IT for CEOs & CFOs

ISSN 2054-3484

Volume 10 Number 1 & 2 2023

Why Digital Forensics and Incident Response must go remote
What CIOs Need to Know about Zero Trust
Overcoming the Barriers to Automating Your Cybersecurity
Knowledge Graphs Push the Boundaries of Data Science
With Great Power, Comes Great Responsibility (and Cooling)

Cyber Recovery Guarantee Marks New Era for Channel Sales Strategy

https://www.itceoscfos.com

All orders and subscription enquiries:
Telephone +44 (0) 1277 201554 or order online at www.creditcontrol.co.uk/_private/forms/subscribetocc.htm

Missing issue claims*:+44 (0) 1277 201554
* Missing issue claims will be fulfilled if claimed within four months of dates of despatch. Maximum of one claim per issue.

Reprint service enquiries:
Sally Williams, Editorial Assistant

Copyright permissions:
Carol Baker, Editor-in-Chief

Internet services available worldwide on URL https://www.itceoscfos.com

IT for CEOs & CFOs (ISSN 2054-3484)

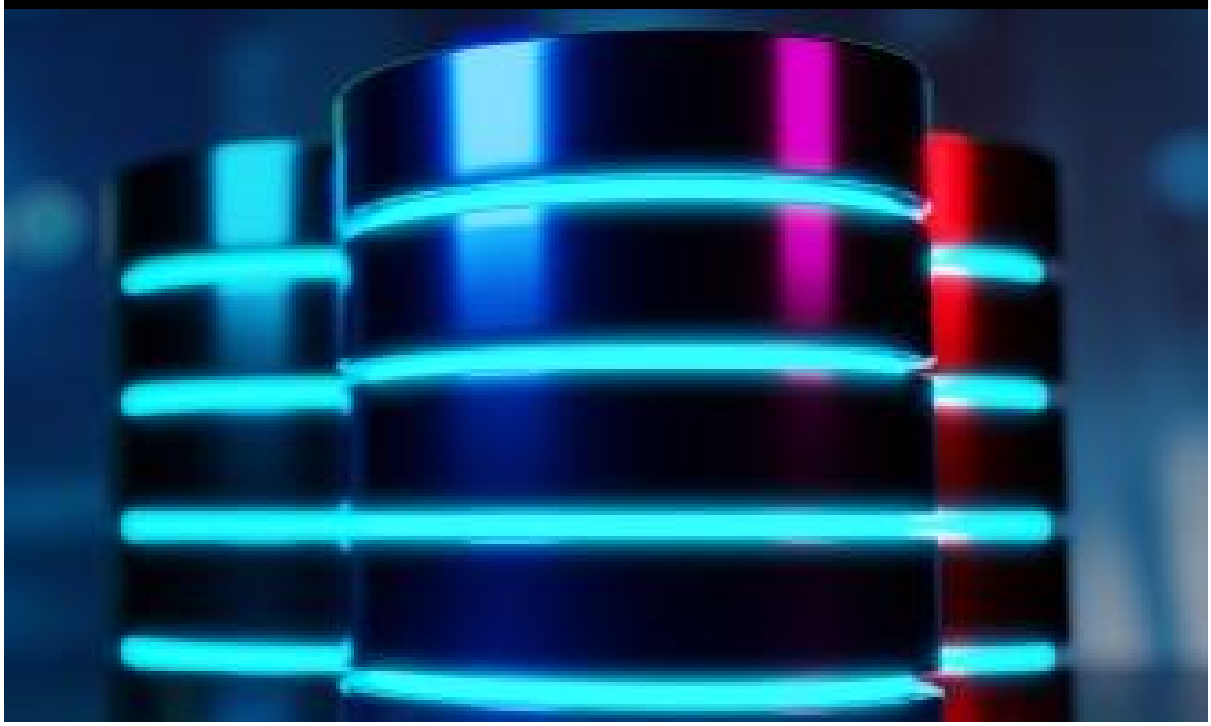
Published and Distributed by
House of Words Media Limited
7 Greding Walk
Hutton
Brentwood, Essex
CM13 2UF, UK

Tel: +44 (0) 1277 201554
E-mail: carol.baker@creditcontrol.co.uk
website: www.creditcontrol.co.uk

IT for CEOs & CFOs is abstracted and indexed in a wide range of academic and professional abstracting journals and on-line systems. A full list is available from the Editor-in-Chief.

Printed by

Cover Feature



Cyber Recovery Guarantee Marks New Era for Channel Sales Strategy

The rise of vendor guarantee programs is increasing, but if customers are going to use them to help make an enterprise storage purchase decision, it is important to really understand which program facets offer differentiating value and which are just baseline capabilities available from most vendors. Since debuting in 2015, storage vendor guarantees are commonplace. These days almost every vendor offers something to reassure its would-be customers. Some guarantees are clearly more valuable than others and when in the market for storage, today's enterprise buyers actively compare what is being offered when they evaluate suppliers. To guide end users in the right direction, IDC has published a detailed analysis of storage vendor guarantee programmes and this lists ten different areas of focus, from data reduction, storage media endurance, money back satisfaction and availability, to breadth of coverage and floor space reduction.

In Technology and Innovation ...

Why Digital Forensics and Incident Response Must Go Remote

Up to 90% of crime now features some element of digital evidence but discovering that information is becoming ever more challenging. There has been a proliferation in platforms, data formats and devices as we have become more dependent on technology, from our smartphones, to the Internet of Things (IoT) and the cloud, all of which has seen data become more disparate and dispersed. So when it comes to performing a covert investigation, for instance, to detect if a user has been stealing intellectual property, it's no longer a case of physically borrowing that laptop. Security teams now need to obtain remote access to that device and to scan and image it – all of which is making digital forensics increasingly more challenging.

Table of Contents

Editorial

RESEARCH PAPERS

Technology and Innovation

Data Centre and Virtualization

IT Security

Case Studies

Editorial

Cybersecurity risks rise as IT directors fear current IT estates cannot support hybrid workforces

Carol Baker
Editor-in-Chief

Last year, organizations globally witnessed incessant ransomware and other malware attacks and the IT industry is forecasting that cybersecurity attacks will become increasingly aggressive in 2023. Verizon's 2022 Data Breach Investigations Report reminded us how one key supply chain incident can lead to wide ranging consequences. Compromising the right partner is a force multiplier for threat actors.

Unlike a financially motivated actor, nation-state threat actors may skip the breach altogether and opt to simply keep the access to leverage at a later time. For this reason, Surya Varanasi, Chief Technology Officer, StorCentric says "Channel solutions providers and end users will prioritize data storage solutions that can deliver the most reliable, real-world proven protection and security. Features such as lockdown mode, file fingerprinting, asset serialization, metadata authentication, private blockchain and robust data verification algorithms, will transition from nice-to-have, to must-have, while immutability will become a ubiquitous data storage feature. Solutions that do not offer these attributes and more won't come even close to making it onto any organization's short-list."

But with research from managed workplace services provider, Apogee Corporation, citing over 70% of IT directors saying they are not placing IT investment at the top of their priority list for 2023, many are relying on existing IT estates which are unable to support hybrid workforces and prevent effective collaboration. Not only is this putting remote workers at a disadvantage, but it is also driving up cyber risks.

Likewise, consumer attitudes towards online security and privacy is heightening. "A key driver here will be that while enterprises getting hacked and hit by ransomware continue to make the headlines, cybercriminals have begun to hit not just enterprise businesses with deep pockets, but SMBs and individuals who are far more vulnerable to successful attacks as they do not have the level of protection that larger

enterprises have the budgets to employ," says Varanasi.

"Given that there have been several high-profile cases where scraping has harmed user privacy and simultaneously damaged the reputations of companies in recent years, it's never been more important for companies to learn how to effectively handle data scraping," adds Patiwat Panurach, Vice President of Strategic Insights & Analytics, NewtonX. "While internet platforms must remain open in order to be useful, that openness poses a risk to users and companies alike that their data can be automatically extracted for malicious purposes."

NewtonX surveyed more than 1,300 professionals specializing in data protection across industries to not only better understand the policies companies are using to prevent harmful data extraction, but to get a firm handle on best practices as well. The study found that while companies broadly recognize that personal user data must be protected, more than half don't have sufficient anti-scraping strategies in place. Therefore there needs to be more proactive best practices in place to effectively protect consumer data and preventing harmful data extraction in the wake of global data-scraping scandals.

Ideally cybercrime defence needs to be a layered defence that starts with a powerful password, and continues with Unbreakable Backup solutions says Varanasi. "These can provide users with two of the most difficult hurdles for cyber criminals to overcome: immutable snapshots and object locking to ensure that data cannot be deleted or overwritten for a fixed time period, or even indefinitely."

Apogee research shows that over a quarter of IT directors have reported that employees say they worry about cyber breaches when using sharing solutions, fearing that current technology stack is likely to not be up to standard. So, whilst work from home (WFH) and work from anywhere (WFA) has given the flexibility to help employees to attain the elusive work/life balance, it comes with serious security challenges which have the power to slow the progress and even knock some organizations off their IT transformation journeys.

Why Digital Forensics and Incident Response Must Go Remote

Harsh Behl

Harsh Behl
Director of Product Management (DFIR)
Exterro

Biography

Harsh Behl is Director of Product Management (DFIR) Exterro (https:/www.exterro.com). He is responsible for overseeing the entire product lifecycle of Exterro's forensic products.

Prior to joining Exterro, Behl was on the front lines working as an evidence analyst and forensic investigator, forensic consultant, and a technical engineer. His hands-on experience and expertise provide a unique perspective that results in the development of products that are easy-to-use, intuitive, and practical.

Harsh brings a wealth of experience, knowledge and technical skill sets, steering the vision and execution of Exterro's marketing-leading Digital Forensics and Incident Response technologies.

Harsh shares his insights in Exterro company blogs at https://www.exterro.com/blog

Keywords Digital forensics, West Midlands Police, FTK Central, Cloud, DFIR, Evidence, Defensible
Paper type Research

Abstract

Corporate digital forensics are proving harder to carry out with a remote workforce. When performing a covert investigation, for instance, to detect if a user has been stealing intellectual property, it's no longer a case of physically borrowing that laptop. Security teams now need to obtain remote access to that device and to scan and image it. By centralizing the data, it can be analyzed by a designated expert or segmented and sent to multiple teams all of whom may also be working remotely. By as the author of this article explains, digital forensics is becoming increasingly more challenging.

Introduction

Up to 90%[1] of crime now features some element of digital evidence but discovering that information is becoming ever more challenging. There has been a proliferation in platforms, data formats and devices as we have become more dependent on technology, from our smartphones, to the Internet of Things (IoT) and the cloud, all of which has seen data become more disparate and dispersed.

It's a situation made yet more complex by the sudden shift in working patterns. The Enterprise DFIR Benchmarking Report 2022[2] found half of those businesses that

took part had a workforce that was over 50% remote while close to a third had a workforce who were 75% remote, revealing that working from home is here to stay. This rise in remote working has forced organizations to adapt their policies and technologies and that includes how they conduct digital investigations.

Investigations are carried out for a myriad of reasons, from ensuring regulatory compliance or data security to incident response. The latter usually concerns some element of breach and it's estimated that over a quarter of employees[3] steal intellectual property when leaving a company. Moreover, a recent study by PWC[4] found almost a third of fraud cases are carried out by an internal perpetrator. Should such a breach occur, the security team must be able to quickly, remotely, and at times covertly investigate matters.

Remote reconnaissance

It's common practice in such circumstances to carry out an audit of the device, usually by requesting it be handed in for a routine security check. However, remote working now makes it impossible to physically access the device, which means the investigating team need to obtain remote access to scan and image it. This requires access both on and off the corporate network so that data can be captured irrespective of whether the device is logged on to the VPN. Live data can then be captured directly at the endpoint the moment it connects to the internet, and should that connection be lost, the capture is paused and resumed when the connection is re-established.

According to the DFIR report, organizations routinely investigate between 25-30 devices per month with some analyzing up to 350, making digital forensics and incident response (DFIR) time consuming and costly. Yet very few of these businesses had in place well defined, repeatable, managed, and optimized processes for handling remote digital forensics and incident response (DFIR). This suggests there's a real need to streamline and automate these workflows.

The automation of web-based review such as key word searching, tagging, and labelling was seen as a key objective by 40%, followed by endpoint collection and evidence processing by 20%, and then case creation and case management. But further advances in workflow automation are expected to help organizations adapt to the new normal of remote working. These include the use of machine learning to extract non-relevant data before assigning for review, integrated visualizations (including timelines, maps, charts and social communications analysis, along with image recognition), and cross-evidence insights that will flag possible causal connections.

The report found that most of the businesses that had a mainly remote workforce already had a Security Information and Event Management (SIEM) and/or Security Orchestration, Automation and Response (SOAR) solution in place but only 6% had integrated this with their DFIR solution. Doing so enables the business to capture and preserve evidence automatically on endpoints at the very moment that an intrusion or anomalous event occurs, which ensures evidence is collected 24/7.

The growing need for collaboration

Yet one of the biggest challenges of carrying out digital forensics and incident response with a remote workforce is in fact a people problem: the facilitation of cross-team collaboration. While the majority (77%) of those questioned reported occasionally or routinely collaborating on cases, 23% still work independently. Over half of the respondents said they have or would like the ability to share cases with reviewers outside their organization, such as legal counsel or third parties, indicating that technology supporting even broader collaboration would be welcome.

Such collaboration is likely to become more pressing as we go forward, given the shortage of skilled investigators, as this will allow the business to draw upon expertise from further afield. Centralizing the data will allow it to be analyzed by a designated expert or segmented and sent to multiple teams. Indeed, it's now becoming increasingly common for different departments across the business to get involved, with HR, compliance, and legal playing a more active role in data preservation, as well as collection and analysis as part of investigations.

However, involving these teams makes it even more vital that automated processes are in place to preserve the evidence correctly in the chain of custody. This is driving demand for integrated tools that enable and foster collaboration without requiring unnecessary data movement. The conventional approach sees data pass between platforms and tools, risking corruption or potential loss as well as elongating the time to resolution. In contrast, a single data store ensures that data doesn't have to move between separate, disparate platforms, and products, thereby minimizing risk to the chain of custody.

The move to take digital forensics remote is not just limited to the corporate sphere, however. The gathering of digital evidence is of course also key in law enforcement which is struggling to cope with a backlog of data. A recent report[5] by His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) revealed that more than 25,000 devices are still waiting to be processed and the report also flagged the need for a national lead/programme of improvement as well as the shortage of trained digital media investigators.

Police priorities

Law enforcement have three asks when it comes to Digital Forensics. To provide front line officers with the ability to review evidence, taking the pressure off investigators. To move from on premise to in the cloud with a secure defensible process. (There is no national blueprint on how to achieve this, leaving police forces to make the decision for themselves which has been daunting) – and finally, to automate as much of the workflow as possible and provide a scalable resource.

At the present time, forces are having to balance out the infrastructure, training, and cost of implementation against the advantages of transitioning to an automated suite. They recognize the value of being able to review their data from anywhere without the geographical constraints of getting data to the Digital Forensics Unit, can see the advantages of more powerful processing and moving from a CapEx to a subscription model but are unsure of how to do so.

The overarching concern has been how to store data in a legally defensible manner. But a testbed implementation has now paved the way in this regard. The West Midlands Police (WMP) has now rolled out a digital forensics solution in the cloud which sees FTK Central hosted over Microsoft Azure and its proved ground-breaking, significantly reducing the time and costs associated with reviewing evidence.

The project demonstrates the viability of a cloud-based solution but also the benefits of using a single platform. Up until recently, police forces have been using

five or six tools, but this makes it complicated for accreditation with the ISO 17025 standard that they are legally obliged to comply with. It's also harder for the reviewer, who will need to learn how to use a range of products, plus the force is also saddled with mounting software licensing costs. In contrast a single platform that can integrate with other software can cover all the standard operating procedures in ISO 17025 while providing efficiency gains, seeing the pendulum swing back in favour of an integrated workflow.

Alleviating the burden on investigators

The WMP project has revealed how bringing investigators into the workflow can relieve some of the burden that specialist investigators must bear. The front-line officers don't need to make determinations over the relevance of that data, as the software parses out that data and presents it to them to review but this does prevent investigators from becoming bogged down by data collection. If the review findings are brought into question, an investigator can then use their specialist skills to establish relevance, although this is rare as most digital evidence is accepted as fact by the defence or is met with a guilty plea at trial.

For police forces the journey from business case to implementation will undoubtedly be a long one. But the demand is now materializing from multiple directions, with enquiries coming from different elements of policing, investigators wanting immediate access to the data and specialists wanting to use their time in a targeted way. Many forces are bound by vendor agreements lasting three or four years with respect to ISO 17025 but as those contracts come up for renewal, we can expect these divisions to reconsider their options and to look to make a change, whether that be through automation, remote review or cloud hosting.

What the experiences of those operating in the private and public sectors reveals is that DFIR is now on the cusp of substantial change. There's a real need to be able to collect, process and review digital evidence remotely, in near real-time, and using defensible processes. But this will also facilitate the kind of collaboration between teams necessary to expedite processing and drive down data backlogs, ultimately leading to speedier resolutions.

Reference

1 House of Lords (1 May 2019), Forensic science and the criminal justice system: a blueprint for change. House of Lords Science and Technology Select Committee. Available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/333.pdf

2 Exterro (2022), Enterprise DRIF Benchmarking Report. Exterro. Available at: https://exterro.com/resources/2022-enterprise-dfir-benchmarking-report

3 Biscom (16 April 2021), Enterprise Data Protection. Biscom. Available at: https://www.biscom.com/employee-departure-creates-gaping-security-hole-says-new-data/

4 PwC's Global Economic Crime and Fraud Survey 2022. PwC. Available at: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

5 An inspection into how well the police and other agencies use digital forensics in their investigations (1 December 2022). His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS). Available at: https://www.justiceinspectorates.gov.uk/hmicfrs/publications/how-well-the-police-and-other-agencies-use-digital-forensics-in-their-investigations/

Knowledge Graphs Push the Boundaries of Data Science

Maya Natarajan

Maya Natarajan
Senior Director Product Marketing
Neo4j

Biography

Maya Natarajan is Senior Director Product Marketing at native graph database leader Neo4j (https://www.neo4j.com).

Responsible for knowledge graphs at Neo4j, Maya is passionate about bringing different technologies together to solve complex problems. At Neo4j, Maya is championing the use of knowledge graphs to bring context to various systems. Maya has positioned technologies from Blockchain to Predictive & User-Based Analytics to Machine Learning to Deep Learning to Search to BPM and beyond in a myriad of industries at various small and large companies.

Maya started her career in the biotechnology area where she was in R&D focusing on cardiovascular drugs, and she has five patents to her name.

Keywords Knowledge Graphs, Graph databases, Artificial Intelligence (AI), Data analytics
Paper type Research

Abstract

Defined by The Turing Institute, the UK's the national institute for data science and artificial intelligence, as the best way to "encode knowledge to use at scale in open, evolving, decentralized systems," Knowledge Graphs[1] are a big trend in the advanced data science world, but they aren't as widely known as they could be. In this article, graph database expert Maya Natarajan asks: Does the real magic of knowledge graphs come into play when they are used to get the best from machine learning?

Introduction

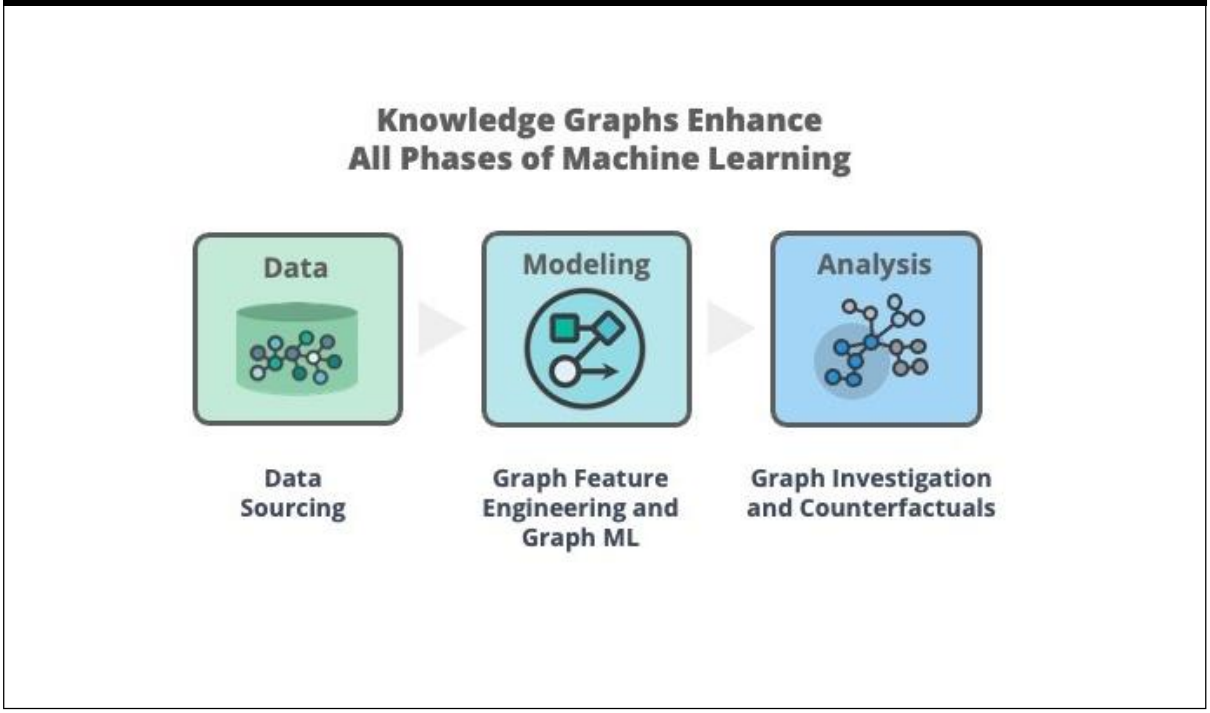
Organizations are increasingly using Artificial Intelligence (AI) for decision-making. However, due to a lack of contextual information, such systems have not yet been able to achieve their full potential as reliable ways to find solutions for complex business and social problems.

Recently, we asked 100 senior tech executives – CIOs, CTOs, and Chief Data Officers – what they think they need to solve this problem. A massive 88% said the same thing: knowledge graphs.

Given that these executives represent large organizations across verticals using graph technology for a wide array of use cases, something's clearly going on. If

you are not familiar with the term, 'knowledge graphs' are a proven way to capture data relationships and convey their meaning. Knowledge graphs are defined by Stanford University[2] as "a compelling abstraction for organizing world's structured knowledge over the internet, and a way to integrate information extracted from multiple data sources".

Figure 1: Knowledge Graphs enhance all phases of machine learning



That's a good definition, for knowledge graphs drive intelligence into the data itself in many ways. They give AI the 'context' it needs to be more explainable, accurate, and repeatable. Knowledge is every company's most prized asset. Its value is limited, however, unless organizations can leverage that knowledge in the correct context. While neither AI/machine learning (ML) or knowledge graphs are new technologies, it's only lately that they have come of age to derive that context.

The powerful combination of the two is spurring an explosion of interest in Contextual AI. Machine learning is enhanced using knowledge graphs because of their innate ability to reveal context. Contextual information is known to increase predictive accuracy. Context also makes decisioning systems more flexible and it provides a framework for tracking data lineage.

This is where knowledge graphs come into play. A knowledge graph places data in context by establishing connections among data. A knowledge graph enriches the data's meaning and utility by adding a layer of semantics, thereby allowing software agents to reason about it. By adding relationships to data and enhancing it with semantics, knowledge graphs drive intelligence into data, making it smarter.

That's useful, as machine learning is used in every industry. In healthcare, it's being used to better detect cancers. In supply chains, to find factors that positively and negatively impact business. In financial services, ML is used to allow investors to identify new opportunities or know when to trade.

Why data scientists give up too easily on context

Unfortunately, most current data science approaches leave out contextual information. Connections are difficult to process in standard relational databases. However, knowledge graphs capture and make this contextual information usable, as they utilize graph data structures. They can enhance every step of the machine learning process – from data sourcing and training machine learning models to analyzing predictions and applying results. Contextualized AI systems end up more reliable, robust, explainable, and trustworthy. If you can't trust the data used for ML, you can't trust the results, after all.

In the initial step of data sourcing, knowledge graphs are used for data lineage to track the data that feeds machine learning: knowledge graphs track where the data came from, how the data changed, where the data is used, and who used it. Data lineage and master data management using knowledge graphs also serve as an audit trail for compliance, especially in regulated industries.

The next phase is training a machine learning model. This involves providing an ML algorithm with training data and significant features to learn a function for making predictions. Machine learning models without context require exhaustive training, strictly prescriptive rules, and can only be applied to specific applications. Knowledge graphs also allow graph feature engineering using simple graph queries and/or more complex graph algorithms. We know that relationships are highly predictive of behaviour, so using these connected, contextual features maximises the predictive power of models while increasing how broadly a solution can be applied.

Once a machine learning model has been developed, it is essential to understand if it is useful and makes correct predictions. Knowledge graphs with incorporated relationship information allow for easy graph investigations and counterfactual analysis. A domain expert might test hypotheses by exploring similar communities in the knowledge graph. They might also question odd results by drilling into hierarchies and dependencies.

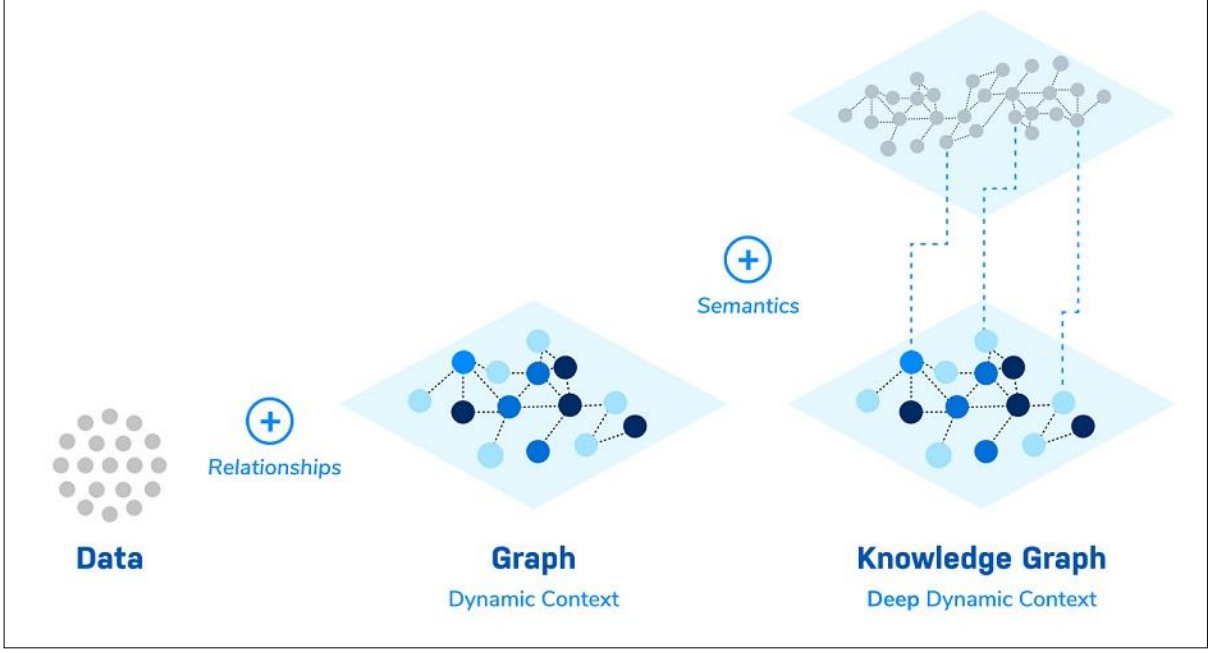
Knowledge graphs built on graph technologies have significant advantages as graphs naturally store, compute and analyze connections and relationships among data. Moreover, graph algorithms are specifically developed to leverage the topology of data through connections. The algorithms find communities, uncover influential components, and infer patterns and structure. Incorporating the predictive elements of context from a knowledge graph into machine learning not only increases accuracy but reduces false positives.

Leveraging knowledge graphs with machine learning

Graph-native learning involves computing machine learning tasks within a graph structure. It takes knowledge graph augmented machine learning to the next level.

It provides the ability to learn generalized, predictive features directly from within the graph. You needn't know what data structures are most predictive. This is significant, as organizations don't always know which features are most important. Organizations also don't know how to represent connected data for use in machine learning models: again, knowledge graphs help.

Figure 2: Knowledge Graphs provide deep dynamic context



Neo4j users today are leveraging knowledge graphs with machine learning for many use cases. Such use cases include enhancing heuristics to more complex uses like training embeddings in a graph-native learning model. A global e-commerce leader that has created a shopping bot to add context to machine learning to make better heuristic decisions about user intent. Finally, a global pharmaceutical company that is combining a knowledge graph, graph queries and graph algorithms with traditional ML approaches to map and predict patient journeys.

AI-enhanced knowledge graphs are driving the next wave of competitive advantage for companies that use them together successfully.

Reference

[1] The Alan Turing Institute, *Knowledge graphs - How do we encode knowledge to use at scale in open, evolving, decentralized systems?* Available at https://www.turing.ac.uk/research/interest-groups/knowledge-graphs

[2] Stanford University, *Knowledge Graphs - What should AI know?* Available at: https://web.stanford.edu/class/cs520/2020/notes/What_is_a_Knowledge_Graph.html

Cyber Recovery Guarantee Marks New Era for Channel Sales Strategy

James (JT) Lewis

James (JT) Lewis
Channel Director,
EMEA & APJ
Infinidat

Biography

James (JT) Lewis is the Channel Director, EMEA & APJ, Infinidat (https://www.infinidat.com). He is an experienced international Sales Director with a proven track record in the enterprise IT, storage, and network security industries.

His broad industry experience includes roles involving cyber security, Storage Area Networks (SAN), enterprise storage, IT service management, IT strategy, professional services, cloud computing and virtual computing environments. Based in Frankfurt, Lewis will have responsibility for Infinidat's EMEA and Asia Pacific regions, including Japan. Lewis served in the US Military before embarking on his technology sales career.

Most recently, he worked for Data Interchange as Head of Channel Sales and was the Strategy and Growth Officer for Altdata Technology Solutions, focusing on the cyber security market. He also spent 15 years at EMC and RSA, based in London and Frankfurt, where he built up comprehensive experience in the recruitment, enablement, and leadership of channel partners and distributors.

James blogs at https://www.infinidat.com/en/blog

Keywords Vendor guarantee programs, Procurement, Cyber resilience, Enterprise-class storage systems
Paper type Research

Abstract

The rise of vendor guarantee programs is increasing, but if customers are going to use them to help make an enterprise storage purchase decision, it is important to really understand which program facets offer differentiating value and which are just baseline capabilities available from most vendors explains the author of this article.

Introduction

Since debuting in 2015, storage vendor guarantees are commonplace. These days almost every vendor offers something to reassure its would-be customers. Some guarantees are clearly more valuable than others and when in the market for storage, today's enterprise buyers actively compare what is being offered when they evaluate suppliers.

To guide end users in the right direction, IDC has published a detailed analysis of storage vendor guarantee programmes[1] and this lists ten different areas of focus, from data reduction, storage media endurance, money back satisfaction and

availability, to breadth of coverage and floor space reduction. Its author and a big proponent of guarantee programs, Eric Burgener, research vice president, Infrastructure Systems, Platforms and Technologies Group at IDC, believes they can offer real value for customers. In his June 2021 report on storage vendor guarantee programmes, he says that provided customers understand which program facets offer differentiating value and which are just baseline capabilities available from most vendors, guarantees can reliably be used to help inform enterprise storage purchasing decisions.

As IT has become more critical to day-to-day business operations, availability requirements have been on the rise. Most enterprise-class storage systems are marketed as supporting at least 'five-nines' availability, which translates as 99.999% uptime, or roughly five minutes of downtime in an 8,760 hour year. Many support 'six-nines' and Infinidat is one of just four vendors offering a 100% data availability guarantee on a single storage array. However, although a 100% data availability guarantee indicates that the vendor stands behind their system reliability, it cannot replace data lost after a ransomware attack.

Until now, none of the guarantees offered to date have specifically addressed cyber resilience and the threat of ransomware, yet this is one of the most critical risks facing enterprise users today. We all know that the level of cyber threat today is so high that it is not a case of 'if' there's an attack, but 'when'. Enterprises need to be

expecting that their data will be breached at some point, and they need a rapid recovery plan in place to mitigate the effects. Rather than worrying about simply keeping intruders out, the key question needs to be 'how quickly can you recover compromised data and avoid reputation risks or business downtime?'

It was with this thinking in mind that Infinidat introduced its cyber security guarantee, described by Eric Burgener at IDC as a 'game changer'. Channel partners focused on the storage sector should take note of its arrival because it expands the sphere of buying decision influencers and potentially creates a new, lucrative business opportunity.

Cyber resilience is such a big threat that many enterprises now employ a Chief Information Security Officer (CISO) and their recommendations will accompany those of the Chief Technology Officer (CTO), and the Chief Information Officer (CIO) when purchasing decisions are made. Storage is a highly collaborative buy and although the CISO is not usually a budget holder, they are an important influencer and so presenting a cybersecurity guarantee during negotiations could be the differentiator that tips the scales. Just consider all the digital first businesses for whom a ransomware attack could mean a drop-in service to appreciate why CISOs need to be included in your messaging.

Apart from the potential to reach a new influencer, how else does the cyber recovery storage guarantee translate into a business opportunity for the channel?

It's another feature driving the overall improved CX now expected as standard by enterprise storage buyers.

Cybersecurity it is all about recovery, minimizing any service disruption and being able to get back online as quickly as possible. For any enterprise planning to deal with a cyber threat, they should understand that a breach is bound to happen. It's not just about prevention, recovery time and general preparedness is what matters.

These issues are important for channel sales to understand because discussions about cyber resilience do not involve the traditional personas as when selling storage. Storage industry vendors need to be acknowledging the importance of cybersecurity and moving away from simply talking about performance, to offering guarantees that are more practical and helpful, designed to support current industry issues. We believe Infinidat's new cyber resilience guarantee is the first of a new era.

Reference

[1] Burgener, E (June 2021), How to Evaluate Enterprise Storage Vendor Guarantee Programs, IDC. Available at: https://www.idc.com/getdoc.jsp?containerId=US47768121

With Great Power, Comes Great Responsibility (and Cooling)

Darren Watkins

Darren Watkins
Managing Director
VIRTUS Data Centres

Biography

Darren began his career as a graduate Military Officer in the RAF before moving into the commercial sector. He brings over 20 years experience in telecommunications and managed services gained at BT, MFS Worldcom, Level3 Communications, Attenda and COLT. He joined the VIRTUS (https://virtusdatacentres.com) team from euNetworks where he was Head of Sales for the UK, leading market changing deals with a number of large financial institutions and media agencies, and growing the company's expertise in low latency trading.

Additionally, he sits on the board of one of the industry's most innovative Mobile Media Advertising companies, Odyssey Mobile Interaction, and is interested in all new developments in this sector. Darren has an honours degree in Electronic and Electrical Engineering from University of Wales, College Swansea.

Darren has an honours degree in Electronic and Electrical Engineering from University of Wales, College Swansea.

Keywords Power, Cooling, Data centre, Sustainability, Efficiency, Performance, Power usage effectiveness (PUE)
Paper type Research

Abstract

Data centres account for 1% of the world's total electricity usage each year, and by 2030 this is set to rise to around 3-13% with much of the power going into cooling servers and systems according to research conducted by Huawei Technologies. With the demand for cloud services, edge computing, IoT, artificial intelligence (AI), and other digital transformation technologies taking hold and hybrid workforces continue to develop, the need for efficient and sustainable data centres is increasing. In this article, the author discusses exactly why power and cooling are a crucial consideration for efficiency and performance in data centres.

Introduction

While data centres don't generate waste like other industries, this high energy – and high water-use sector faces unprecedented demand for sustainability measures, use of clean energy and efficient facilities. Although necessary to create the optimum environment for servers housed in a data centre, it's the power and cooling that consume the most water and energy, making them a crucial consideration for efficiency and performance, and whilst a laser focus on sustainability is key to the future of the data centre industry, it is not a new priority.

For several years we have recognized the need to produce more efficient data centres, with increasingly lower Power Usage Effectiveness (PUE) and Water Usage Effectiveness (WUE) designs to ensure that not only can we deliver a premium service to our customers, cost efficiently, we are also extremely aware that we must continue to achieve our own ambitious sustainability goals.

Power

Collectively, our sector uses a huge amount of power and generates a vast amount of heat due to computational demands. Data centre power consumption alone amounts to around 416 terawatts, or 3% of all electricity generated on the planet. So, when it comes to energy use, at VIRTUS we are leading the way in UK data centre sustainability.

Carbon neutral is the stated position of many providers, but we have gone a step further and are committed to using 100% carbon zero energy sources, helping our customers to meet environmental goals whilst also providing efficiencies through cost savings and increased reliability.

All of the energy consumed at our facilities is from 100% renewable sources thanks to partnerships with companies like Bryt Energy who only procure power from wind, solar and tidal sources. This saves around 45,000,000 tonnes of CO2 every year, which is enough to fill Wembley Stadium five times over.

We've also had great success with regards to minimizing PUEs. We strive to produce a 1.0x PUE and, according the Uptime Institute's annual survey[1], our PUEs are well below the 2020 average of 1.58x. To put it into context, all operators try to get the PUE ratio down to as near to 1.0x as possible, with most new builds falling between 1.2x and 1.4x.

Cooling

Cooling is the most power-hungry component of cloud and data centre management. On average, as much as 40% of a facility's electricity consumption goes towards cooling the servers. By increasing the efficiency of cooling systems, the data centre's environmental impact can be reduced.

We have been particularly innovative when it comes to cooling. Since 2014, we have been operating LONDON2 (certified to UTI Tier 3) using exclusively indirect evaporative cooling technology, which provides cooling with a very low energy use. When it was designed and built, we also included water sourced from a natural underground aquifer to minimize usage of mains water. At other VIRTUS sites, rainwater harvesting, and reuse of heat waste are common features as well as liquid cooling (we had our first liquid cooled customer racks back in 2015).

LONDON4

It was as far back as seven years ago when we first deployed adiabatic cooling. With the de-carbonization of the grid, the purchase of accredited green energy, innovation in compute and mechanical cooling, we don't see a need to use additional valuable natural resources, for instance, water, to cool. Instead, we use a closed loop chilled water system, with little to no impact on the environment driven by energy which is derived only from renewable sources. This enables us to still achieve the same PUE or less.

When it comes to the cooling demands of Hyperscale Data Centres, the requirement tends to favour chilled water-cooling systems, where the water impact is negligible. This is because once a system is operational, only limited amounts of top-up water are required. Chilled water systems have significantly improved in terms of energy efficiency with the increase in 'free-cooling' capability for instance, using ambient outside temperatures for cooling.

While cooling is a vital part of keeping data centres up and running, a recent Uptime report estimated that in the US alone nearly 12.5 billion kW hours would be wasted by over-cooling in data centres and improper airflow management. This points to a wider trend of energy waste in the sector, including "zombie servers" and a significant amount of retired equipment being sent to landfill rather than recycled. To tackle this, we not only invest in comprehensive recycling schemes, but we also use highly efficient UPS (uninterruptable power supply) systems which can hibernate parts of the system when they are not being used.

Running the digital economy

This kind of constant innovation is possible because we have a team within VIRTUS Operations who have a cycle of continuous improvement. For example, they review customer data halls and manually adjust airflow or containment. This "cycle of review and optimize" uses techniques that we have developed over years of operational experience to improve data centre efficiency.

We are proud to be the UK leader in an industry that has become one of the most crucial components of business infrastructure in the modern world. We are responsible for storing and processing vast amounts of information needed to run the digital economy – if data centres don't work, businesses won't be able to operate . At VIRTUS, we have spent over ten years working with supply partners and customers to innovate, enhance product development and ensure that we're providing Operational Excellence to all our customers – something we continue to do now and in the future.

Reference

[1] Ascierto, R. and Lawrence, A (20 July 2020), 2020 Data Center Industry Survey Results, Uptime Institute. Available at: https://uptimeinstitute.com/2020-data-center-industry-survey-results

What CIOs Need to Know about Zero Trust

Nathan Howe

Nathan Howe
Vice President of
Emerging Technology
Zscaler

Biography

Nathan Howe is Vice President of Emerging Technology at Zscaler (https://www.zscaler.com).

As a digital transformation and telecommunications expert, he has assisted hundreds of enterprise customers seamlessly modernize their environments adapting to distributed workforces cloud migrations and standing up private 5G networks.

He has more than 20 years of experience in the security industry and previously worked for Nestle and Verizon. He now sets the strategic direction of Zscaler.

Nathan is a regular book author having co-authored several books including: SSE eBook: https://www.zscaler.com/resources/ebooks/selecting-an-SSE-solution.pdf, ZeroTrust book and eBook v1: Published April 2022; ZeroTrust book; and eBook v2: Published August 2022: https://www.zscaler.com/resources/ebooks/seven-elements-of-highly-successful-zta.pdf.

Nathan blogs at https://www.zscaler.com/blogs

Keywords Cybersecurity, Zero-trust, Security, Investment, Infrastructure, Transformation, SSE
Paper type Opinion

Abstract

Zero trust is a cybersecurity strategy wherein security policy is applied based on context established through least-privileged access controls and strict user authentication – not assumed trust. This guiding principle of "never trust, always verify" has been in place since John Kindervag, then at Forrester Research, coined the term. Many Chief Information Officers (CIOs) mistakenly assume that they can leverage their existing IT security infrastructure to introduce zero trust protection. But as the author of this article explains, what CIOs need is a modern approach if they want to harness the full potential of zero trust.

Introduction

CIOs must learn to trust this strategic approach to security – and, eventually, say goodbye to traditional security hardware once and for all. The first thing that a CIO needs to understand about zero trust is that it is not a product, but a strategic approach to security. Forrester first proposed the concept of zero trust in IT security back in 2010. Since then, the initial idea has been developed by other parties; Google fleshed out the concept in its 2014 "Beyond Corp" strategy, and further

refinements were added by Gartner and the National Institute of Standards and Technology (NIST) from 2017 onwards. It was NIST that coined the acronym ZTA (zero trust architecture), and the organisation has published guidance documents that describe the disruptive approach – which is fundamentally different from traditional perimeter protection.

Rethink required

In a traditional, data-centre-based security setup, hardware appliances were stacked in racks. With each new security requirement came a new security appliance, with companies ultimately tying themselves up in an intricately woven web of firewalls, VPN gateways, load-balancers, and Denial of Service protection. As each new component was added, the infrastructure became more and more difficult to manage. As data centres relocated to the cloud, these concepts were frequently transferred across to the virtual realm and implemented in all cloud zones or with multi-cloud partners. This approach not only increased complexity and sent the number of security instances skyrocketing; it also increased the organization's attack surface risk, as many of its these components were visible online and therefore vulnerable to attack. Zero trust, on the other hand, reduces complexity and "hides" systems to slash the risk of an attack.

Driven by the shift towards the cloud and hybrid working models, data and applications are no longer solely hosted in data centres, and employees no longer only on company networks; they need to be able to access their work from any location. Accordingly, zero trust does not begin by connecting users to the

traditional company network. Instead, its goal is to provide a secure and high-performance connection to the applications that an employee requires – without placing the user on the network at all, and regardless of whether the application is hosted in a data centre or a multi-cloud environment.

These days, it is easy for CIOs to profile themselves as enablers of cloud transformation, as multi-cloud environments have become part of day-to-day life. But there is a lot of catching up to do when it comes to the security transformation that goes hand in hand with the shift in how we access applications and structure our workplaces – and it requires a fundamental rethinking of security.

Here are a few of the main considerations for any organization embarking on their zero trust journey.

Simplify or upgrade?

Just like the shift from combustion engines towards electromobility, switching to a fully zero trust-based approach requires a fundamental change in thinking. It takes a great deal of courage to gradually step away from the network-centric security infrastructure that has been built up over the course of many years. So, it comes as no surprise that many CIOs first attempt to upgrade their existing infrastructure in response to evolving requirements. But, trying to combine zero trust with traditional security hardware simply relocates problems without ever really solving them – just like when a “lift and shift” strategy moves existing weaknesses to the cloud rather than tackling the root cause of the problem. The performance and user experience provided by traditional virtual private network (VPNs) and legacy hub and spoke network architecture cannot match the standards achieved by the secure, high-performance application access of zero trust. Zero trust renders VPNs, which are often associated with poor performance and increased security risks, completely obsolete.

As traditional security hardware is gradually phased out, it can be replaced by a simplified, platform-based model offering security services and a central management platform. Rooms stacked high with appliances – and the administrative complexity they bring – become a thing of the past with a cloud-based Security Service Edge (SSE) approach built on zero trust principles.

Lightweight software on the client, and adjacent to the server in the data centre or in the cloud, replaces the traditional appliance stacks and ensures that all data streams, access rights, and policies can be brokered on a single security platform. This means that zero trust reduces the need for maintenance and, in turn, operational expense. The bottom line? Zero trust replaces the complexity of old with a new, easy-to-manage approach to security – an approach that focuses on the administration of rules for application access, monitoring data streams, and preventing unwanted access to or disclosure of data.

Investment protection or added value transformation?

This radical change can initially be difficult for network and security teams to accept, all the way up to CIO level, because protecting investments is always high on the agenda. Companies want to see their investments in security hardware and IT staff training pay off. Often, write-downs need to be finalized and business cases must be completed successfully before new approaches are evaluated. The CIO also needs to get to grips with the transformation of the business model that is inevitable when infrastructure is taken out of house. IT administrators will need to acquire new skills, and the centralised, platform-based mode of operation will consolidate the business model significantly.

The zero trust access (ZTA) approach gives security teams an insight into all data streams in a single management console. This paves the way for secure digitalization, as even traditional operational technology (OT) or industrial internet of things (IIoT) environments can be secured with zero trust. This holistic approach not only provides users with remote access to applications, but also provides an interface for connecting external parties or technologies and enables external parties to access production environments to perform maintenance.

Infrastructure exposed online or reduced vulnerability to attack?

The most important result that can be achieved with the implementation of zero trust – alongside providing high-performance and secure access to applications – is to effectively eliminate the external attack surface. A traditional infrastructure of firewalls, proxies, and VPN gateways needs to be exposed online in order to work; however, this mode of operation also makes it vulnerable to attack.

Over the past two years, we have all witnessed how vulnerable infrastructures and web services are when malware attackers exploit weak links that have been exposed on the internet. But attackers can't exploit what they can't see. The Log4J vulnerability is just one example of a security concern that caused widespread panic in IT teams around the world as they rushed to patch susceptible systems. Zero trust organizations, on the other hand, could afford to adopt a more laid-back approach, taking their time to decide how to respond. Of course, the vulnerability affected them too – but because their systems were not exposed online, they were able to update the affected servers in their own time, without worrying about getting to the weak link before the hackers.

A zero trust architecture provides effective protection against ransomware attacks because it also addresses other vulnerabilities, that could potentially be exploited by hackers. In particular, it effectively prevents attackers from moving laterally across systems, jumping from the infected system to the next target. The approach has a similar effect to micro- or nano-segmentation, directly connecting the user to

their application to prevent other systems from being infected and, by extension, stopping attackers from causing large-scale system failures.

From operational responsibility to business enabler

Compared to the pre-digitalization, pre-IT cloudification era, today's CIOs have a totally different role to play in their companies. Their job is no longer just about keeping IT infrastructure running; it's about achieving the company's objectives, with IT often playing the role of enabler. The value of the new role of IT became clear to all of us at the start of the pandemic. IT teams were required to perform the dual role of keeping operations running while also optimizing business processes, all as employees left the office in droves to work from home due to new social distancing regulations. With IT not only providing secure, high-performance remote access to all systems, but also helping to transform the company's core business, management naturally began to realise the value of the domain.

Mergers and acquisitions are another area that highlights why IT – and zero trust – make such a crucial difference to companies. When a company acquires another business, time-to-value is a critical parameter of value creation. For this to work, two separate IT structures need to be merged to enable secure, bilateral communication – and this needs to happen as quickly and securely as possible.

A zero trust exchange platform can provide secure access to dedicated applications in another network from day one. For example, the SAP or Oracle ERP system, or HR functions, might be made available first; selected employees can be given secure, rules-based access to the system they need using zero trust technology, without needing to join networks or link AD domains. Further down the line on day X, once the contract between the two companies has been finalized, IT can easily enable additional access to applications. Employees can work securely via the zero trust exchange platform, without either side being directly connected to the other company network.

Relocating applications to the cloud and making use of SaaS has become part of day-to-day life, yet security transformation is lagging behind. Opting for a platform-based zero trust concept is a way to holistically protect all a company's digital assets and enable secure business process transformation. The modern, cloud-delivered zero trust platform is continually enhanced, ensuring that any necessary adaptations are made quickly – and providing a sustainable, long-term solution that offers a whole host of benefits for its users.

Overcoming the Barriers to Automating Your Cybersecurity

Yann Le Borgne

Yann Le Borgne
International Vice President of Threat Intelligence Engineering
Threat Quotient

Biography

Yann Le Borgne, International Vice President of Threat Intelligence Engineering, Threat Quotient (https://www.threatq.com/) and is a specialist in Cyber Security with over 15 years of experience. He joined ThreatQuotient in January 2016.

Before ThreatQuotient, Yann was in charge of a technical team of 12 people across Southern Europe at Sourcefire which have been acquired by Cisco.

Yann blogs at https://www.threatq.com/resources/

Keywords Automation, Cybersecurity, XDR, Orchestration, Detection, ThreatQuotient, Threat intelligence
Paper type Opinion

Abstract

The phrase "automation" has gained traction in the cybersecurity community. However, the benefits of automation are not being realized by businesses due to a lack of money, time, and trust in the results. In this article, the author explores these issues and looks at how confusion around the meaning and potential of "automation", "orchestration" and "XDR" may be a barrier to implementation and offers insight for organizations on where to start so they can resolve pain points and achieve cybersecurity automation success.

Introduction

"Automation" has become a buzzword in cybersecurity circles. That is not surprising in an environment where security specialists are in short supply and under intense pressure to defend the business against a huge variety of threats from innumerable different sources. Using technology to do at least some of the work seems like a no-brainer. Nevertheless, it seems that organizations are finding it hard to get the right approach to cybersecurity automation. Threat Quotient conducted research last year that found resources, time, and a lack of trust in outcomes are preventing companies from realizing the benefits of automation. In a recent webinar, myself, Nabil Adouani, CEO of Strange Bee and co-founder of The Hive Project, and our Global VP of Threat Intelligence Engineering Chris Jacobs discussed the current state of automation, the expectations around what automation can achieve, and what this means for implementation in the real world.

From automation to orchestration and XDR – all sides of the same coin?

One of the challenges around automation is defining what we mean by the term, and where it differs from orchestration. Really, automation is anything that replaces a manual human-driven activity with a computer-driven alternative. It has applications across the technology sector wherever there is a repetitive manual task that would be better done by a machine that never gets bored or makes mistakes.

In the incident response area of cybersecurity, automation can be used at any stage of the process. Examples include ingesting alert data, enrich alerts, and even automating elements of response. Often automation and orchestration seem to be used interchangeably, but there should be a distinction. Automation is the conversion/adaptation of a single manual process to be completed by machine, whereas orchestration is applied to a multi-stage workflow involving multiple different tools, which are automated and brought together to execute a process.

When it comes to XDR, there is further uncertainty around what this means. Analyst company Gartner suggests that XDR should have a minimum of three elements, such as endpoint detection and response, security incident and event management, and incident response capabilities on your platform. This would constitute XDR and orchestration could also be part of coordinating a series of automated actions based on the technology capabilities of the platform.

However, despite all the buzz around automation, orchestration, and XDR the path to implementation has not proved easy.

Orchestration is not a silver bullet

On the face of it, orchestration is a no-brainer, lifting the burden of repetitive tasks and saving time so cybersecurity teams can focus on higher-value activities. Yet adoption remains limited. Industry observers have even seen examples where businesses shifted from having no orchestration, straight to full orchestration, and then back to no orchestration again because they found they were spending all their time and resources fixing the automated workflows to function properly. They concluded that a simple script could work just as well for their use case.

Chris Jacobs advises that teams shouldn't assume that by buying and installing a platform they'll suddenly find themselves "magically" capable of doing things they weren't doing before. First, they need to look at what processes they currently undertake manually and identify how these will benefit from orchestration into an automated workflow on the platform.

Nabil Adouani suggests that another reason for low adoption relates to the number of existing tools already in use. When there are already a lot of tools in play adding an orchestration platform that must be maintained increases the pressure on teams – the exact opposite of the desired effect. If security professionals who want to be focusing on security need to frequently add new use cases, update workflows and work on integrations, this may lead to task avoidance and low adoption of the tool.

Deciding where to start

Organizations can feel overwhelmed when faced with the potential scale at which they could automate cybersecurity detection, management, and response, so where is the best place to start?

First, decide what types of incidents you want to handle with the tool. Then look at what you are already doing and where you are doing it when an incident occurs. So, for example, you might be using spreadsheets, one note, and emails to record and handle incidents, following a manual playbook. Look at that process and work out which elements could be automated, and then orchestrated into a multi-stage

process in the platform. This approach has the added benefit of overcoming lack of trust in the outcomes of orchestrated processes. If you know what your process outcomes typically look like before you orchestrate them, you will find it easier to rationally accept a similar outcome from the orchestration tool.

Detection and vulnerability management are strong use cases for automation, and we recommend businesses put most of their focus here initially. Network detection, email security, and endpoint detection are all areas where, once issues are identified, multiple automated actions can be launched, such as informing the relevant stakeholders, enriching the alert data, and prioritizing the actions needed to mitigate the issue. In the case of vulnerability management, scanning identifies the weaknesses, and an automated workflow can share it with the people that need to action remediation.

It is also important to understand that the level of automation and orchestration that is appropriate will depend on the use case. Very few organizations will want to remove human oversight entirely from a process. For example, in patch management, it's not advisable to automatically patch all your servers because the tool has identified a vulnerability and an available patch; there must be human input. Instead, you can use automation to find the right combination of compensating controls, so when the tool identifies a vulnerability, it automatically sends alerts to the relevant stakeholders so compensating controls can be put in place before the patch is implemented.

One of the major advantages of using a centralized platform is that all teams are using the same data and starting from the same point. This helps get cross-disciplinary IT and security teams working together and starts to break down the siloes that often exist between departments.

In conclusion

In summary, when starting out with automation, first identify the repetitive, time-consuming workflows you already undertake that can be orchestrated. Then design the workflow with the appropriate balance of automation and human input for the use case, focusing initially on the detection phase before determining what aspects of response can or should be automated. Finally, explore how access to the tool can go further to break down siloes between departments and get all teams working effectively together on a unified security mission.

This approach should reduce some of the pain points around implementing automation and ensure organizations are realistic in their expectations of what they can achieve.

Case Studies

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. **YourDMS transforms FJ Chalke** – As with most businesses that experience rapid growth, the challenges of managing increased amounts of paperwork become a much larger task. The Sales Department were storing deal files in costly off-site storage and the team were spending a lot of time searching for the files they needed, but the challenges didn't stop there.

2. **Vox Telecom delivers impressive business benefits with InfiniBox** – With technology and telecommunication solutions becoming key to business operations today, service providers need a stable, available and high-capacity storage platform to deliver an excellent customer experience.

3. **Global development company uses Nuix to analyze 3TB of data in Misconduct probe** – A global development company faced allegations of misallocated funding and general misconduct within a four-year program with multiple delivery strands that crossed international borders and involved more than 150 staff operating in many languages.

FJ CHALKE CASE STUDY

Established in 1929, FJ Chalke is a family owned multi-franchise car dealership representing Abarth, Fiat, Isuzu, Jeep, Kia, Nissan and Suzuki.

ANALYSIS

With showrooms throughout Somerset, FJ Chalke continues to grow, which has allowed their most recent Kia & Nissan flagship showroom to open in Yeovil in December 2019.

As with most businesses that experience rapid growth, the challenges of managing increased amounts of paperwork become a much larger task. The Sales Department were storing deal files in costly off-site storage and the team were spending a lot of time searching for the files they needed.

The challenges didn't stop there. The accounts department were now managing more invoices, dealing with more queries, paying more suppliers, and struggling to ensure documents didn't get misfiled to comply with audits. Staff were constantly having to travel between all of the branches, compiling paperwork, sending it back for approval and signing, then collecting it again, with each 50 mile round trip taking over 1.5 hours. Whilst this was a critical process for the department, it was time consuming, put a strain on resources and meant keeping track of specific documents was difficult.

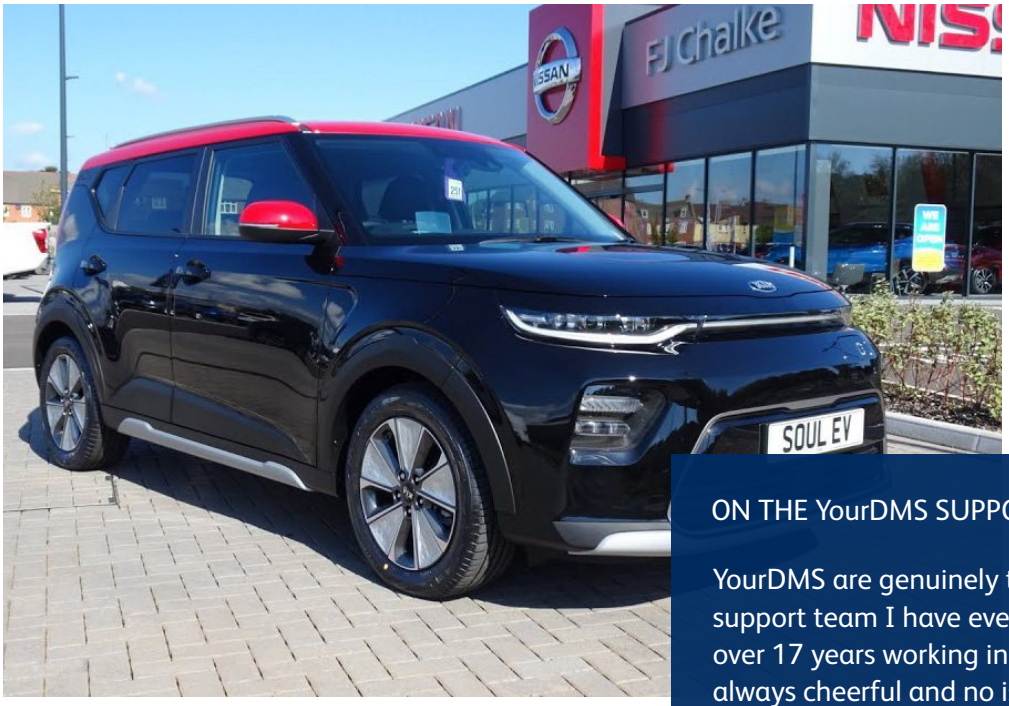
YourDMS SOLUTION

FJ Chalke wanted to store their files securely, in one place, so that all departments could easily access the information they needed.

Initially, YourDMS helped implement an Invu Document Management system in the Sales department. This allowed staff, in a matter of weeks, to scan old and current deal files in a structured manner, giving them visibility and the ability to locate any document within seconds.

With the success within the Sales department, YourDMS's mission didn't stop there. As part of the service, conversations moved swifty on to how they could help save time and money within other areas of the business, starting with the accounts department.

Invu was rolled out with integrated digital workflow functionality. A document would start its digital journey as soon as it enters the business (via post or email). Invoices are filed in Invu and users add relevant pieces of information in order for the document to be stored and distributed to the correct department manager for approval.



ON THE YourDMS SUPPORT TEAM...

YourDMS are genuinely the most helpful support team I have ever come across in over 17 years working in finance! They are always cheerful and no issue is ever a problem for them to try and help you with. They are also very understanding when it comes to implementing change at a slower pace than maybe some other businesses would.

Nicola Green
DEALERSHIP ACCOUNTANT AT FJ CHALKE

Security presets are configured when the system is setup to ensure that an invoice can only be accessed by the team member who needs to process it.

Managers could clearly see the invoice, add notes and see what is required from them with Invu's fully customisable workflow all within a click of a button.

Other features include duplicate checking, document audit trails, fixed lists, ability to action multiple work tasks at once.

RESULT

The Invu Document Management system has transformed the way the FJ Chalke Group work.

The Sales department now have their files stored in Invu, which allows them to find deal files in minutes, respond to queries quickly and deliver fantastic customer service. It also removes the risk of files being damaged and the need for off-site storage.

The Accounts team no longer have to travel between branches to collect paperwork, or to send paperwork off to be signed - it is all done through Invu. Not only does this save them a huge amount of time, it completely eliminates the issue of paperwork going missing as invoices can now be tracked through the whole process. Managers can easily query an invoice and reject it with comments.

Invu features multiple search options including by date range, invoice status, invoice number, and supplier, so the Accounts team can always find the files they need in seconds. This is especially helpful during an audit.

As Nicola Green, Dealership Accountant at FJ Chalke explains, *"It has also helped them massively when it comes to our yearly audit, because everything can be found so quickly searching through Invu, rather than having to sort through masses of paperwork in boxes in a cupboard."*

Nicola is also pleased that YourDMS have helped to identify where Invu can help in other areas of the business, with other departments such as HR using Invu to manage their paperwork.

Future steps

FJ Chalke are keen to explore how automating their Invoice Processes, to include 3 way matching, can benefit the business.

What is FJ Chalke's advice for other companies tackling similar problems?

Nicola comments, *"My advice would be to just go for it. We faced quite a bit of resistance when implementing the new system, as most organisations do, but as soon as staff started using Invu, they could see how much better it was for everyone. Any initial difficulties are well worth the effort, when it makes everything so much easier in the long-run."*

CASE STUDY

Vox Telecom delivers impressive business benefits with the InfiniBox enterprise storage system from Infinidat

Technology and telecommunication solutions have become key to business operations today, and service providers need a stable, available and high-capacity storage platform to deliver an excellent Customer Experience (CX). Vox Telecom (Vox) is a leading South African ICT and telecoms operator delivering a variety of services and solutions to the southern African market.

They rely on the cost-effective, high performance, high capacity and 100% availability of the InfiniBox enterprise storage solution from Infinidat, which plays a central role in supporting the entire Vox offering and has improved the performance of all services across the business.

The Challenge

At the start of 2019, Vox faced two significant difficulties around its existing storage platform. Firstly, the five-year maintenance period was coming to an end, and secondly, the company was running out of capacity much faster than anticipated. Adding to these issues, Vox was unable to utilise the full capacity of its existing storage solution, as some 40TB needed to remain 'unused' for the system to function.

"We reached the capacity limit of the system faster than anticipated. Coupled with the prohibitively expensive maintenance extension option, we made the decision to perform a technology refresh and replace the platform with a completely new solution," explained Keith Laaks, Executive Head for Technology, at Vox.

The Solution

Vox needed a cost-effective, high-performance storage array for its hosting environment in order to assist the business to meet customer demands and rampant data growth. An agile partner, who would be able to deliver quickly, was also a necessity. After evaluating 12 different storage arrays on criteria such as performance, Inputs/Outputs Per Second (IOPS), storage efficiencies, compression, deduplication and redundancy, Vox selected the InfiniBox solution from Infinidat, supplied by local partner and solutions integrator, Datacentrix.

Two InfiniBox F4304 arrays were deployed, one at each of Vox's data centres in Johannesburg within the production and Disaster Recovery (DR) environments respectively. For workloads with low Recovery Point Objective (RPO) and Recovery Time Objective (RTO), Vox makes use of VMware's vSphere replication feature.

"These arrays primarily service our virtual servers, database and voice infrastructure, and also play a key role in our data protection strategy. The solution allows seamless integration with our data protection vendor," said

"Thanks to excellent relationships, solid teams and effective planning from the outset, the implementation went smoothly and no challenges were experienced. The training and support provided by Infinidat throughout the journey ensured we got it right the first time. The proof of our success came from our customers' users, who noticed performance improvements without being aware that a storage upgrade had been performed."

Keith Laaks, Executive Head for Technology at Vox

Solution Advantages for Vox Telecom

INFINIDAT

95% minimum cache hit ratio

Enhanced performance and guaranteed uptime

Seamless provisioning of new services and solutions

Selby Maake, Cloud Storage and Virtualisation Engineer at Vox. "Each array delivers 1.7 Petabytes (PB) of virtual capacity with the actual available capacity variable depending on the compression ratio. This gives us far more storage for an extremely cost-effective rate per terabyte."

The Result

Implementation of the solution began in September 2019 and took one month to complete. Local Infinidat partner, Datacentrix, worked closely with Vox on the installation, helping Vox take the project from racking, stacking and initialisation, through to switching, provisioning, testing, and finally into the production environment. Infinidat also provided certified administration training through Datacentrix, flying in experts from its head office in Israel to South Africa. This was to ensure the data migration was seamless.

"Thanks to excellent relationships, solid teams and effective planning from the outset, the implementation went smoothly and no challenges were experienced. The training and support provided by Infinidat throughout the journey ensured we got it right the first time. The proof of our success came from our customers' users, who noticed performance improvements without being aware that a storage upgrade had been performed, said Laaks.

The InfiniBox arrays offer flexibility when it comes to scale and ease-of-use for critical workloads. Also, they deliver superior performance with a low total cost of ownership (TCO) without compromising the CX. The InfiniBox ultimately empowered Vox with a data-driven competitive advantage at petabyte scale.

"One of the key benefits we have realised results from the low-touch configuration and administration of the InfiniBox arrays. This has allowed us to provision new services and solutions seamlessly and with minimum manual interaction. Our previous solution was laborious to configure, taking up to an hour with multiple steps, increased complexity and room for error. The Infinidat solution takes less than a minute, improving our customer service, while freeing up time for our teams to attend to other business needs," Maake added.

Redundancy is another critical feature of Vox's operations. Previously, the company experienced some issues with failures, so a robust solution was required. InfiniBox's triple redundancy controllers guarantee uptime, ensuring Vox can always deliver an uninterrupted service to both internal and external customers.

Future plans

"Aside from our connectivity, broadband access and voice solutions, our cloud offering is a growing element of our business, with impressive market penetration figures. We needed the right platform to support our growth goals and storage is the key ingredient. The InfiniBox solution supports our requirements by delivering the right blend of cost-effective storage and high performance, coupled with the ability to slot seamlessly into our existing infrastructure," said Laaks.

"Infinidat also provides excellent proactive monitoring and local support through Datacentrix to ensure constant uptime and availability. This is critical to Vox from an operations perspective. Based on our forecasts, we will require additional capacity by the end of 2021. We are extremely happy with the platform and will likely expand our storage with additional InfiniBox arrays, when the time comes," he concluded.

GLOBAL DEVELOPMENT COMPANY USES NUIX TO ANALYZE 3TB OF DATA IN MISCONDUCT PROBE

SUMMARY

A multinational development company established an internal team to quickly investigate allegations of misconduct. The team turned to First Response and Nuix for help to rapidly process, search and analyze three terabytes of data from disparate sources within the company. Within hours, the investigations team found the critical information it needed to respond properly to the allegations, saving the weeks that it would have taken using any other software to get the same results.

CHALLENGE

A global development company faced allegations of misallocated funding and general misconduct within a four-year program with multiple delivery strands that crossed international borders and involved more than 150 staff operating in many languages.

The organization launched a forensic investigation to find out if there was any truth in the allegations. The data analysis requirements of the investigation were large and complex. Investigators quickly needed to find accurate answers to these allegations from approximately 3TB of data which was spread across multiple file types and locations, including:

- More than 250,000 documents stored within a cloud system
- 92GB of data in two different mailbox formats
- Numerous folders within multiple Microsoft SharePoint sites comprising over 250GB of data
- A hosted program knowledge management system.

SOLUTION

The organization called in computer forensic specialists First Response, a Nuix services and training partner, to support its internal investigations team. John Douglas, Technical Director at First Response deployed Nuix Workstation, a supercharged data processing, search, and analysis platform, which he used to index the large quantities of program data and make it easily searchable for timely analysis with the team.

RESULTS

FORENSICALLY PRESERVED RELEVANT EVIDENCE

Using Nuix, Douglas and the investigations team quickly and efficiently identified the evidence sources required to respond to the allegations. Investigators kept data from all these sources within a compound Nuix case file, removing the need to convert or move data between formats and tools during the investigation.

“This made it much easier to maintain provenance and trace critical evidence identified during the investigation back to its original source,” said Douglas.

“We also needed to maintain evidential integrity and produce a legally sound forensic technical report,” he explained. “This is why it was so important to use Nuix.”

A spokesperson for the company added, “Nuix helped us meet organizational imperatives for transparency in our programming and we would not hesitate to use it again for any future due diligence processes.”

PROCESSED 3TB OF DATA WITHIN HOURS

First Response used Nuix on two reasonably powerful office work computers to process all 3TB of case data within hours. This enabled the team to start searching the data using keywords almost immediately.

“Consolidating the data from the various project sources and indexing it to enable effective keyword searches would have been impossible without Nuix’s forensic processing capabilities,” said the spokesperson.

“The advantage of using Nuix when you have a lot of data to analyze in a short time frame is the speed with which it can index your data—it’s the fastest data slicer and dicer there is,” said Douglas.

“Other forensic tools can’t process the same volume and variety of data types as Nuix can, in the time it can do it. Nuix has made this information available for search, analysis, and review while other tools are still churning through the dataset.”

> “...it only took us 45 minutes to narrow down these search results and find the answers we needed.”

QUICKLY ELIMINATED DUPLICATES AND IRRELEVANT DATA

Nuix's inbuilt data analytics capabilities automatically deduplicates data during processing, which significantly reduced the size of the dataset investigators needed to review.

"Nuix saved us a lot of time by matching identical content regardless of where this data was stored and identifying the unique items," said Douglas. "This was particularly useful given our data was spread across multiple repositories and networks.

"We could then identify within hours rather than days which documents were relevant to the investigation. By reviewing only the relevant files, we could pinpoint the critical information we needed to understand the facts of the case much faster."

COMPARED SIMILAR DOCUMENTS SIDE BY SIDE

Nuix gave investigators a single pane of glass to compare and cross-reference intelligence across all data sources at once.

"Nuix automatically grouped and visualized the most important forensic artifacts," said Douglas. "We could also display a complete chronology of events in one timeline and see communication networks and maps of activity across all sources."

"At the start of this investigation we had no idea about what Nuix could do," said the spokesperson. "Once John outlined the possibilities of the tool, we provided timelines, GPS locations, email addresses, keywords, and other information that John combined into search terms and applied to the entire database of indexed data.

"As a group, it only took us 45 minutes to narrow down these search results and find the answers we needed. Without John's forensic expertise and the power and capability of Nuix, we have no idea how long it would have taken us."

ABOUT FIRST RESPONSE

First Response is a London based specialist cyber incident response and digital investigation company that helps organizations navigate the complex issues surrounding systems breaches, server compromises, and data loss. They work with a wide variety of clients including banks, law firms, energy and manufacturing companies, and public sector bodies.

Learn more about Nuix or contact us for a free demo
www.nuix.com/contact-us

nuix

Nuix (www.nuix.com) creates innovative software that empowers organizations to simply and quickly find the truth from any data in a digital world. We are a passionate and talented team, delighting our customers with software that transforms data into actionable intelligence and helps them overcome the challenges of litigation, investigation, governance, risk, and compliance.

APAC
Australia: +61 2 8320 9444

EMEA
UK: +44 203 934 1600

NORTH AMERICA
USA: +1 877 470 6849

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:

Cyber Insurance and ITDR – In a world where cyber threats are varied (and constantly changing), cyber insurance can protect organizations from losses due to security incidents. As well as minimizing business disruption and providing financial protection during an incident, cyber insurance may help with any legal and regulatory actions after an incident. But with organizations struggling with the escalating cost of cyber insurance, now is the time for every business to demonstrate a strong posture when it comes Identity Threat Detection and Response

Customer Insight Driving Tech Businesses – Most companies strive to run a customer-centric business, but with customers becoming more self-sufficient and more in control than ever before, but delivering positive customer experiences, providing optimal value, and earning long-term loyalty may seem an easy goal, but achieving it on a continuous basis is proving more challenging for the business world.

HOUSE *of* WORDS MEDIA LIMITED
Guiding you with knowledge