Remote access and the workforce of the future

Contents:

Introduction

Historically, remote access has been a tactical solution adopted to respond to specific, time-sensitive business needs, particularly in relation to IT help desks. Organizations would often use several remote access products at any time.

Recently, businesses have shifted towards a more strategic approach to remote access. This goes beyond the usual help desk / service desk environment, expanding to facilitate functions such as homeworking, training, and sharing of IT resources.

Rather than using several screen sharing solutions, organizations are consolidating their remote access strategy. By working with more sophisticated, enterprise-ready products this has proven to be beneficial, providing compelling ROI and increased security benefits.

Many companies are using the power of such products to help drive change in their organizations, particularly in relation to an increasingly mobile workforce.

To gain an insight into the way IT professionals are developing new enterprise-wide remote access strategies, we interviewed over 50 senior technology professionals in a wide span of industries across the UK, US, and Canada. The results of these interviews have been distilled into this eBook.

Chapter 1

Remote access global trends

"70% of people globally work remotely at least once a week" [1]
IWG

Remote and flexible working has increasingly become the norm for businesses in the UK and the US – and it's a growing trend. The UK's Office for National Statistics reported that 4.2 million people in the UK regularly worked from home in 2015[2], marking an increase of 800,000 in a decade.

The figures are mirrored in the US, where a 2017 Gallup poll[3] showed that 43% of US workers spent at least some time working remotely. In addition to the figures associated with telecommuting employees, travelling staff are now expecting to be able to access information wherever they happen to be. In return, IT help desk and support teams need to be able to assist these workers remotely.

Enabling people to work remotely, efficiently and securely is a huge challenge for employers.

Demand for remote access

"People can work in most roles from pretty much anywhere these days"
Rob Ossian, National Instruments

Matthew Bellinger, Microsoft Services Manager at the University of Sussex, feels that employers now expect from their employees a consistent quality of performance, whether they are in the office or working from home:

"The real shift is that staff expect to be able to perform their work duties wherever they are, and to have the exact same experience regardless of where they are working... we're going to have to develop some newer solutions to deal with the current expectations"

Remote access global trends

The hunt for a high-quality remote access software to facilitate mobile working is something to which William Merritt, Enterprise Operations Manager at Medidata Solutions, Inc. alludes to. Merrit employs IT consultants across the globe who need access to the company's network to carry out specific IT tasks that Merrit and his team are not able to handle internally. Occasionally he found himself needing to send hardware out to the consultants, with potential loss of equipment and security breaches.

"I believe that if we had a better remote access solution, we could solve a lot of the challenges we're facing ourselves, rather than onboarding different consulting companies to help out with these tasks."

Rob Ossian, Senior Manager of Digital Support at National Instruments, agrees with Merritt that with a better remote access solution you can be more flexible in the way that you work.

"It's undeniable that people can work in most roles from pretty much anywhere these days, if conditions allow. And of course, if the role is compatible with flexible working, there's a really large collection of people that don't have a justification for commuting on a daily basis". The infrastructure needs to be there, though, he stressed: *"The right infrastructure leads to better organization. You need to have the ability to organize your tools, your access and your resources."*

Bo Armstrong, Hotel Technology Manager at OTO Development, supports the IT needs of staff across 60 hotels. As part of his job he is also looking for a single solution to meet all the company's needs:

"We'd love to find one tool that allows us to do everything we need to do. We want our staff to be able to login remotely with unattended access, and we also want to access the computers ourselves. We want to be able to send someone to a website, give them a code and be allowed in, possibly with a reputable tool that is widely accepted by other businesses."

Drivers of remote access adoption

According to Rob Ossian, recruitment is an area that is driving the uptake of remote access by helping organizations find the best people, wherever they are:

"If you can get past the geographic distribution plan, which is obviously a big deal for many companies, you find that the best people aren't necessarily all in the same location."

Improved customer service is another driver of adoption, according to Suhail Halai, Senior Manager of Strategic Accounts for Ultimate Software. A good remote access solution provides speed and simplicity in solving customer issues:

Remote access global trends

"I have been in a situation when clients cannot email me a sensitive Excel document that we need to edit together. In this case, and in other instances when they could benefit from my expertise, it's much more effective for us to just kick up a remote session and collaborate."

Regulatory compliance is also a consideration that now, more than ever drives companies to consider adopting a remote access strategy. Most industries are subject to compliance regulations such as HIPAA, PCI-DSS, and the newly-introduced GDPR.

These regulations specify strict requirements about how organizations must store and process corporate and personal data. To achieve compliance there are multiple considerations that must be addressed in relation to security, privacy, and visibility.

Compliance as a driver of remote access is something William Merritt mentions, particularly for companies working internationally:

"From a compliance and security standpoint, a consolidated, company-wide remote access solution would make things a lot simpler for us."

Failure to meet compliance can have disastrous consequences, including legal punishment, data breaches, and loss of reputation, reinforcing the role of remote access as a permanent component of enterprise-wide strategies.

Matthew Bellringer of Sussex University also agrees that adopting a remote access software that enables companies to observe compliance is extremely beneficial:

"One thing I really like about using a secure remote access solution is that it makes governance and compliance so much easier."

Chapter 2

The major remote access adoption challenges

Security

Given that the main purpose of remote access software is to allow people to take control of devices that are located remotely, security becomes a critical consideration. Our interviewees have shared with us some of the security concerns they needed to address as part of their remote access strategy.

Rob Ossian fears that without the right security measures in place, giving people the right to access information outside the walls of the organization puts the system at risk of being compromised. An example of this would be a small company that outsources IT support and needs to give access to external IT consultants. The use of open source software or unencrypted tools and single-factor authentication could also put companies at risk of cyberattacks and data breaches.

Kevin Sheahan, Director of Network Security Practice at Presidio Inc, puts it this way:

"It's about vulnerability: you are sending your surface area into environments, processes and people that are not subject to your control. You can instruct every person you work with to follow your procedures and security measures when they connect to your systems, but there is always the possibility that they may fall short."

Solving these issues can vary in complexity, depending on the environment. Boris Kalitenko is responsible for IT at University of Miami - Miller School of Medicine, where requirements are often in conflict:

"The healthcare industry is extremely regulated, so the challenges that we are experiencing are probably unique. While we need to provide a remote access to our clinical providers, we are obligated to guard patients' healthcare information and control access to them". Issues of confidentiality must be balanced with the detailed needs of people accessing the system for different purposes, so *"collaboration between clinical providers inside and outside the hospital brings extreme complexity into the puzzle of remote access."*

> *"Once a system has been made remotely accessible, it also becomes remotely vulnerable."*
>
> ***Rob Ossian***

The major remote access adoption challenges

In a more general context, Larry Monuteaux, who resides in the US and is the IT manager at Continuum Managed Services, was particularly concerned about the use of devices at home:

"If people access our system remotely via a VPN, it creates a potential vector for data leakage."

Additionally, Suhail Halai from Ultimate Software fears that external users might be accidentally given access to an excessive amount of information:

"IT security guys and admins are occasionally reluctant to give access, as they fear that some of the tools they use might give the user too much control. The prospect of a data leakage means that sometimes they don't make their work computers available in the way they should," he said.

While Monuteaux's and Halai's concerns are shared by many, it is worth noting that, unlike a VPN, a good remote access solution enables a high degree of control of what each user can and cannot access.

The BYOD (Bring Your Own Device) dimension of home working was also raised as a security issue, as remote employees might adopt more lax security measures when it comes to their personal devices. Our interviewees identified secure user authentication as an essential feature of remote access tools.

Our technology experts had some suggestions on how to make remote access software more secure:

Kevin Sheahan, Director at Network Security Practice, commented: "

Multi-factor authentication (MFA) is a great feature offered by remote access providers for peace of mind. In the future, I would like to see the addition of a biometric authentication option, in line with phones becoming more capable of supporting fingerprint reading and facial recognition."

While no remote access solution will provide guarantee of absolute security, features such as encryption, MFA and controlled access to teams and groups, contribute to create a very strong defense by enabling additional security layers.

Cultural change and mindset

Research by Forbes in 2016 established that almost two-thirds of the workforce are fearful of change[4]. It's no surprise that one of the major challenges our interviewees identified is motivating employees to adopt new ways of working with remote access:

"Changing your company culture is always the most difficult part. The cost of adopting remote access is no longer a significant issue, because we know that this technology can save us a lot long-term and will help to mitigate risks. The main obstacle now is user acceptance."

The major remote access adoption challenges

While the costs of using remote access software depend on the use case and the number of licenses required, consolidating on a single remote access solution allows you to cut down the costs as well as the time which goes into deploying the software.

Successful implementation of remote working however involves a change of mindset, not only from the individuals, but also from the executive management. Rob Ossian explains:

"It takes a certain mindset to be able to work productively outside of the office environment, and employers need to be upfront about expectations. When I discuss remote working with my employees, the first thing I do is to establish what their success criteria is. While flexible working policies are good for the company, telecommuting is also a staff perk, and it can be suspended if performance deteriorates."

Equally, he said, the manager needs to understand how to work with staff at a distance:

"I have worked for a number of very skilled managers who just don't know how to manage remote workers. In my experience, if they are bit skeptical about flexible working and reluctant to allow it, it's because they don't fully understand it."

Ultimately, the demonstrable benefits provided by a flexible working approach are slowly shifting this mindset, and employing remote workers is becoming a normal part of doing business for a growing number of organizations.

While changing the culture of a workplace can be very challenging, doing so is far from impossible. One way to make it easier for businesses to embrace remote access software would be to use a software which is more user-friendly.

User-friendliness

Traditionally, most remote access solutions were created specifically to support IT help desk activities. For this reason, their functionality can appear unfamiliar to non-help desk employees, making its adoption a bigger challenge than it needs to be. Medidata's William Merritt talks about his experience:

"If you get a system that's overly-complicated, the end-user experience really suffers. When that happens, we get into a situation where people are not happy with the solution chosen because they just can't wrap their head around how to use it."

Helen David at Big Woof Consulting agrees: *"Software suppliers try to create a user-friendly product, but sometimes they fail to deliver on this area".* She also identified a specific pain point that could create and cause delays when getting new users authenticated, especially following mergers between companies: *"Single point of user authentication within a large corporate system is a challenge."*

The major remote access adoption challenges

Remote access systems need to work seamlessly, agrees Matthew Bellringer of Sussex University:

"Users don't want to think about technology. They just want their application, their data, and they want to work without thinking about it. I think the real space for innovation is making software easy to use for corporate end-users, allowing us IT departments to deliver a service that feels much smoother and more intuitive."

The IT professionals seem to agree that technology and software tools that are intuitive and easy to use, especially for teams and staff members outside of the IT department, will be accepted more easily by the workforce.

Multi-platform support

These days, businesses are dealing with a hugely diverse hardware landscape. The prospect of handling such fragmentation can be very daunting, as it often brings challenging operational issues capable of creating frustration and costing the organizations valuable time and money.

This proliferation of devices and platforms is not going to go away any time soon, and embracing this new reality is a challenge on its own. When companies consolidate remote access to one user-friendly platform, however, the potential to roll out that solution across the organization becomes much greater:

Andre Smith, Network Administrator at Hampton University, observes: *"That's the beauty of remote access: it's so simple! While writing our own remote access tool would require a great deal of effort, it is very easy for end-users to implement and for businesses to incorporate into many applications."*

Chapter 3

The benefits of using remote access

Our interviewees observed that when an organization moves from using remote access merely as a tactical tool to using it strategically, they see numerous commercial and operational benefits.

Flexible connectivity

When it comes to building remote access solutions for your business, flexibility is an important consideration that often affects the choice between direct and cloud connectivity.

Both options present clear benefits. While direct connectivity is liked by many due to the to not needing any third-party servers to establish connections, it can be trickier to configure. Cloud connections instead are in general more accessible, versatile and easier to manage, but they do introduce additional security and reliability considerations.

Cloud connectivity is also a must to support remote employees, and is part of that infrastructure that Rob Ossian addressed in his interview:

"While most office-based people can work from anywhere and allowing them to do so can be beneficial to both the company and the employee, the organization needs to have the right tools in place for this to happen."

Overall, remote access solutions offering both direct and cloud connectivity are more likely to meet the needs of organizations who don't want to have to choose between direct or cloud and may want to use both depending on the use case.

The benefits of using remote access

Employee retention

The opportunity to work from home, is extremely attractive to employees. The CBI Forecasts for 2017[5] concluded that flexible working was a key factor in attracting and retaining talent, to the point where a third of employees claimed to prefer flexible working to a pay rise.

A Canada Life Study[6] revealed that home workers say their levels of productivity and morale have increased. This feedback results from a decrease of stress levels, the enjoyment of maintaining a casual attire, having more time to exercise and socialize, and the ease of not commuting daily.

Rob Ossian concurs:

"Good flexible working policies increase staff morale, so it's easier keeping employees with the company. A big factor is being able to grant valuable staff members the ability of working from home a couple of days per week."

Control of Data

For William Merritt of Medidata Solutions, moving towards one centralized remote access solution is essential for maintaining control of company equipment and data:

"It becomes too costly to maintain corporate-owned equipment and send it home with people, and it's too much of a risk. They can lose it, they can leave, they'll have data stored locally … Because our business is mostly data, if we don't have a great degree of control we put ourselves at greater risk. Having a remote access solution that's centrally managed, where the data actually lives and remains within the company, is very important."

Chapter 4

The future of remote access

Looking into their crystal ball, the technology professionals we spoke to have no doubt that remote working is here to stay. They are also equally adamant that while remote access software has made considerable progress over the last few years, it needs to evolve further to support this trend in a wider variety of contexts.

For many, it's a question of aligning remote access with the company's business objectives. In many ways, a good remote access strategy enables companies to expand their businesses, reduce costs, recruit the best employees, support them working efficiently and keep them motivated, and ultimately gaining competitive advantage over less progressive companies.

Mike Harm, Chief Technology Officer at Workplace for Atos, sees a BYOD scenario feeding into a centralized platform:

"We think that BYOD will become much more prominent in the digital era. I feel that the inevitable diversity of devices would benefit from multi-platform solutions."

Suhail Halai has spotted a similar, cloud-based hub emerging:

"Companies are adopting more and more SaaS (Software as a Service) solutions. At present times, these solutions mainly work on the internet rather than being installed on a machine. Conversion of company IT systems into cloud-based solutions allows employees to log in to the software from anywhere."

Halai added the caveat that some sectors will need to adopt a more cautious approach to adoption of remote access:

"If you think about insurance companies and banks, this model will not work as easily from any computer, as you would have to connect via a VPN or a corporate laptop for monitoring purposes. But I feel there is a healthy playground for remote access solutions"

Conclusion

Our survey, which included the participation of 50 IT leaders, established that a solid remote access strategy is considered very desirable for businesses. One of the biggest benefits identified by our interviewees is the ability to support flexible working policies, aiding recruitment and retention of the best employees regardless of location.

There is also the efficiency and cost-reduction potential of remote working. Flexible working practices increase the profitability of businesses with mobile workforces, while maintaining control of productivity and meeting compliance standards.

Organizations that make the leap from viewing remote access as a tactical tool to using it in a more strategic way will see considerable operational and commercial benefits.

While currently the specter of security breaches looms large for all businesses, the main reservations among our interviewees relate to the relatively unknown risks of allowing company data to be accessed remotely. This view, however, was balanced by those who felt that a consolidated, centralized approach, focused on encryption and secure authentication of devices, offered a high level of control and compliance.

The difficulty of changing the culture of a workplace was considered by most an obstacle in the way of embracing remote access software. Many interviewees agreed that making the tools easy to use is key to their uptake among the workforce.

Overall, our interviewees concluded that remote access will inevitably be adopted by progressive companies using it to deliver a considerable strategic advantage.

Final thoughts from REALVNC

This survey has been very valuable for us at RealVNC. We are always interested in hearing how IT professionals experience remote access and what challenges they encounter when adopting the technology. This is essential to help us improve our own screen sharing product, VNC Connect. We were happy to learn that the results reported in this survey were in line with the feedback we receive by interacting regularly with our customers and prospects.

Remote access global trends

As RealVNC is a fast-growing tech company, we have been able to experience first-hand some of the factors that drive other organizations to adopt remote access technology.

Remote working, for example, is a new business reality for many businesses, such as our own: many RealVNC employees have been taking advantage of our flexible working policies and telecommute regularly. While implementing these policies came with its challenges, allowing our employees to work remotely lead to in an overall increase in productivity, a morale boost for staff, and the ability to hire from a much wider pool of candidates.

Regulation compliance has also been a trending topic in 2018, given the recent enforcement of the new GDPR (General Data Protection Regulation). For us, enabling and meeting compliance has been a year-long mission, but we know that efforts to maintain regulatory compliance will pay off in the long run.

Every company, and especially those in their growing stage, should strive to develop a strong best practice-culture, so that compliance and security are part of every remote access session. Ultimately, these are essential for protecting the reputation and future of any business.

Final thoughts from

REALVNC

The major remote access adoption challenges

Remote access software, like any technology has some inherent barriers to deployment. In our experience, the main concern people have with remote access software is security.

At RealVNC, we have always done our best to address these concerns by having a transparent approach to our security architecture, and by supporting critical features that add further layers of security, such as multi-factor authentication, encryption and controlled access to teams and groups.

We found that transparency and regular security-oriented product updates go a long way when it comes to giving our customers and prospects total peace of mind. This approach, together with businesses becoming more aware of the benefits of using a reputable remote access solution such as VNC Connect, are making it easier for organizations to overcome the traditional obstacles associated to new software adoption.

The benefits of using remote access

The current evolution of technology and business models is raising the visibility of remote access as a strategic, rather than tactical, corporate tool.

We were happy to see that the IT professionals who participated in the survey agreed that a good remote access strategy enables progressive business practices like remote working, supporting new revenue models and helping IT teams manage an increasingly complex BYOD landscape.

The future of remote access

Over the last few years we have witnessed remote access technology evolving well beyond its traditional help desk use case. We are also observing a proliferation of BYOD and other new business ecosystems, and we expect this trend to continue.

Communicating with our customers reinforced our opinion that remote access is not only here to stay, but also that organizations are more aware of the improved business efficiency that can be gained by using it across departments and sectors.

We are already seeing the remote access market expand beyond the traditional office workspace into retail, consumer devices, automotive, banking and even healthcare.

Another likely future scenario that supports this trend is the use of remote access in combination with third-generation technology, such as augmented reality, for training and education purposes.

Acknowledgements

Mike Harm **Chief Technology Officer - Workplace, Atos**

Mike Harm is the Chief Technology Officer for the Workplace domain at Atos and has spent over 20 years providing, designing, implementing and envisioning differentiated workplace services in partnership with clients worldwide. With a background that spans support services, process engineering, IT Service Management, systems engineering and innovation product management, he is passionately connected to the technological, behavioural, and procedural pulse of the user experience from end-to-end. He is a member of the Atos Scientific Community where he explores the impact of digitization on the human experience, the future of work, and new concepts of productivity and employment emerging from digital trends. In his role at Atos, He is responsible for technology partnerships, supplier strategic relationships, overall workplace vision and strategy as well as delivery technology policy in the workplace domain and adherence enforcement to those policies throughout service and product development lifecycle.

Larry Monuteaux **IT Manager, Continuum Managed Services, LLC**

IT Professional with over 23 years of experience architecting, building, securing, administering, and troubleshooting complex, enterprise-level computing environments. Holds a Master of Science in Computer Information Systems with a concentration in Information Security. Currently works as the US IT Manager for Continuum Managed Services in Boston, MA.

Acknowledgements

Bo Armstrong Hotel Technology Manager, OTO Development
Currently working in the hospitality industry as a Technology Specialist where I provide IT expertise and support to key stakeholders including Development, Operations and Owners. I analyze, design, recommend, support and implement hotel technologies for major brands and a geographically dispersed portfolio of hotels. Past jobs include Hotel Technology Manager, Technology Consultant, and teaching as an Instructor. Certifications from Microsoft, Cisco, VMware, Citrix among others

Boris Kalitenko Senior Manager System Development - Enterprise Imaging, University of Miami
Boris Kalitenko, originally from Ukraine, completed his training as an ER physician in Donetsk State Medical School. He conducted clinical research and published articles in Cardiology Journal and Therapeutic Archive in late 80s. In the late 90's he become an Information Systems Analyst for the Kindred Hospital in South Florida. Later, as a Clinical Information Systems trainer at Broward Health, he developed training materials, and created best practices. Results were published in Journal of Emergency Nursing (June 2006). From 2006 to 2017, Boris Kalitenko was a Senior PACS Administrator at Broward Health, where he is responsible for the imaging system of the radiology department. Currently Boris Kalitenko is a Sr. Manager for Enterprise Imaging for University of Miami. Responsible for: Radiology PACS, Cardiology Imaging, VNA, Eye Care PACS at Bascom Palmer Eye Institute. Additionally he contributes to system development and system integration with other hospitals. He was contributing author to the HIMSS publication "Guide to the Wireless Medical Practice" [ISBN 0-9777903-8-X]. Boris Kalitenko received National Recognition for Innovation for designing a wireless network solution for legacy imaging devices. He graduated from FIU with Masters of Science in Managing Information Systems. He is Certified Imaging Informatics Professional and Microsoft Certified System Engineer.

Suhail Halai Sr. Manager, Strategic Accounts, Ultimate Software
Suhail Halai is Principal Consultant at Ultimate Software where he leads a team focused on Artificial Intelligence and Machine Learning-based solutions to solve today's business challenges. He is focused on finding solutions in the Customer Experience, Employee Experience, Recruitment, and Talent Management space. He has been a strategic advisor to a global roster of clients in the field of business transformation, risk management, human capital, and technology-related initiatives. He has also been actively involved with early-stage software start-ups in areas of retail operations and corporate finance. Suhail earned his Bachelors in Business Administration majoring in Management Information Systems from the University of Georgia at Athens and currently lives in San Francisco enjoying coffee shop conversations about the future of work, the sharing economy, social media, and crypto-mania.

Acknowledgements

Rob Ossian Senior Manager, NI Downloads, National Instruments
Over the past 20 years, Rob Ossian has held several senior leadership positions within the high-tech industries of Austin, Texas. Currently, as Director of Global Support for Codero Hosting, Rob is responsible for the delivery of scalable and world-class Customer Success experiences through globally distributed technical teams through leading-edge, data-driven, omnichannel, and predictive support strategies. Earlier, Rob was a member of the National Instruments leadership team responsible for Digital Transformation of online and in-product User Experiences for all managed software. Prior to National Instruments, Rob led the Global Cloud Services teams supporting Dell's Software as a Service Portfolio, building international Follow-The-Sun Support Operations, and managing multiple high-complexity engineering teams located in Ireland, Mexico, Brazil, United States, and Malaysia.

Andre Smith Network Administrator, Hampton University
Andre Smith, IT Professional and Tech Business Entrepreneur began his professional career as a PC Technician in 1998 doing hardware repairs and replacements. and began managing multiple sites in North America as a Valeo North American Network Administrator in the Clutches and Transmissions Division with Manager, Friend and Mentor, Grzegorz Nowak. In 2006 he started Smith Computers, building workstations and Servers for small to medium sized companies. They became a one stop shop designing, building and supporting networks of all types for everything from Medical, Manufacturing, and Law, to Home offices, Government Facilities, Retail, and International Multi-site VPNs with Hybrid Cloud Infrastructure. In 2009 Smith started a training program and began offering externship opportunities to students from surrounding Universities and Colleges, focusing on those having difficulty finding their path or place in IT, that he runs to this day. Andre also became one of Hampton University's Network Administrators in 2009 where he facilitated the transformation and upgrade of the Scripps Howard School of Journalism and Communications. Andre later went on to Co-Found AMEOT LLC a non-traditional Cyber Security Company with his Wife, Monique and Son, Trevon. AMEOT LLC, capitalizing on cloud infrastructure, strategic partnerships and artificial intelligence, continues to grow and expand to this day. In 2018, frustrated with education's failure to keep up with current Technological Standards and the way IT training was being delivered, Andre Co-founded UrCerted LLC with partners in education, Dr B. Ernest Nwidag, William Moore, and Jemal Taborn. Creating a pipeline for those new to the Tech field as well as they wishing to transfer into the field from other career paths

Acknowledgements

William Merritt Enterprise Operations Manager, Medidata Solutions, Inc
Global IT Operations Manager with over 25 years experience in the Financial industry. Following the principles if ITIL, I have transformed the IT support experience all the organizations that I have worked with. I'm a graduate of the New York Institute of Technology with a BS in Electrical Engineering. Currently I am pursuing a MBA at Penn State University.

Helen David Strategic IT Transformation Programme Manager, Mitie
Professional consultant specialist in legacy migration of IT and applications covered in cob every mature business has and don't know where to start moving them. From 30years of working directly in IT for worldwide Blue Chip businesses and Government, has rare skill of understanding the needs of all layers of an IT system that needed to be designed for a sucsess in IT migration programmes.

Matthew Bellringer Microsoft Services Manager, University of Sussex
Matthew Bellringer is Head of Platform Development at the University of Sussex. He manages the team who look after all Microsoft-related services across campus. Coming from a technical background, Matthew leads the development and deployment of innovative new services for the University. He has worked in IT for over 15 years, mostly in education and the third sector.
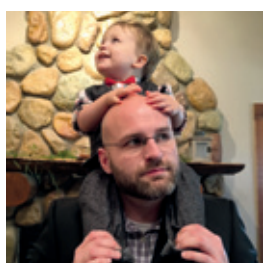
Kevin Sheahan Director, Network Security Practice, Presidio, Inc.
Kevin is the founder of Killbox, a security product development company, and an expert in enterprise network defense. Drawing from over 10 years of experience, Kevin has achieved some of the industry's highest certifications in honing his technical skills consulting for clients from every category and size up to Fortune 100. Previously, Kevin served in the US Army as a Systems Analyst and managed a Task Force NOC/SOC in support of OEF10. More recently, Kevin served as Network Security Practice Director for Presidio, where he consulted on a broad portfolio of network security products and technologies as well as operational processes to help clients achieve sustainable and effective security.

Acknowledgements

Acknowledgements

Sources:

[1] www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html

[2] www.tuc.org.uk/news/four-million-people-are-now-homeworkers-more-want-join-them

[3] news.gallup.com/businessjournal/206033/america-coming-workplace-home-alone.aspx

[4] www.forbes.com/sites/markmurphy/2016/08/14/the-big-reason-why-some-people-are-terrified-of-change-while-others-love-it/#a20595d2f635

[5] www.cbi.org.uk/businessvoice/latest/10-forecasts-for-2017/

[6] http://autotime.co.uk/homeworkers-more-productive-than-office-based-staff/

REALVNC

Every day millions of people around the world use VNC Connect to improve the efficiency of their businesses. Flexible and secure, VNC Connect remote access and support software gives organizations the power they need to "Connect & take control"

Contact

Sales: 0800 888 6410
www.realvnc.com

Address

RealVNC Ltd
Betjeman House
104 Hills Road
Cambridge
CB2 1LQ
United Kingdom