MORPHEAN

WHITE PAPER

PHYSICAL SECURITY AND THE CLOUD

Why now is the right time for Video Surveillance as a Service (VSaaS)

TABLE OF CONTENT

01	FOREWORD BY RODRIGUE ZBINDEN, CEO, MORPHEAN SA	02
02	INTRODUCTION	04
03	THE CLOUD SURVEY – A PROVEN TECHNOLOGY FOR TODAY	05
04	ADDRESSING MISCONCEPTIONS – THE CLOUD IS SECURE	06
05	THE FUTURE OF THE CLOUD	07
06	CONCLUSION	10

> WHY NOW IS THE RIGHT TIME FOR VIDEO SURVEILLANCE AS A SERVICE (VSaaS)

FOREWORD

Rodrigue Zbinden,
CEO, Morphean SA

The physical security industry is standing at an important inflection point. Cloud infrastructure is now well established as an enabling factor for connecting platforms and services that is cost effective and safe, and the business benefits of doing so are clear.

Some 89% percent of businesses in the UK, France and Germany are already using cloud solutions, the majority for email but also for CRM, HR and finance purposes. We know this, because we have commissioned an independent survey to establish the attitudes of business decision makers towards the cloud in the UK, France and Germany. The results of this survey are revealing and, in some cases, unexpected. There's a high degree of confidence in the cloud, an understanding of the benefits, and a high sensitivity to issues of security.

When it comes to IoT, however, the historical lack of attention to lifecycle security for IoT devices makes businesses nervous of adoption. Successful attacks and well publicised vulnerabilities, together with the introduction of strict regulations such as the EU's General Data Protection Regulation (GDPR), are enough to make many think twice.

Nowhere is this more true than for those of us involved in physical security technology such as video surveillance. Poorly designed products, rushed to market with no plans for lifecycle support, have proved to be an easy target for criminals and other threat actors. Well publicised attacks, such as the Mirai botnet, have exploited inadequately secured devices to reach their targets.

These risks can be managed and mitigated against. Not every vendor treats security as an afterthought, and those who are very best in class understand that security is an inherent – if not the most important – part of their value proposition. The potential of the cloud to deliver real benefits in the area of physical security is unquestionable, so long as it can be trusted, and there are solutions which will stand to the most stringent due diligence.

In this white paper, we look honestly at the challenges, outline some of the emerging benefits - which go far beyond physical security - and raise the questions that potential customers of such services should be asking their suppliers.

We're doing this because physical security as a service is an exciting area to be in, and we believe in our vision of how it can drive efficiencies, inform decision making and protect business assets and personnel more effectively than legacy solutions. Businesses agree: in our research, more than 90% of respondents said that it was important that security solutions are able to provide data that can be used in wider decision-making processes. Over 45% said that they would definitely consider moving physical security to the cloud, which could make access to this data happen.

This value can only be unlocked through relationships of trust between suppliers and customers, which is only achievable when those of us who offer technical services have proven ourselves to be worthy of that trust. That means we must treat cybersecurity as being as important as physical security, and this white paper outlines how we can make that happen.

INTRODUCTION

What we call cloud computing today has played a central role in our work and home lives for nearly two decades. Google's Gmail is close to its 15th birthday and was predated by earlier webmail services such as Hotmail and Yahoo! Business messaging services such as Microsoft Teams, Slack, WhatsApp or Skype are also popular, but they inherit most of their capabilities from 20th Century applications such as ICQ, MSN Messenger and more.

Cloud computing is near ubiquitous. From Netflix and Spotify in the home to Microsoft Office 365, Salesforce and AWS in the workplace, the days of uncertainty about the cloud are over. Increasingly, the cloud is computing, delivering cost effective services, reduced capital expenditure, better communications and collaboration and, of course, real-time business intelligence through Artificial Intelligence (AI) and connecting devices via the Internet of Things (IoT).

Up until recently, fears about cybersecurity held back cloud adoption in the large enterprise: the attitude that "if we don't own it, we can't control it" lingered on while upstarts like Dropbox or Airbnb demonstrated why elastic computer models could power disruption. These are fears which might reasonably have expected to worsen as news of cybersecurity incidents repeatedly made mainstream headlines over the last few years, but they haven't slowed the pace of cloud adoption.

These incidents have covered the full gamut of cybercrimes. They include the Mirai botnet, which co-opted IoT devices to create the largest Distributed Direct Denial of Service (DDoS) attacks the internet has seen , to the rise of ransomwares such as Wannacry, which brought the UK's National Health Service (NHS) to its knees . In 2018, a code injection attack on the British Airways ecommerce platform exposed the payment details of 380,000 customers .

The potential for a combination of poorly maintained endpoints and the scale of cloud-based networks has been made clear. Yet businesses are still moving to the cloud, as this white paper shows. In the following pages, we discuss the results of an independent survey commissioned by Morphean, in which the cloud-purchasing habits of IT decision makers in 1,500 companies with more than 25 employees are revealed. Interviewees were based in the UK, France and Germany.

What we find is that businesses are migrating their legacy systems to cloud platforms for email, CRM, ERP and HR. Not only do the benefits outweigh the risks, but as cyber-attacks become more highly automated and damaging, they become more expensive to protect against too.

Investing heavily in cybersecurity is a double win for cloud platform operators: not only is security the single most important factor for end customers when evaluating a cloud operator, the economies of scale achieved by platform providers means that better security can be achieved more cost effectively in the cloud than in legacy on-site data centres.

In the face of ever-evolving threats, it's the cloud services that can adapt and mitigate against new dangers more swiftly than traditional IT.

To better understand the attitude of businesses towards the cloud, and the future of physical security in a cloud world, Morphean interviewed respondents about their current and anticipated approaches to cloud computing, and what consideration they give to physical security as a service.

This white paper outlines the findings of that survey and identifies the opportunities that it presents for those offering physical security technologies via traditional IT today.

https://en.wikipedia.org/wiki/Mirai_(malware)
https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/
https://www.forbes.com/sites/bishopjordan/09/09/2018/british-airways-hacked/4369852567#ae

THE CLOUD SURVEY

A TECHNOLOGY FOR TODAY

Business confidence in cloud solutions has risen sharply in recent years. While stories of data breaches and exposed credentials have dominated headlines, the ability to offer better security at a lower cost than your own data centre has become a key part of the business strategy for cloud providers.

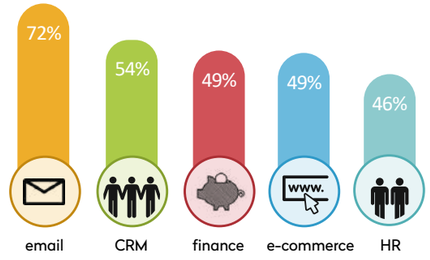
And the message is getting through. Cloud adoption is widespread, and companies are comfortable running their business-critical applications from the cloud.

In the Morphean survey, 89% of business decision makers in the UK, France and Germany said that they use cloud-based solutions in their company already. Adoption levels are high across all industries, although notably lower in healthcare (82.5%), where the processing of personal data is a highly sensitive issue. In retail and hospitality, just 5.7% of firms say that they are not using any form of cloud service yet.

It's often said that small businesses are more enthusiastic adopters of cloud technologies than large enterprise organisations, because they have no legacy infrastructure and value the cost savings more. In the Morphean survey, however, nine out of ten firms with more than 250 employees said that they used cloud software solutions compared to just 81% of firms with 25-49 employees, a reversal of the perceived wisdom in this regard.

Geographically, German firms were slightly less likely to report that they are already using cloud software solutions (85.6%), while the UK is the most enthusiastic adopter at 93.4%. The largest international discrepancy is in healthcare – only 60.9% of German healthcare providers interviewed are using cloud services, the lowest of any group. In the UK, meanwhile, where a big push towards digitised health records has been made in recent years, 96.8% of respondents in this sector are using the cloud at work.

Of those who use cloud services, 60% said that their level of adoption was "medium" and 24.2% consider themselves "high" level adopters. 71.6% said that these services are used for email, 54% for a CRM service and 49% for e-commerce and finance alike. HR and ERP solutions are also popular, with 46% and 44% of respondents deploying them respectively.



Overall, there are few differences in cloud adoption between respondents in different countries. French businesses reported being less likely to use cloud-based financial software (43%) compared to the UK and Germany (51% in each). British firms, meanwhile, are considerably less likely to use ERP systems in the cloud (34%) compared to German (43%) and French (56%) businesses.

Cloud infrastructure is well established for core business processes, then, but outside of these business mainstays only a small number of firms have begun to experiment with cloud services for other purposes (6%) – such as physical security. What we see is widespread adoption of certain proven services, but still caution towards non-mainstream activities as yet.

This will change. On average, a third of IT budgets have been spent on cloud services in the last 24 months, and 78% of firms believe that this will rise in the next two years. For 16% of respondents, more than half of their budget is already spent in this way.

Respondents estimate that this increase in spend should result in an estimated 47% of internal data being processed in the cloud. When asked about the most important factors in evaluating cloud solutions, however, a healthy scepticism emerges. Security considerations emerged as by far the most pressing for businesses: some 60.7% listed security as one of the most important considerations when evaluating a cloud solution. That compares to just 40.3% for the cost efficiencies compared to capital investment, the second most important consideration cited.

ADDRESSING MISCONCEPTIONS – THE CLOUD IS SECURE

If businesses are enthusiastic adopters of the cloud, however, it's not without some understandable caution. IT has been under relentless attack over the last few years, with stories of major data breaches common. Poorly implemented IoT devices, including networked video cameras, have emerged as a weak link in security procedures as they expand the attack surface dramatically for organisations used to operating behind sturdy network firewalls.

Criminal actors and white hat hackers have repeatedly demonstrated that badly configured IoT devices can be used as a backdoor to important databases. In one well publicised incident, a Las Vegas casino found that its customer records were stolen by hackers who infiltrated their system via a badly configured thermostat for an internet connected fish tank .

At the same time, the regulatory environment is becoming stricter and more insistent on cybersecurity precautions through legislation such as the EU's General Data Protection Regulation (GDPR). This raises awareness of the issues at stake, and places companies who don't take adequate precautions at risk of punitive action in the event of a breach.

These concerns are reflected in the Morphean survey. Security emerges as the number one concern for decision makers when it comes to adopting any kind of cloud services – unsurprising as one in four reported that they had suffered a data breach in the last two years. Three quarters of respondents have already implemented a GDPR review of their processes, underlining the importance of compliance too.

Two thirds of all respondents said that they consider security an important factor when evaluating cloud solutions. This topped the list of considerations above subscription costs (51%) and speed of deployment (46%). For those who haven't yet adopted cloud solutions, security was cited as the main reason why (45%). In addition, of the 11% of respondents who said that they would not consider a cloud-based physical security service, 64% reported that this was down to cybersecurity concerns.

https://www.washingtonpost.com/news/innovations/wp/21/07/2017/how-a-fish-tank-helped-hack-a-casino/?utm_term=.8bd5622dddge

If businesses are understandably cautious, they are still eager to proceed with digital transformation projects in the cloud. We've already established that the vast majority are using cloud services, and while security is the number one obstacle to cloud adoption – it's also the number one enabler. Nearly 27% of respondents said that the reason they moved applications to the cloud was to improve security, compared to 26% who were primarily motivated by cost implications and 22.7% who looked to improve collaborative working.

These responses did differ across national boundaries. In France, 35% of decision makers said that security was the main reason for migrating to the cloud – the most popular reason ahead of collaboration (23%) and cost efficiency (20%). German firms, meanwhile, were most likely to cite flexibility in working locations (30%), while in the UK cost is king (34%).

These reasons were consistent across company size, however, with only the very largest organisations generally favouring costs over security.

These findings paint a picture of a business world which is mature enough to understand the risks associated with cloud and IoT technologies, but savvy enough not to be put off by them.

WHY IT'S TIME FOR PHYSICAL SECURITY IN THE CLOUD

Organisations who took part in the Morphean survey are clearly comfortable with the way in which cloud services have developed for core business processes, and have widely adopted cloud solutions for email, CRM, ERP, ecommerce, finance and HR services. Uncoincidentally, these are the areas which have received heavy investment in cybersecurity by the world's largest tech companies.

Adoption of the cloud outside of these activities is still low, but one indication that the time is right to start migrating other services lies in the responses to the question of whether or not respondents were comfortable with the concept of moving physical security services to the cloud. Only 12.9% of decision makers said that they would not consider a cloud based solution for physical security, while 45% said that they would definitely consider one (44% said that they would possibly consider one).

Larger firms were more likely to be interested. 53% of firms with 501-999 employees said they would definitely consider such a solution, while only 26.6% of firms with fewer than 50 staff said the same.

Attitudes towards physical security as a cloud service also help us to understand what businesses see as the benefits of cloud technology. Some 92% said that it was important that a cloud solution for physical security provided businesses data that could be used to meet overall business objectives. Some 47% said that this was very important.

For physical security, then, there is a clear desire to move to the cloud, and the right platforms exist for customers to migrate to. What we anticipate is rapid growth in take-up of present and future offerings as providers become better at articulating the benefits and developing the right end products and business models to fit customer needs.

This is an important message for service providers. Over three quarters of businesses expect to increase spend on cloud solutions in the next two years, making this a growth opportunity. It's imperative that providers understand that a key driver is that more services you can connect in the cloud, the more value you can deliver for business intelligence and decision making.

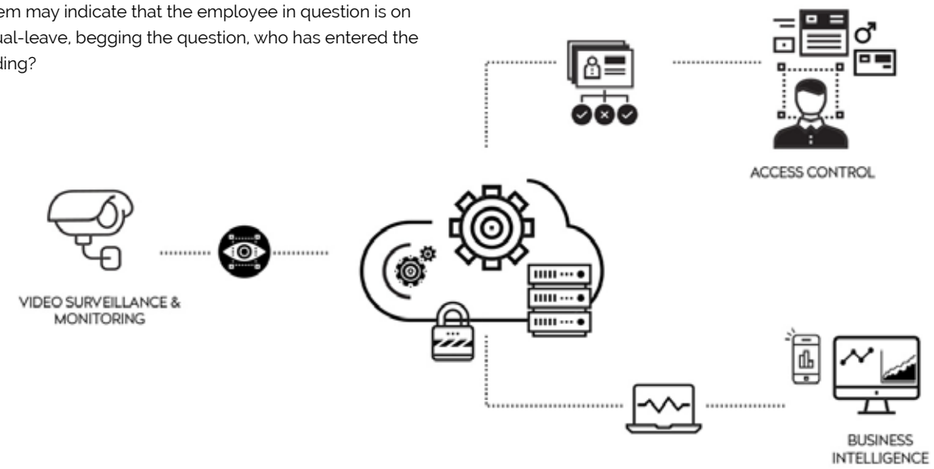
For video surveillance providers, cameras provide useful data beyond the existing monitoring and forensic examination of potential criminal incidents, which can be combined with other data in creative ways.

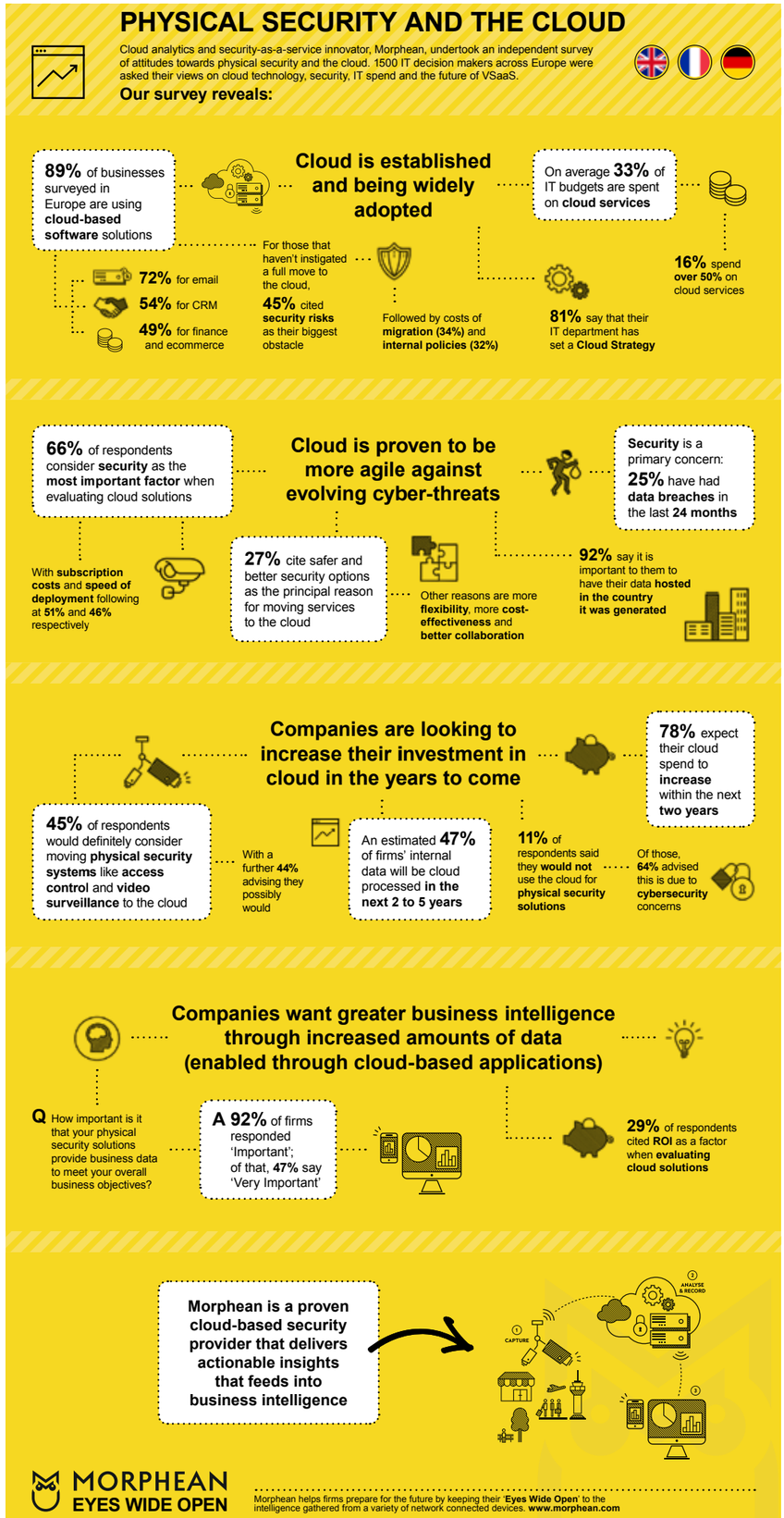
Morphean's video surveillance as a service (VSaaS) platform, for example, provides intelligent analysis of camera images that can offer cost efficiencies and improved incident detection for physical security teams, as well as benefits for other areas of the business. In retail, for example, a cloud-based platform for analytics means that in store cameras designed for stock protection can also alert managers when queues begin to develop at checkouts.

Other forms of physical security also benefit from platform integration. An IP-based access control system, for example, connected to a HR system. The access control solution may identify that an employee has entered a building at 8.53am. On first viewing, this seems like normal activity that doesn't require intervention. However, the HR system may indicate that the employee in question is on annual-leave, begging the question, who has entered the building?

And just as the business model for IT infrastructure changed with the advent of the cloud, so physical security is changing too. New revenue models based on monthly licences for cameras and software are developing, removing the up-front capital investment of a security system and ensuring that devices and platforms are always running the latest, most secure version of software and firmware.

All thanks to the cloud.





Conclusion

The findings of the Morphean survey reflect business decision makers who have confidence in the cloud, and aware of its benefits and the importance of security when making purchasing decisions. It shows the widespread adoption of cloud for core business processes, and a largely untapped market for "as a service" products that meet business objectives – so long as they can prove they deliver value and are secure enough.

One way of interpreting this would be that businesses trust the cloud, so long as they trust the implementing partner to secure it and provide the actionable information that they need to be more competitive.

For VSaaS, the opportunity is clear. A proven platform such as Morpheans can effectively fill all these important boxes for decision makers. It can deliver real cost savings, turn physical security hardware into an operational rather than a capital expense, and offer value beyond its core purpose with analytics and integration into other systems, such as marketing and monitoring customer behaviours.

From a cybersecurity point of view, it represents best-in-class design and features for security hardening, with round the clock support and incident monitoring.

VSaaS can prove that it is demonstrably more secure than an on-site solution. By removing the need to store video and personal data on-site, for example, VSaaS removes the risk of theft or tampering, and because devices are maintained and patched over strong, authenticated connections they are always up-to-date with the latest features and firmware.

What's more, VSaaS can help with GDPR compliance as personal data is fully encrypted with appropriate levels of anonymisation in a secure environment. GDPR ensures that risk is shared throughout a supply chain and proving these credentials to potential customers is a must.

The onus now is on system integrators and installers to understand the cloud platforms available to them and help end customers reap the benefits on offer. A drive for education throughout the supply chain now will help to grow VSaaS and other forms of physical security in the cloud just as adoption for general IT has boomed over recent years.

MORPHEAN
EYES WIDE OPEN

Morphean is a Swiss technology company with a strong presence in more than 12 countries worldwide. Founded in 2009 and with over 60 partners across Europe, the secure Morphean platform informs decision making and drives efficiencies for all organisations by generating unique and actionable insights from a multitude of data sources. With expertise across retail, transport & facilities management, among others, the company is recognised as a leader in secure service platform delivery through the use of cloud and AI technologies. The platform helps firms prepare for the future by keeping their 'Eyes Wide Open' to the intelligence gathered from a variety of network connected devices.

www.morphean.com

> MORPHEAN HELPS FIRMS PREPARE FOR THE FUTURE BY KEEPING THEIR **'EYES WIDE OPEN'**

MORPHEAN

MORPHEAN SA

Rte du Château 112
1763 Granges-Paccot
Switzerland

P : +41 26 422 00 90
M : info@morphean.ch
www.morphean.com