. This fear is compounded by the frequent data breaches that hit the headlines, where people hear or read about millions of records being exposed or stolen. Often, one outcome of these mega breaches is a class action lawsuit, where individuals whose data has been breached launch a suit against the organization that has been accused of not securing their data.

As experts in cybersecurity and the dark web, where breached data is often destined to end up for sale, BlueVoyant professionals may be called in as expert...
witnesses to help analyze the risk increase a breach has, or has not caused, and explain to the court how personal data is sourced by cybercriminals and used to commit fraud. So, what are some of the factors we consider when we assist in these cases and how can individuals minimize their risk of fraud, even if their data is involved in a breach?

The first thing to note is that no one wants to end up on either side of a class action lawsuit over a data breach. Plaintiffs are worried about whether they need the protection of anti-fraud measures, and defendants have suffered loss of customer trust, reputation, and potential financial damage. We focus on helping courts come to a fair conclusion based on evidence that we can provide thanks to the expertise of our cyber threat and dark web analysts and the insight we can provide into cybercriminal communities and tactics.

**Can the stolen data be used to commit identity theft?**

One of the critical determinants of a class action lawsuit hinges on the type of data that has been stolen and whether it can be used on its own to commit identity theft. In this sense, all data breaches are not quite the same.

When data is stolen, if it has any value at all to fraudsters, it usually turns up on dark web marketplaces, where it is clear that pieces of personal data have differing value to cybercriminals. Opening bank accounts, making purchases, or claiming benefits based on someone else’s identity requires specific privileged information. We can make precise determinations on what information is necessary to commit specific criminal schemes and we are able to comment to the contrary when data breaches do not contain sufficient PII to advance fraudulent activities.

Dark websites that cater to identity thieves usually carry inventory that focuses on the types of data required to commit financial fraud. In the cybercriminal world these data packages are referred to as a ‘Fullz’. Fullz, at a minimum, includes the victim’s full name and billing address, credit card number, expiration date and card security code, as well as their social security/national insurance number and birth date.

**Risk exposure on the dark web**

Another aspect we are often asked to investigate as part of class action work is the level of exposure those affected by the breach already have on the dark web. The rationale for this is to establish whether the breach in question has genuinely increased individual identity or financial fraud risk.

It often comes as a surprise when people learn just how much of their data is already available on the dark web. Our dark web analysts conduct exhaustive searches of deep/dark web sources to establish what personally identifiable information is obtainable and identify the historical breaches from which it originates.

We can build a full picture of an individual’s presence online. This could include lists of stolen account log-in and password details, as well as PII such as driver’s
license information, residential history, and social security data. If class action participants had low exposure prior to the breach at issue, their claim that the breach has raised their risk can be validated. If, however, much of their personal data was already available, their position – in the case of this specific breach – is, potentially, not as strong.

Assembling this evidence requires support from an authoritative and credible expert witness with covert presence on the dark web from which to conduct investigations, such as the presence we maintain at BlueVoyant. Our analysts, who have honed their craft in international intelligence agencies and at the highest levels of private sector cyber intelligence, can build this portfolio of information to lend evidence-based clarity and substance to legal arguments.

What can individuals do to protect their data?
Experience tells us that it’s vital individuals keep high-value personal data under tight control so that, in the event of a breach, your risk of identity theft or financial fraud can be reduced. This means keeping social security/national insurance numbers, credit card information and PII closely guarded, for when combined they can be the prime tools for identity verification by financial and government institutions.
Also, the importance of account password hygiene cannot be overstated. Cybercriminals who buy a list of names, emails and passwords exfiltrated from a breach at one organization will try them out with other businesses, meaning if you use the same log-in details with your favourite clothing store as you do for your bank, a breach of one of them compromises your security with the others.

Ultimately, no one wants to be involved in a data breach class action but, when they do happen, understanding the value of the data stolen, whether it has surfaced on the dark web, and the level of victims’ existing exposure are the key factors the court needs to use to reach its verdict. That is where we can help. At BlueVoyant, we can research, analyze, and present evidence that helps courts to reach a fair conclusion in data breach class action lawsuits.
Congratulations on your new job. What will your new role as CTO at WSO2 entail?

Thank you. I am very happy – after about ten years of working for banks – to go back into the tech sector. In financial services I was chief security architect for the consumer bank division of Citibank, and before that role, I was chief architect for the treasury and trade division of Citibank which handles the accounts of the Fortune 500 and Governmental organizations worldwide, encompassing payments, foreign trade, and financing for corporate treasury departments. Previously, I had been the chief architect for the banking division of Credit Suisse. But prior to this, I spent about 25 years in the tech industry, with my most recent job before financial services being CTO for IONA Technologies.

In many ways, my job at WSO2 is very similar to the role that I had at IONA, but today, the tech industry has moved on so dramatically and is so forward-thinking that my role will be quite visionary and very exciting.
My technology career started as an engineer at Digital Equipment Corporation, that
is now part of HP, before I moved to IONA Technologies (now part of HP). As I
was in transactional database processing I began specializing in that area co-
writing several text books including, Principles of Transaction Processing (with Phil
Bernstein), Understanding Web Services, and Understanding SOA with Web
Services (with Greg Lomow). The books were well received and respected as
college texts, and I have had the privilege of working with some real industry
heavyweights.

My move into financial services came as one of IONA’s largest customers was
Credit Suisse. At IONA I had worked with the team dedicated to Credit Suisse and
got to really understand how IONA’s technology vision and products were being
received, and where we might look for improvements and future changes.

During that time, I got the company involved in web services, which made them
pivot over to web services and help establish a lot of the standards which these
services are based on. This is when I first met Sanjiva Weerawarna and Paul
Freemantle – so I knew both founders of WSO2 long before they started the
company.

For me now to have the chance to move back into the tech sector and work with
Sanjiva, Frank Layman, Jonathan Marsh, and some other industry veterans which I
knew from those days is really wonderful. The enthusiasm and the culture at
WSO2 is tremendous. The technology capabilities, collaboration and talent of the
employees are at an exceptionally high level, and my role as CTO will be to help
figure out the future direction of the company – especially as we move towards
cloud and cloud-native computing, and I am looking forward to working with our
customers and analysts to get the word out.

Generally, I summarize the role as trying to facilitate a virtuous cycle – to use an
Amazon word ‘a flywheel’ – that starts turning between what is going on in the
engineering and technology department at WSO2 for new ideas and new solutions,
new proposals for contributions to solving and addressing some of the problems in
the industry, and bringing that out, talking with press, analysts, customers, and at
events and most importantly, getting some feedback on those ideas.

We see our contribution to that cycle as the ability to have the conversation at the
table, as opposed to standing outside the building trying to work out what everyone
is talking about. So we will be contributing our intellectual capital into the broader
industry for the purpose of participating in the discussions, getting information about
what everyone else is doing.

We found that by having a seat at the table, and getting the feedback from
customers, we can feed that all back into the company. This is the context in which
we are playing in the broader industry. Now let’s see how we can tweak and refine
our core message and our strategy to deliver that service.

At the same time, we are making sure we are thinking two or three years forward –
especially around the transition to the cloud. We’re figuring out together what and
how we can contribute to the cloud data trend. What we can offer to our customers, and to the industry in general.

**Now that you are back in the tech world, so to speak, in addition to your blog, will you also be writing further text books?**

I have started reviewing some of the collateral which has been drafted inside the company to help frame the content especially as I have been involved in writing as a profession.

I am really thinking about whether the programming language Ballerina could be the subject of my next textbook, as Ballerina was originally designed by WSO2 to improve productivity for application developers that have to work with distributed cloud-native systems.

**As you have come in to help set the vision of the company, is there a particular timeline you are working towards for Ballerina?**

The first order of business is really around the move to the cloud.

I was speaking about this to Sanjiva only this morning, discussing how the technical underpinnings of the cloud provide value for money – almost like a seismic shift in value for money – compared to the older IT environments.

Inevitably our customers will want to move there for all the benefits of cost and flexibility, scale up, large data handling, and machine learning – which can all be achieved by going into this new computing environment. Whether it be on-premise or hosted in public cloud, there is a seismic shift in IT infrastructure and all companies are trying to get there.

Of course, web companies such as Google, Facebook, Amazon etc are already there. Whenever a new company launches it can already access ready-made flexible infrastructure which gives it an immediate advantage over legacy competitors. This is how they are in part disrupting established companies by using better, cheaper, faster IT infrastructure.

For instance, if you look at financial services there is a long list of fintech companies entering the market and all of them are based on this new infrastructure which means in some ways this flexibility is the competitive advantage for improving the user experience. They can change their applications more quickly in response to customer feedback. They get the feedback through machine learning and AI. They also collect data more quickly than via legacy infrastructure and older enterprise applications. Therefore, industries are looking for a more responsive agile IT environment, so they can get the same benefits that machine learning feedback loops are able to generate for web companies.

For example, today I was looking at a hotel booking and it appeared in my facebook feed later. It is very annoying, but at the same time it is the enigmatic power of these technologies on these infrastructures which is driving customer experience,
and therefore revenue. So assuming companies are going there, our task has to be to figure out how to help them get there, and what to do to help advise them once they get there.

**Coming from the financial services market, has there been anything which has been a real driving force for you to go back to the tech world?**

When I joined financial services it was almost like taking a step back in time dealing with legacy systems and the lack of agility, for instance, compared to what you would be able to do in a fintech.

In a technology company you are always looking forward seeing where the latest trends are, the technologies coming on board, and how they can help solve customer problems. Whereas in an established company such as a bank (which often has a long-established and archaic history) you are always looking backwards at what has been proven, what you know is going to work, and what you can adopt safely.

It is definitely exciting to be back in a forward-looking role and with WSO2 I think the opportunity is great as the company evolves. It has been a very successful company with its current strategy, and now everyone realizes it is time to pivot and revise the strategy, so it is a great time to participate in that.

Also I think Ballerina is a very fascinating project, that we touched on before, to create a new language for the purpose of assisting customers in this journey to the cloud. There is a lot of potential right there.

Today Ballerina is being used in our integration projects to make them easier to provide a low-code for integration. But longer-term, I think there is even more potential for it to be the language which is relevant for this migration to the cloud – and that is very exciting.

**What sort of trends are we likely to see moving forward?**

The movement towards a more modern IT infrastructure is one, and the benefits of that, and the need to re-engineer for it, is an on-going trend.

Re-engineering is symbolized by the micro service trend. Some folks such as Martin Fowler talk about it as a development trend, but it is not really. That is not why it exists. It exists because commodity data centres are made up of hundreds of thousands of PCs and you want to have the right size workload running on them.

You create your application, and you have hundreds of these micro services working together in a PC-based environment. This is the reason why they have become so popular because they are the best way to create applications suitable for this new IT infrastructure.

I think that will continue, and in conjunction with that is a culture shift in the existing enterprises where you will be creating these smaller units of work, then stitching
them together to build your applications. Organizations will need to reorganize their teams.

It’s not just about technology, but about adopting more agile techniques, and smaller teams which can work together on these units of work as opposed to bigger teams that work on these larger monolithic applications. That is definitely going to be continuing as companies try to figure out what is the right way to organize their IT staff to handle this; re-engineering and forward-looking movement into big data, machine learning and AI.

This is another trend that is going to continue, and accelerate.

We are seeing how some colleagues in the area of edge computing are viewing machine learning and AI capabilities at the edge of the network. Probably the best-known example of this is Alexa – there is some machine learning AI in there which is why Alexa is so fast. There will be similar technology in cars, planes, trains, washing machines, electric meters, etc. It is going to be amazing to think that we will have a world of APIs.

This brings us back to what we are all interested in – API management.

It is amazing to think you can have APIs on all these devices which you can call and send a request for AI execution out on the edge of the network. This is a fascinating trend which will continue during the next year and we will see a lot of activity in the API space.

We also touched on the machine learning and AI feedback loop where you collect sufficient amounts of data – and you really do need a lot of data sets for this – to go through and understand customer trends.

In particular, we are talking about financial institutions who are interested in having the ability to provide good customer-intuitive experiences – easy to use mobile apps, easy to use web apps. Being able to get the feedback loop in place so that these companies can tailor these experiences to the customers much better is another trend that is going to continue, and that will involve a lot of the data management activities to ensure data quality.

The challenge for machine learning tends to be getting the data in such a form and space that it can be used successfully for those algorithms. You can’t just feed any garbage in – you will simply get garbage out, if you do.

Because of the ongoing Covid-19 situation, there is the need to push everything to digitalize, and at WSO2 we will find a way to help companies achieve this.

Is there one forward thinking thought you would like to leave our readers with?
One of the most interesting things going forward is the cultural aspect of how IT is being done. Until we change that and align the agile culture to the agile nature of
the software in the API landscape, we will not be able to realize the full benefits of the new technology.

If you are talking about automating the development process and pushing out changes to your website every couple of hours – as some of the web companies do – that is a culture shift, that is not just technology.

Going forward, it is how you organize your department. How you do your testing and your development, it’s how you give responsibility to your teams, how you oversee them, how the teams work with other teams and so on. For me this is probably the biggest problem on the horizon, but when resolved it will make a big difference to the organization.
Putting theory into practice can be both challenging and satisfying for the technology industry. The ability to fully understand a client’s problem, analyse the situation, and then find the best solution that meets a client’s technology requirements, while delivering, managing and supporting the infrastructure and services which drive progress towards the client’s business goals are key elements in the industry’s success.

A well written case study will follow a customer as they define a problem, determine a solution, implement it, and reap the benefits, and offers readers the ability to see a situation from the customer’s perspective from beginning to end. Case studies give a first hand look at how IT companies think, work and interact with their clients.

In this section, we feature three Case Studies which have particularly caught our attention:

1. **Fileturn – streamlining the accounts process**
   YourDMS

2. **Café Zupas Extends WatchGuard Simplicity and Protection from the Network to the Endpoint**
   WatchGuard Technologies

3. **MM Manufacturing – eliminating the waiting game**
   Taulia
FILETURN LTD CASE STUDY

Fileturn is an innovative interior fit-out contractor, with experienced and reliable construction teams, creating outstanding environments for their clients. Their extensive experience in fitting out and refurbishing a wide variety of premises for high profile brands has ensured an unparalleled reputation for excellence and an enviable client list.

ANALYSIS

Fileturn had a busy accounts department who were manually processing around 1200 invoices per month. To process each invoice, a member of the team had to attach a bar code, stamp the date, sign and code, remove any staples, scan the invoice, and re-staple it. The scan would be saved, and the data from the invoice would be entered into the accounts system by hand. The paper invoice would then need to be filed away in a filing cabinet.

The whole process was time consuming and labour intensive, taking a team of 3 people to complete this job alone. With ten invoices taking around 30 minutes to process, the team were always under pressure to meet deadlines. Processing invoices manually made it harder to spot duplications, errors in the invoice data and incorrect VAT percentages.

Fileturn knew that in order to continue growing successfully and stay in control of their finances, they needed to find a faster and more accurate way of working.

“We wanted a solution that would stop us having to input everything manually, and that’s what YourDMS has provided. It’s streamlined the way we work, which has allowed us to process more invoices without increasing the size of the team.”

Laura Holden
ACCOUNTS AT FILETURN LTD

YourDMS SOLUTION

Fileturn were already using an Invu Document Management system to store their electronic files. YourDMS proposed implementing an automated Invoice Processing solution to reduce the need for manual data entry and checking. The solution would integrate fully with the Invu system and also with Fileturn’s existing finance software.

The automated solution would also make it easier for the accounts team to quickly respond to queries as they would have access to all the information they needed at the click of a button.

Once an invoice is entered on the system, it would be securely stored in Invu and Fileturn would no longer need to keep the paper copy, freeing up valuable office space.
RESULT

With the new automated system in place, the accounts team can now process ten invoices in around two minutes, saving a huge amount of time and allowing them to focus on other tasks.

The system now automatically checks the invoice data and alerts the team to any errors, so they only have to intervene if there is an issue. Pre-defined rules allow ‘correct’ invoices, up to a pre-agreed amount, to be processed automatically.

As Fileturn grows, this will allow them to increase the number of invoices they can process without increasing the size of their team.

YourDMS provided training and assistance with using the new system. Laura Holden, part of the accounts team comments, “I found it quite easy to go from working manually to using a digital system. The programme is simple to use, so I can’t see why anyone couldn’t do it. The support we get from YourDMS is always really good. They are always happy to show us how to do things so that we can get on and do them ourselves in the long run.”

“In the accounts department, it’s very important that our work is accurate. We need to make sure that invoices aren’t duplicated, VAT percentages are correct, and invoices are processed before we have to close off for that period. Using the automated system has allowed us to be more productive by checking amounts and alerting us to any problems, so that we can resolve them straight away.”

Laura Holden
ACCOUNTS AT FILETURN LTD

What is Fileturn’s advice for other companies who are tackling similar problems?

Laura explains, “I would advise them to have a look at the solutions that YourDMS offer, and then weigh up the pros and cons. Yes, it’s a brand new system but you have to consider how much time, effort and money you would save. We’re really happy with how it’s working for us.”
Café Zupas Extends WatchGuard Simplicity and Protection from the Network to the Endpoint

CHALLENGE
Café Zupas first opened its doors in 2004 with the desire to create a family-friendly restaurant where their guests could enjoy a quick meal without compromising on the nutritional benefit that real homemade food provides. To do that, Café Zupas has a clear, company-defining mission “to make each soup by hand, each dressing and sandwich spread from scratch, and create dishes just as you would at home.” While others in the industry doubted it could be done, and particularly at scale, Café Zupas found a way to never sacrifice quality for convenience. Today, Café Zupas serves their “house-made” food at nearly 60 locations across eight different states.

As a company in the hospitality industry, Café Zupas is a prime target for cyber attack. “Being in hospitality, we are one of the most heavily targeted industries for hackers looking for credit card numbers or personal information. We have to stay ahead of the cyber criminals and on top of our PCI DSS compliance audits. We are constantly evaluating security products to make sure we have the best solutions we can,” explained Wes Beaman, CIO at Café Zupas.

Café Zupas recently set out to review their endpoint security solution, “We were using CrowdStrike, which is a good product in terms of the security it provided. But it just wasn’t offering the reporting and management capabilities that we needed,” says Beaman. In addition to CrowdStrike, Café Zupas was evaluating ESET, Trend Micro and the newest addition to the WatchGuard portfolio, Panda Adaptive Defense 360 (AD360).

SOLUTION
Café Zupas, a longtime WatchGuard customer, deployed their first set of Fireboxes in 2014. Today, they continue to trust WatchGuard to secure their network and restaurants - with a Firebox T30 deployed at each location, M300s at the corporate headquarters and Firebox Cloud to secure their AWS environment. Additionally, the IT team is currently in the

CLIENT
Café Zupas

NUMBER OF EMPLOYEES
1500

INDUSTRY
Hospitality

REGION
United States

WATCHGUARD PRODUCTS
- Firebox T30 & M300
- Firebox Cloud
- AP325 with Total Wi-Fi
- Panda AD360
- Panda Advanced Reporting Tool
- Panda Patch Management
process of rolling out WatchGuard AP325 access points with Total Wi-Fi including WIPS, and analytics and engagement tools to create a Trusted Wireless Environment.

So, when it came time to evaluate potential endpoint security solutions, Café Zupas knew they needed to include the new WatchGuard endpoint platform into the mix. “As we tested the Panda AD360 product, we found that it was able to offer the same security and protection that we’d seen with CrowdStrike but provided the improved reporting and management that we were looking for,” explained Beaman. Café Zupas chose to replace their CrowdStrike deployment with WatchGuard’s premier offering, the Panda AD360 product, which combines next-generation antivirus protection with endpoint detection and response into one package for comprehensive protection against sophisticated endpoint attacks.

"I wanted to consolidate our security products under one vendor. With the addition of the Panda products to WatchGuard’s already robust security portfolio, I’m able to do that."

~ Wes Beaman, CIO at Café Zupas

RESULT

The IT team at Café Zupas has come to expect simplified management and deployment with WatchGuard products – and AD360 was no exception. “We were able to deploy the entire solution to all of our restaurant devices and corporate endpoints in less than a week. It was really very simple,” Beaman attests. In addition to AD360, Café Zupas also chose to roll out the Advanced Reporting Tool (ART) and Panda Patch Management to each of their nearly 60 locations. “The reporting is substantially better with the Panda products. With this deployment, my senior engineer expects to save at least two hours each week managing reports. With only six people on my team managing all of the company’s IT and security needs, that’s huge.”

Best of all, Café Zupas was able to consolidate their network, Wi-Fi and endpoint security solutions under one vendor that they’ve grown to trust. “I wanted to consolidate our security products under one vendor. With the addition of the Panda products to WatchGuard’s already robust security portfolio, I’m able to do that,” said Beaman.

ABOUT WATCHGUARD

WatchGuard Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company’s award-winning products and services are trusted around the world by nearly 18,000 security resellers and service providers to protect more than 250,000 customers. WatchGuard’s mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.
The Challenges of Running a Small Business

Like many small businesses, MM Manufacturing faces a number of challenges, including complying with government regulations, managing the rising costs of insurance and keeping her supply chain flowing. Marianne notes, “Being a sole proprietor, I am always sensitive to ensuring I have constant cash flow coming into the business. Taulia has made that easier than ever.”

Given her need for cash flow, she knows she can’t take “too many risks” with her money and her income must remain steady at all times. As Marianne explains, every month her “company starts out with zero.” For that reason, “timely payments are critical,” so that by the end of the month, she’ll have enough to pay her vendors and also set a little aside for herself.

According to Marianne, “Taulia is a great program” for a number of reasons. First, the streamlined, one-stop system sends Marianne notifications through the portal letting her know the status of her orders, invoices and payments. In mere seconds, Marianne can transform purchase orders into invoices and once she submits her invoices, the system speeds up the payment process significantly. “I know exactly when my invoices are approved and can go in and opt for early payment. There’s no more waiting around for paper checks.”

In short, Taulia offers all the features she needs to allow her company to live up to its marvelous namesake. With rapid, more efficient access to cash flow, small businesses like Marianne’s can improve their operations, increase their production and expand to meet customer demand.
Notes for Contributors

**IT for CEOs & CFOs** has one goal: to be the source of the most authoritative information for CEOs, CFO, and CIOs involved in all aspects of IT and Software. **IT for CEOs & CFOs** reports on leading research from academia and other sources and its application in real organizations. This means that we actively encourage applied research, case description and qualitative discussion and analysis as well as quantitatively based papers. The ideas presented in these articles have been tested in the real world of business and can be translated into action.

**Editorial scope**
Articles are written for senior executives by experts whose authority comes from careful analysis, study, and experience, and are relevant to different industries, sectors and geographical locations. Covering the areas of Information Technology, Software, IT Compliance, Data Centres, Cloud Computing, Cabling, Intellectual Property, Hardware, Green IT, Mobile Technologies, and Neural Strategies, etc.

As an IT publication, articles in **IT for CEOs & CFOs** fulfil the Journal’s goal by:

- Offering breakthrough ideas to help top executives establish an intellectual agenda for discussion, and change, within their organizations.
- Describing best practices and hands-on techniques to help executives in myriad companies, e-business start-ups, multinationals, professional service firms and family businesses.
- Report on leading research from academia and other sources and its application in real organizations.
- Commentary on the theory and practice of management by drawing on the experiences of executives and consultants.

**IT for CEOs & CFOs** is international in scope and seeks at all times to present a global perspective on the problems of managing all area of Software and IT.

**Copyright**
Articles submitted to **IT for CEOs & CFOs** should be original contributions and should not be under consideration for any other publication at the same time. Authors submitting articles for publication warrant that the work is not an infringement of any existing copyright and will indemnify the publisher against any breach of such warranty. For ease of dissemination and to ensure proper policing of use, papers and contributions become the legal copyright of the publisher unless otherwise agreed. Once accepted for publication, all authors are required to complete an online Journal Article Record form.

**Manuscript submissions**
Before considering submitting articles and papers for publication, please contact The Editor, Carol Baker for a copy of our *Guidelines for Authors*.

---

**Forthcoming papers in IT for CEOs & CFOs include:**

**Benefits of Leasing IT Equipment** – There’s no question that your business needs responsive, high-performing tech to do what it does, but do you really need to buy your devices outright? Leasing IT equipment is great for cash flow, and that it enables you to access the latest and greatest laptops, tablets and desktops easily and cost-effectively, but there are several other benefits of leasing IT equipment with which you may be less familiar.

**Redesigning Jobs in IT** – New research from international recruitment consultancy, Robert Half UK, shows that one-in-three (29%) employers are currently redesigning roles in direct response to the impact of the pandemic as they look to build more agile, adaptable workforces moving forward.