SECURE SYSTEMS ACCESS IN 2021
STATE OF THE NATION
A Bytes Market Report

BYTES Smarter together

In partnership with okta

About this Market Report

Having a simple to use, effective, robust and adaptable access control solution, where different employees with different roles are granted access to different systems, services and applications, is an essential component of a robust security environment.

Not only are such solutions easy to manage but they materially help minimise the impact of successful cyberattacks as risks are more easily contained by smarter, efficient, user friendly authentication measures.

They also help provide for a first-class user experience, as gaining access to the systems and services they need is typically a lot faster. Providing such a good experience is important as not only does it increase productivity levels, but it also reduces the likelihood of users trying to by-pass company applications and use unauthorised (shadow IT) services.

Jeremy Parsons, IT Architect at Heathrow Holdings comments, “Given the current Security threats Multi Factor should be considered essential in today’s world.”

To understand how UK organisations are responding to today’s Identity and Access management challenges, Bytes and Okta surveyed over 140 IT Professionals, in roles ranging from Security Architects and Administrators, to IT Managers, CISOs and Heads of IT, from a variety of organisations in diverse industry sectors. Our aim is to provide a clear picture of how businesses are addressing access challenges in 2020 and provide recommendations from Okta Identity experts on where businesses can focus next to provide more secure, more convenient access to company resources

This report provides their views and includes further insights, market trends and expert commentary from from Toby Noble, Identity Practice Lead at Bytes and Ben King, Regional CSO EMEA at Okta.

Report Summary

What is clear from the findings in this report is that organisations recognise the threats and challenges they face when it comes to providing secure and convenient access, but need additional guidance to help them mitigate against them – particularly when it comes to addressing some of the emerging risks brought about by the proliferation of home and remote working in 2020.

The survey surfaced some interesting findings:

1. **Security and simplicity out-ranks sheer speed.**
   Respondents recognise the need for users to have a simple and fast experience when accessing their systems, applications and services, but security is deemed just as imperative. One reason for this is to reduce risk by deterring users from by-passing company-approved applications and using simpler, but unauthorised and unmanaged, IT Services.

   Respondents also recognise that providing a great user experience cannot be at the cost of providing a secure environment. Security must remain paramount. It is therefore important to put in place solutions that provide a great user experience that provide the right level of security necessary to protect the organisation against the sophisticated efforts of today's cyber criminals.

2. **Home workers present a challenge.**
   While IT teams need to be applauded for their efforts enabling home working with very little notice at the start of 2020, what is clear today is that home workers are letting their guard down and putting their organisation at avoidable risk. Some bad habits that are creeping in are the sharing of company devices between family members, accessing company systems via unsecure networks, and not updating devices and systems when asked to do so.

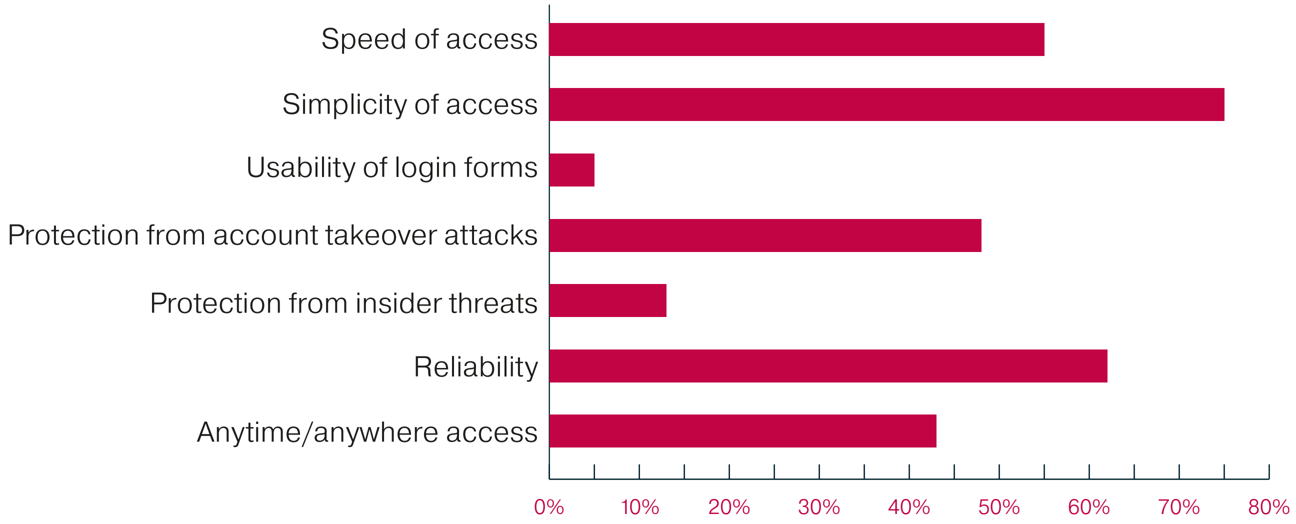
3. **Login forms are dead.**
   Whether employees, suppliers, partners or customers need to access systems, the login form has had its day. Not only do such forms present a slow and poor user experience but they do not offer the level of security needed. Login forms are easy to breach and if they are used across multiple applications and systems, can materially impact productivity.

4. **Organisations are using roughly 50% of applications on-premises, and 50% in the cloud.**
The hybrid environment is alive and kicking which is necessary to provide the level of agility, functionality and collaboration needed by today's progressive organisations. However, it is important to ensure that users do not have to log in to the applications each time they need to use them. Instead, organisations need to be implementing over-arching Identity and Access management solutions that provide employees with the first-rate experience they need, whilst not exposing the organisation to avoidable security and data-loss risks via the use of unauthorised Shadow IT services. One standardised experience across cloud and on-premises is increasingly demanded and expected.

5. **A one-size-fits-all approach to Identity and Access doesn't work**
The challenge with a one-size-fits-all approach to Identity and Access is that it means all employees, regardless of role or seniority, are granted access to the same systems as everyone else. More than 1/5 of respondents reported uniform access controls across the board. While on the one hand this keeps things simple, it does leave the organisation open to risk and rapid infection post-attack. A better approach is to grant access-rights based on the role of the person. This way, if there is a breach it can be rapidly contained and mitigated via the use of additional authentication and security measures. It also reduces the risk of the Insider threat and accidental or deliberate data loss via employees.

Matthew Peacock of Derby College suggests organisations, "Enable multi factor authentication. Offer good quality training to users. Simulate phishing campaigns to raise awareness."

When your IT users log in to your systems, what factors are most important to ensure they have the best access experience?

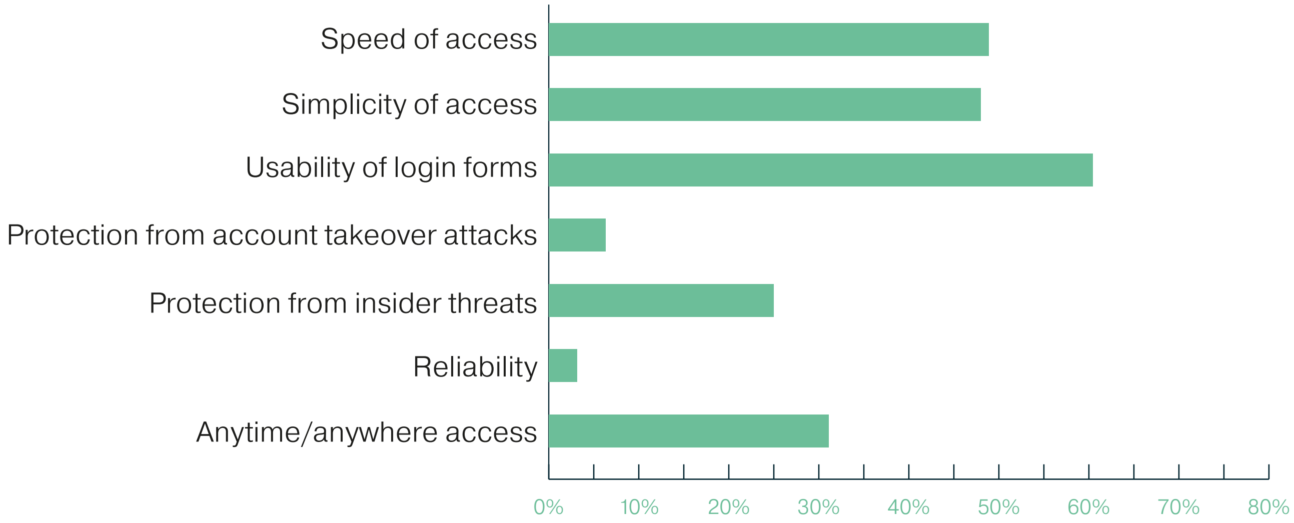


The findings from this question suggest that login forms have had their day – being ranked lowest by the respondents in terms of their importance. Organisations clearly recognise that the time it takes to complete login forms immediately puts people off and creates the wrong first impression when trying to gain access to an application, system or service. With so many better, more efficient and secure options on the market, the need for such an antiquated solution has gone.

Interestingly and reassuringly, "simplicity of access" is ranking higher than "speed of access", as it has been proven that employees that find accessing applications and services cumbersome typically find workarounds that often involve the use of unauthorised shadow IT systems. Creating a simple and efficient experience is a much better way to engage users and keep them working in the way IT would like.

Considering the shift many organisations had to got through technologically due to COVID-19, the relatively low ranking (3rd least important) of "Anytime/Anywhere" access is very surprising, as this is very much what employees need today. Particularly given the balancing act many are having to do with working from home while looking after dependents.

When your IT users log into/access your systems, what factors would you be most likely to compromise on/ sacrifice?



The findings from this question very much support the last question, with the "usability of login forms" identified as being the first thing to be sacrificed.

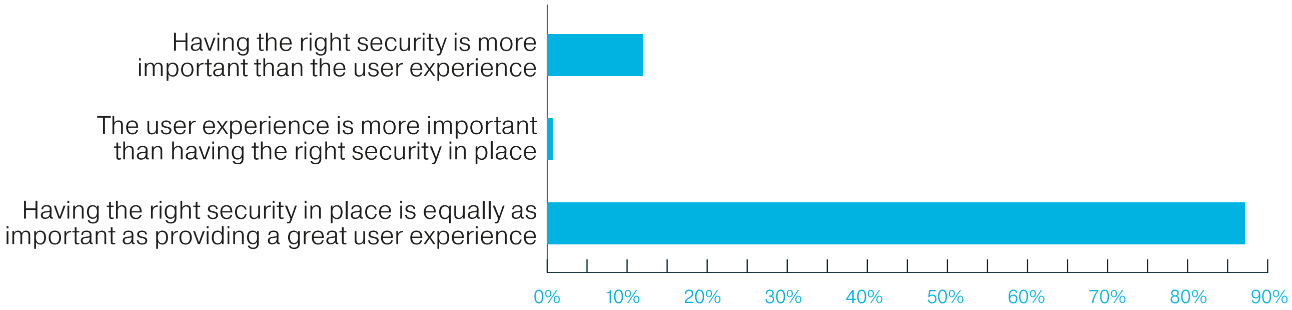
Interestingly, the 2nd and 3rd lowest ranking (the least likely to be sacrificed) are both security related, "Protection from insider threats" (#5) and "Protection from account takeover attacks" (#6), thereby give a clear indication that IT professionals are more likely to make it harder for people to login than compromise on security. With attacks being ever more sophisticated, together with a material increase in their frequency and with more people working from home, IT teams are now in the perfect storm and they need to be ready to weather it.

With the right access systems in place however, IT professionals should not have to make difficult choices as simplicity (and speed) of access are both achievable without having to compromise on security.

Organisations are seemingly asked to do the impossible: protect applications and data from breach and improve overall security — all while simplifying log-ins for users. But it can be achieved through comprehensive, multi-layered security that taps big data to secure user access and automate provisioning. Give users an intuitive and simple sign-in point and empower administrators with robust tools that simplify provisioning, auditing and security practices.

Gervais Carlton-Blake, CIO & CISO at LOD agrees, "Adopting Multi layered / defence in depth approach to security is still a critical strategy ... Regularly review the tech stack and simplify and integrate wherever possible."

When it comes to logging in, which of these statements best applies?



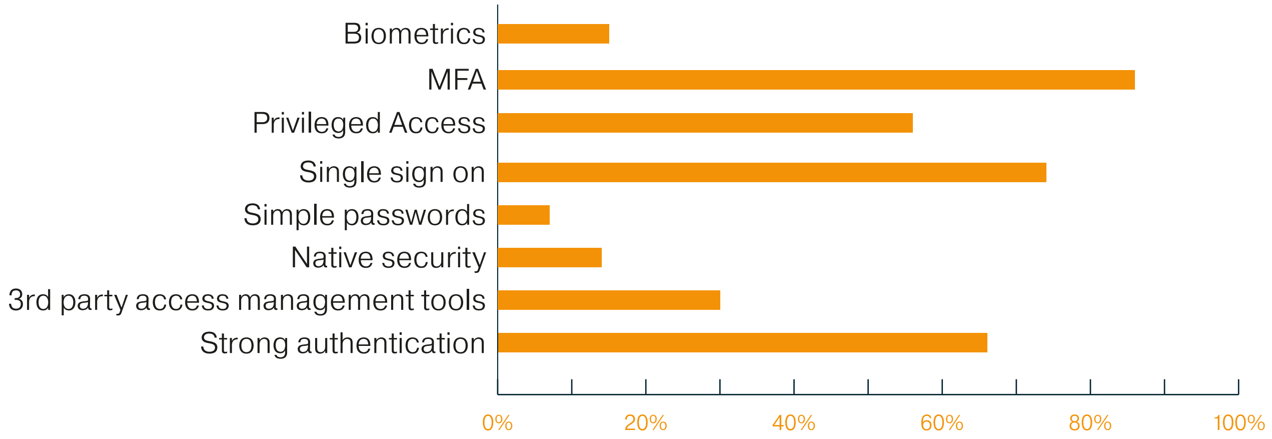
It is reassuring that organisations are putting equal weight on the importance of 'having the right security' in place with the' importance of providing a great user experience'.

However, the 11% of respondents that stated, "Having the right security is more important that the user experience" need to consider the user behaviour that is likely to occur if employees have a poor experience. Specifically, they need to be prepared to see an increase in the use of unauthorised shadow IT systems, such as WeTransfer, Box, Dropbox and other content sharing and collaboration systems that are easy to use but don't have the governance and security protocols necessary to prevent data loss.

More people are working remotely, and due to it being harder for IT teams to monitor what their remote workers are doing, without the provisioning of a great user experience remote workers are more likely to work outside of the company environment, rules and procedures.

As per the recommendation in response to the previous question, IT professionals should not have to compromise between security and the user experience, as both are achievable with the right access solution in place, such as Okta.

What solutions do you have in place to secure your systems?



The findings from this question conclusively show that relying on simple passwords is dead. Organisations are implementing more sophisticated solutions to ensure their environment is secure.

What is surprising however, is the very low penetration of biometrics, particularly given that Windows Hello allows for facial recognition and many of the latest client hardware devices are fingerprint-enabled too, though this may be explained due to the high number of organisations already opting for Multi-Factor Authentication (MFA). Whilst MFA may be perceived to slow down the sign-in process, adaptive MFA and step up authentication ensure the right level of authentication is applied as appropriate to the applications, assets or resources being accesed.

Single Sign-On is still holding up strongly which is not a major surprise. However, what is more surprising is the relatively high number of respondents that have a Privileged Access solution in place as this suggests that a higher than expected number of organisations are putting more focus on protecting their most valuable data.

It is slightly alarming that over 13% of respondents are relying on "native security" measures to protect their data. The problem with this approach is that users will have to navigate and experience multiple different access systems, some better than others, which can deteriorate the user experience and increase the likelihood of employees opting to use unauthorised shadow IT systems. Multiple security silos, such as these, can also limit the quality of reporting, making it harder for IT teams to make informed decisions and deploy standardised management environments.

Furthermore, while native systems are typically very good at protecting the device or system they were designed for, they each come with their own admin management console which can put an unnecessary strain on the IT teams needed to maintain them.

Overall, and despite the fact that almost 20% of respondents are still using simple passwords or native security systems, the findings from this question suggest that organisations are moving in the right direction when it comes to Identity and Access Management (IAM).

How strongly do you agree or disagree that when working from home your users are more likely to:

	STRONGLY DISAGREE	DISAGREE	AGREE	STRONG
Work from an unsecure network	4.03%	19.46%	57.05%	19.46%
Click on a malicious link	6.71%	39.60%	48.32%	5.37%
Use passwords more than once	3.36%	26.85%	50.34%	19.46%
By-pass your VPN	29.53%	40.94%	24.16%	5.37%
Use a non-work device to access company systems	14.77%	21.48%	43.62%	20.13%
Not update systems	8.72%	28.86%	48.99%	13.42%
Use unauthorised apps	16.44%	36.99%	37.67%	8.90%
Give 3rd parties access to systems	30.41%	54.05%	14.86%	0.68%
Lend company devices to family members to use	18.24%	28.38%	42.57%	10.81%
Use a company Zoom/Teams account for online drinks/social events	7.38%	25.50%	50.34%	16.78%

The findings from this question are perhaps the most interesting in this report as they surface some interesting and worrying insights. That said, IT teams up and down the country should of course be applauded for their ability to pivot to remote working with very little warning in March. It was a time of immense pressure. The findings and associated commentary relating to this question therefore should serve as a catalyst for change to help ensure any bad habits highlighted do not become normalised going forward as they risk exposing organisations to avoidable threats.

Let's start by summarising some of the key stats.

- 76% of respondents ether agree or strongly agree that their employees are working from an unsecure network
- 63% of respondents either agree or strongly agree that their employees use a non-work device to access the company systems
- 63% of respondents either agree or strongly agree that their employees are not updating their home systems
- 53% of respondents either agree or strongly agree that their employees lend company devices to family members to use

Why do these findings matter and what possible impacts do they have on the security of company systems and company data?

Linking these four statements paints a telling picture.

Firstly, employees with company devices are lending them to family members, who will be using them in all manner of ways, none of which the company has sight of. Some of which could be exposing the device to avoidable threats, when those devices are being used to access company systems via unsecured networks and when users are not taking the time to update the relevant systems when required. If the device therefore becomes infected, it could quickly infect company systems.

In the instance where employees may not have a company device to work from home, or choose to use another device to work from home, they are also accessing the company systems via unsecured networks, once again potentially exposing the company to threats residing on the non-company owned device.

When employees work from the office, they certainly wouldn't be swapping devices with colleagues nor accessing company systems via unsecure networks, thus the challenge is how to ensure remote workers are either acting responsibly or, at the very least, only access company systems via approved routes.

Additionally, this question has exposed a lack of visibility of who is accessing what systems. The last three options on the grid above are all based around the "who". Specifically, which third party suppliers are able to access company systems and services (such as Zoom, perhaps), who is physically using the device at the employees home (other than the employee), and who is using company systems and services (eg, Slack and/or Zoom) for social interactions. In each case, IT lacks the visibility, and therefore the control to ensure only authorised personal are gaining access to company systems and assets, such as confidential information and/or other sensitive data.

The findings from this question underscores a long thought view that employees that work from home are materially more likely to let their guard down, and avoidably expose their company to potential risk.

The first couple of questions in this report highlighted the desire for IT departments to provide their employees with a great logging on/access experience, and while this is advisable for reasons already explained, it must not be at any cost, specifically it must not expose the company to avoidable risk. This risk is easily mitigated by implementing simple solutions that provide for a great user experience that offer the level of access controls needed to protect the company from unwanted visitors.

Given home working is likely to be here to stay in some capacity, it's important the habits highlighted above do not become the norm, so the time to act is now.

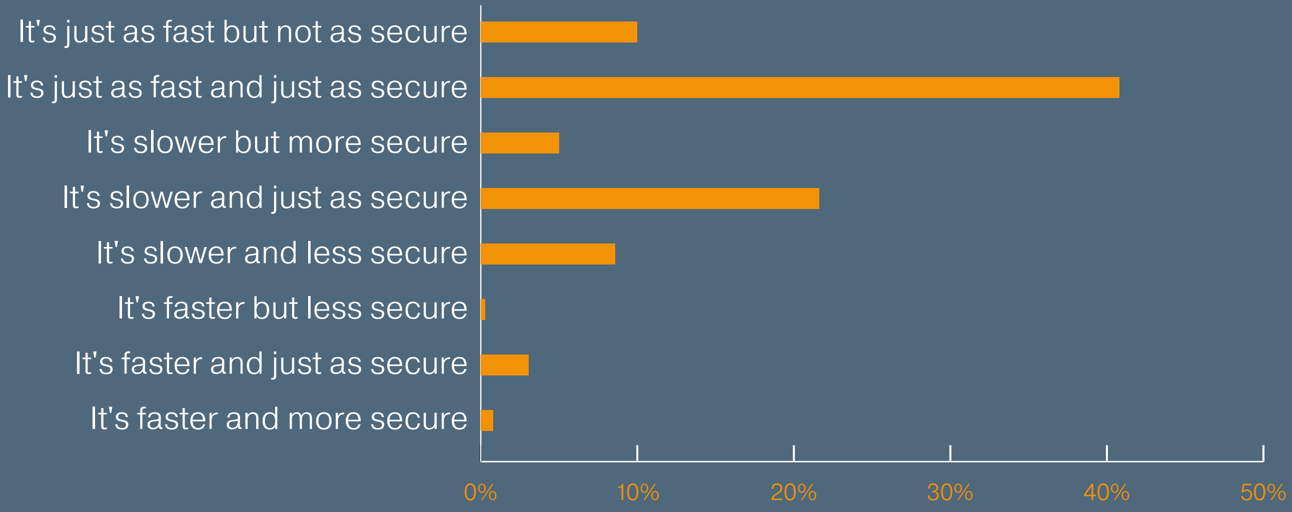
Many organisations take significant steps to secure their internal networks, but those security controls do not necessarily extend outside the office. Employees may inadvertently bypass these security controls as they access corporate resources from new devices and new networks.

We strongly encourage organisations to add a supplementary layer of security to all user accounts in the form of MFA:

- Use strong factors like mobile authenticator applications and biometrics.
- Identify which factors you will make available to your employees. Decide if certain groups require stronger factors.
- Roll out MFA in a phased manner - for apps, on-prem, VPN, servers.
- Rollout access policies for remote workers.

Once you have deployed SSO and MFA to all your employees, consider creating more granular access policies based on user, device, network and location context. Ideally, you can create granular access policies that align the strength of the policy to the potential risk associated with the login.

How has the enablement of home workers impacted the user experience associated with accessing their IT systems?



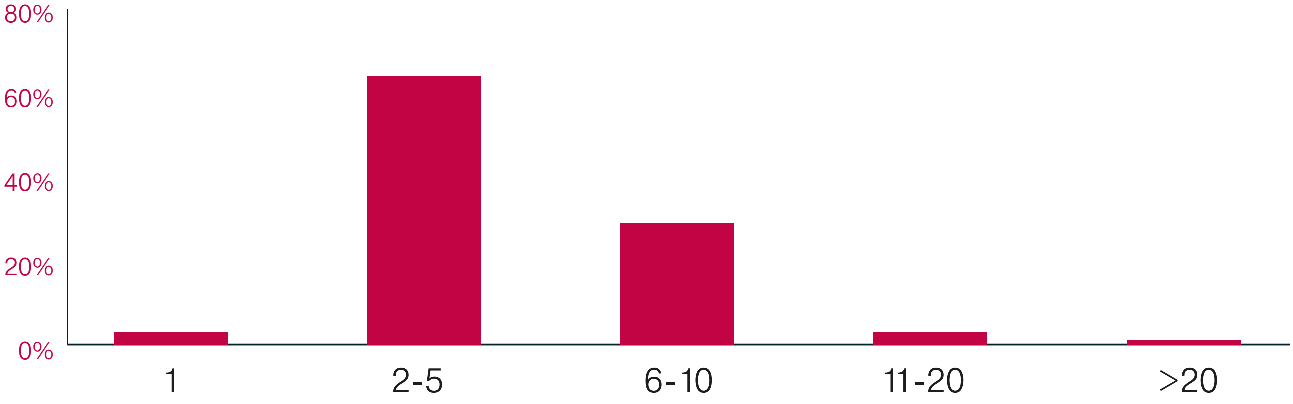
The findings from this question contradict some of the findings from the previous question as it has already been shown that home workers are more likely to work less securely than if they were in the office.

The fact that in nearly 40% of cases (6% + 24% + 10%), respondents stated that working from home is slower than in the office, could be partly the reason for some of the bad habits exposed before as users will always try to find a workaround when the working experience is substandard. Users might ignore or delay updating systems when asked or may bypass company applications and use unauthorised shadow IT services instead.

As employees, and homeworkers specifically, move to BYOD, IT must by definition switch their focus from being device-centric to people-centric. Their apps must be accessible from any device, any time. The challenge for IT then becomes on how to connect that user, independent of device, with the cloud services they need. To deliver this people-centric IT approach the business needs seamless Identity & Access Management for all web applications (in the cloud or on-premises) and across all devices. It's all part of ushering in a new era of IT, in which the IT department is a true service provider: benevolent, efficient and device-agnostic, and focused on making their end-users as productive and happy as they can be.

Barry Wise, Technology Design & Control Manager at Supporting Education Group Ltd comments, "Don't connect to the Internet! If you must, employ MFA, login behaviour alerting and other security tools."

During a typical day, how many of your applications/ systems does a typical user need to log in to?

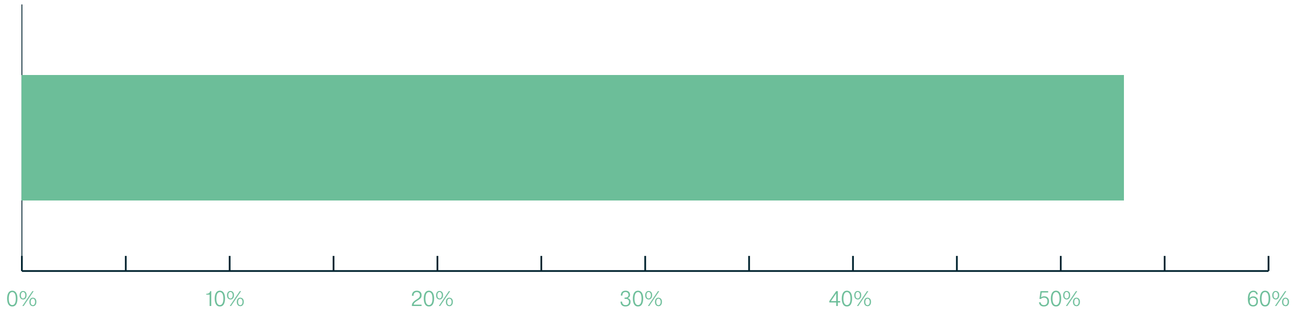


The findings from this question are in line with wider industry research. What is important to note, however, is that if >6 applications/systems are being used in a day, and if employees are expected to log into each of the systems independently, both productivity and the user experience are negatively impacted. This could encourage endusers to use unauthorised shadow IT services that, whilst easier to access, are less secure or visible to IT.

In these situations, it is recommended that organisations implement a unified access solution (Single Sign-On) that minimises the time needed to access the applications/systems thereby creating an all-round more positive and productive experience.

Ethan Sterling, Senior Infrastructure Engineer at GAP UK Ltd comments, "If you've not already implemented MFA, do it now. It's saved our users from compromise on a number of occasions and without it we'd definitely be in hot water."

When providing access to applications what’s the split of onpremises applications vs cloud applications?



Before we review the findings of this questions, let’s just explain the values.

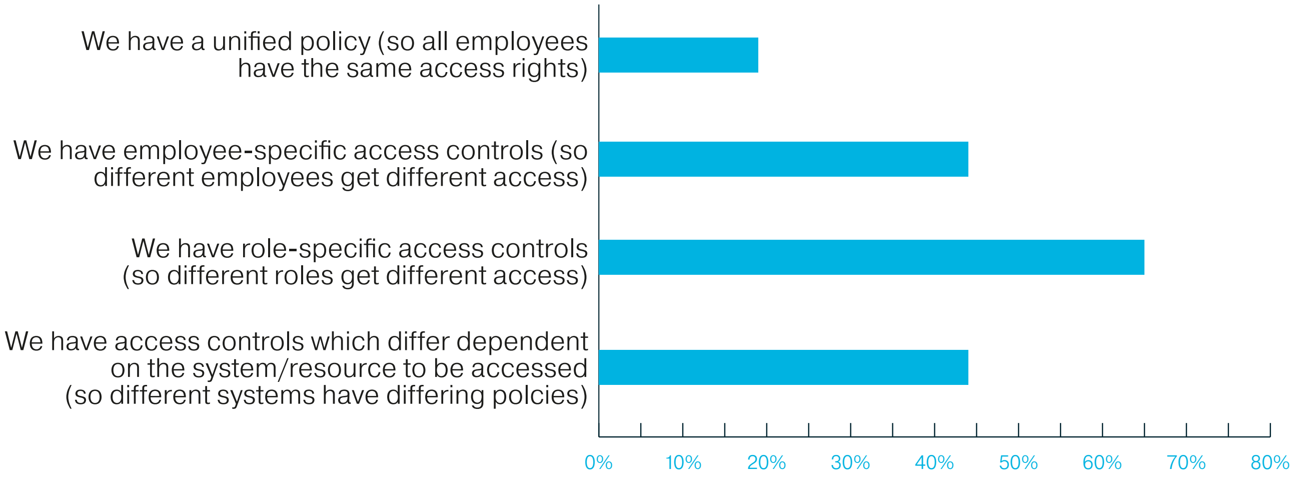
- 0% = 100% on-premises applications (and 0% cloud applications)
- 100% = 100% cloud (and 0% on-premises)

A score of 52 means that 52% of applications are typically on-premises and 48% are in the cloud, thereby suggesting that most organisations operate a hybrid environment, which is very much the norm.

That said, while running a hybrid environment is commonplace, few organisations have invested in a solution that ensures consistency of access across all systems. Some have a solution that covers their on-premises apps, and some have a solution (or solutions) that cover their cloud apps.

To maximise simplicity of access, while providing consistent access controls, it is recommended to have one overarching solution that allows IT teams to tailor and control access rights for all of their employees accessing all of their authorised applications and services.

To what extent do you adapt your security arrangements for different employees and roles?



It is encouraging that almost 66% of respondents have the ability to set role-specific access controls (different roles get access to different applications, systems and/or assets), however, there is still a large percentage of organisations (>18%), that have a one-size-fits-all approach to access, i.e., they have a unified policy so all employees have the same access rights.

One-size-fits-all environments don't allow for any additional controls for privileged users (such as Finance teams) and perhaps more concerning, is that they allow all users access to all areas, thereby potentially exposing the organisation to risk from internal threats or unwanted cybercriminals.

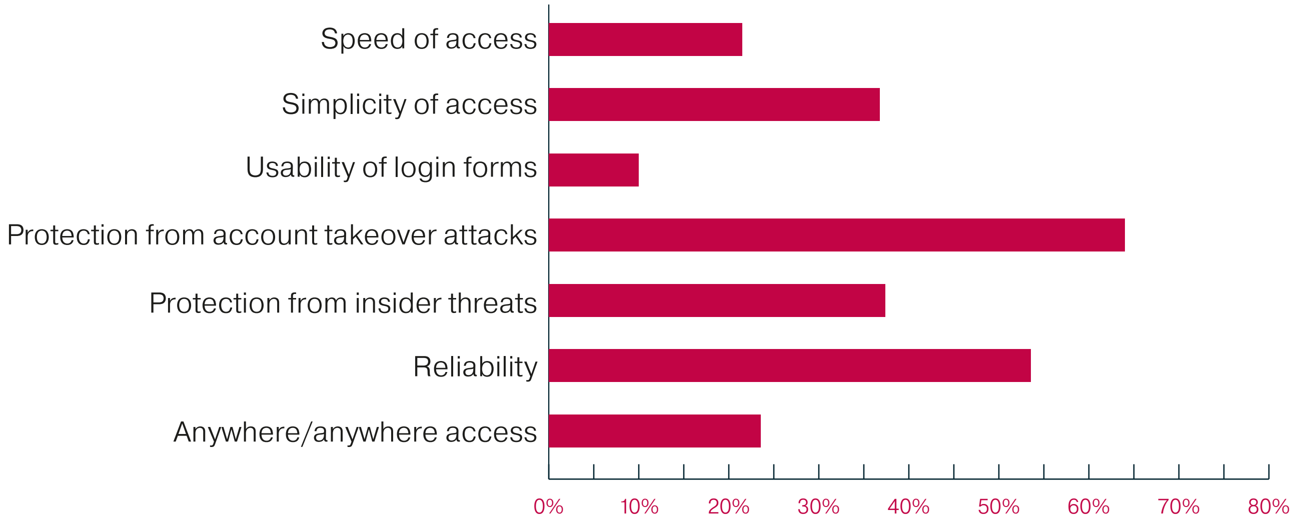
If an employee (of any position) is compromised, a cybercriminal could be able to access everything. This would be easier to control if sensitive data was only accessible by named (or role-based) individuals. It is therefore recommended that the more sensitive the data an organisation has, the more authentication is required.

It's possible to leverage Privileged Access Management (PAM) independently of IAM to manage the access of the most powerful accounts—or privileged identities—within an organisation's IT infrastructure. That said, many modern organisations choose to unify their privileged access policies through their core Identity and Access Management provider. While IAM can become more complex the bigger and more distributed a company grows, many IT teams still choose to establish clear and secure Privileged Access Management this approach.

With a solid identity foundation, organisations can also extend their workforce capabilities through IAM tools like Single Sign-On and Adaptive MFA to boost security, reduce friction, and conquer identity sprawl.

Gus Kilkenny, Infrastructure Manager at J Tomlinson Ltd agrees, "Maintain user's access so they only have access to data they need to do the job. To be sure, review the access you think they have, then adopt a posture of protection - it's not if you will get attacked but when."

When your suppliers/partners log in to your systems, what factors are most important to ensure they have the best access experience?



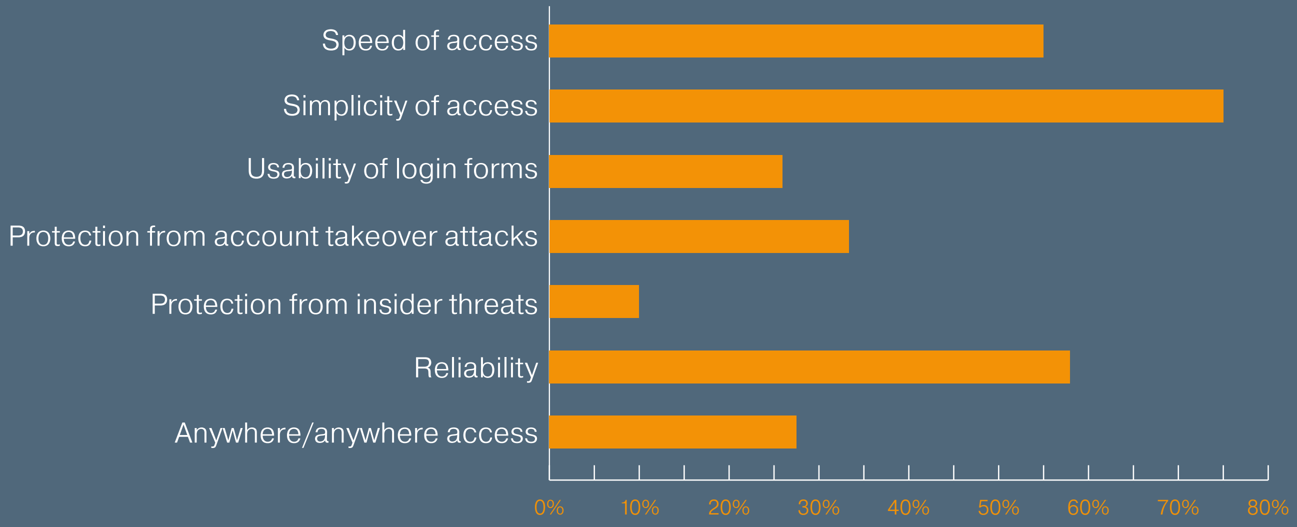
Interestingly, and this is probably due to the fact that the people accessing the systems are suppliers/partners, but security is very high on the list (#1 and #3), so it's logically more important to ensure that people accessing the system are who they say they are.

In line with previous findings, the day of the login form are long gone as they are less secure, slow to complete, and provide for a poor customer experience. From consumer apps, to B2B customer apps, to B2B partner collaboration, to supply chain integration, to support portals, to seamless integration across customer-facing ecommerce sites, to connecting employees to SaaS apps, to providing lifetime access for alumni to university resources, to quickly enabling secure eCommerce.

Organisations want to roll out great new experiences that attract and retain customers while improving their lifetime value.

However, today's endusers are trained by the likes of Google, Amazon and Facebook to disengage to disengage from experiences that aren't technologically advanced, frictionless, omni-channel, and relevant. In order to unify the customer experience and drive engagement, there needs to be an identity layer serving as the connective tissue between apps, devices, channels, and experiences. A modern identity service helps speed up time to market and drive engagement.

When your customers log in to your systems, what factors are most important to ensure they have the best access experience?



Unlike the previous question that was in relation to partners/suppliers, it is no surprise that when it comes to granting customers access to systems, the experience must be a positive one. Simplicity, reliability and speed of access are all deemed the most important. It is therefore essential that the customer experience does not open the organisation up to avoidable threats, as while simplicity and speed are very important, so too are access controls.

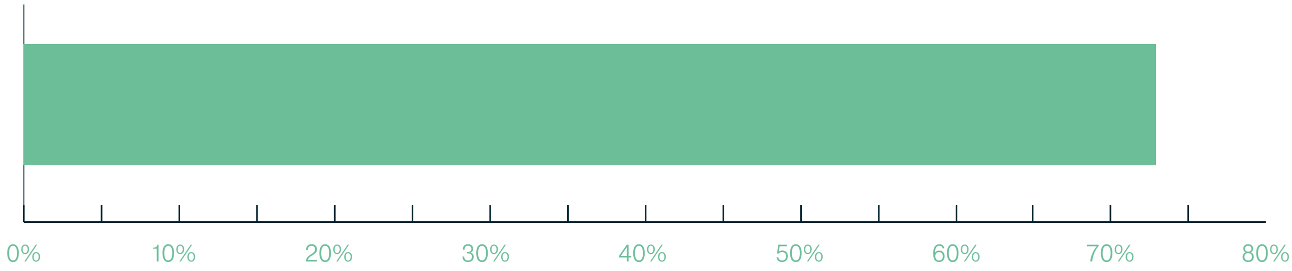
According to research by Digital Shadows, cybercriminals have more than 15 billion stolen credentials to choose from. They take over bank accounts, health care records, company secrets, and more.

In a world where credential harvesting is a constant threat and, according to the Verizon Data Breach Investigation Report, over 80 percent of hacking-related breaches are caused by stolen or weak passwords, risk reduction is critical for organisations, which is why MFA is growing exponentially. This kind of bulletproof authentication solution is essential.

With MFA, it's about granting access based on multiple weighted factors, thereby reducing the risks of compromised passwords. It adds another layer of protection from the kinds of damaging attacks that cost organisations millions.

John Gordon, Infrastructure Engineer at Asco Group suggests to “Get users to partake in Cyber security awareness training so they know what to look out for and to enable full MFA on all user account as well as blocking legacy authentication.”

How confident are you that your user accounts are secure and won't be compromised so customer data and I.P. won't be stolen?



Given the findings in this report, and particularly the findings and commentary earlier in relation to homeworkers and their propensity to let their guard down when working from home, two things can be derived from this confidence score.

Firstly, 73% is probably too high. From our own research and broader studies undertaken, a more likely figure is in the low 50s.

That said, if we take 73% at face value is that good enough? Is it acceptable that IT teams are only 73% confident that their user accounts are secure and won't be compromised so customer data and I.P. won't be stolen? Is this a figure one that organisations would be happy to publicise or share with their customers, or their DPO, or the ICO?

Clearly security is a complex area and where IT teams need to be right 100% of the time, a cybercriminal only needs to be right once. This is why Bytes always recommend a layered approach to security with at least 2-3 different security vendors in place at any one time, as due to GDPR the fines now applicable when a breach occurs are material – and that's before even thinking about reputational damage and lack of customer trust.

Having a robust and secure access solution in place, that allows IT teams to base user access privileges on the role or seniority of the person is a very good place to start, as at least that way if there is a breach, the breach (and associated impact) has a greater chance to be contained. It also means further security policies and authentication measures can be put in place to protect the most sensitive data, so even if a senior employee had their account taken over, the additional authentication measures would kick and limit the threat.

Bytes have an unrivalled level of security expertise and can provide professional advice on the measures organisations should be taking to ensure they are fully and confidently prepared against today's highly sophisticated cybercriminals.

Tim Hodge, CIO at PDSA comments, "Implement MFA and do some analysis of Privileged Access Management."

Key Takeaways

The findings of this report can be summarised as follows:

1. **Providing a great user experience and an efficient access-control security system do not need to be mutually exclusive.** Giving users a simple and fast way of accessing the systems, applications and services they need is easy to do, and by using the right solution, IT teams can be confident that the users only have access to the systems they need, and that users will be less tempted to by-pass the use of official applications and choose instead to use unauthorised Shadow IT services.
2. **Fixing the Home Working challenge needs to be a priority before bad habits become the norm.** Homeworkers are likely to be no less productive when working at home, however, the evidence suggests they are taking unnecessary risks, specifically around the way they are sharing company devices with other members of their household, and also with the way they are accessing company systems via unsecured networks. There is also a greater likelihood unauthorised Shadow IT services are being used to compensate for difficult-to-access company systems which brings with it a whole range of avoidable challenges and risks.
3. **Role-based Identity and Access controls are paramount to ensuring the most secure and robust environment.** Granting access to company systems, applications, services and data assets should not be taken lightly. Anyone that has access to company data can potentially compromise it, whether it be intentionally, accidently, or via an account-takeover attack.

It is therefore important that access is granted only to those people that absolutely need it and that people have access solely to those tools, resources and datasets that allow them to conduct their job role effectively to maximum impact and no wider. If someone mainly uses email and a couple of other basic collaboration tools to do their job, should they be granted access to sensitive customer or financial information?

Tailoring access controls not only limits the associated risk, but also enables IT teams to layer further authentication and security measures around the most sensitive data, so in the case there is a breach, the attacker will only be able to progress so far until further identification is needed. This approach makes it much easier for Management teams to target very precisely where they make their security prevention investments. This helps build confidence in the overarching security strategy and limits the risk of financial penalty and reputational damage should a breach occur.

Future Trends

So what can businesses expect to see next with their Secure Systems Access needs? What threats and trends are we likely to experience in 2021?

We asked top experts to give us their thoughts:

The following Future Trends predictions have been compiled by Jesper Frederiksen and Ben King, both senior leaders in their fields, based on their experiences and visibility of global emerging threats and trends.

About Jesper Frederiksen,
Vice President and General Manager EMEA

As General Manager, EMEA, Jesper Frederiksen is responsible for driving Okta's growth in Europe, the Middle East and Africa. He is also tasked with developing and retaining talent, driving customer success, giving back to the local community and increasing Okta's brand awareness in the region.

Jesper brings more than 25 years of sales, technology and leadership experience to Okta, most recently spending four years with DocuSign, leading the company's expansion across EMEA as Vice President and General Manager. Prior to DocuSign, Jesper held various leadership roles at Parallels, Symantec, Google and NetIQ.

About Ben King,
Regional Chief Security Officer (CSO) at Okta for EMEA

Ben King is the Regional Chief Security Officer (CSO) at Okta for EMEA. As Regional CSO, he leads internal security for the region and provides the operational interface to the global security function. In addition, Ben leads the global Security Assurance function at Okta, responsible for both Customer and Supplier Security Assurance activities.

Prior to joining Okta, Ben operated in a regional cybersecurity leadership role for Symantec, and spent 11 years at the Commonwealth Bank of Australia in a variety technology and cybersecurity strategy and governance roles. Ben has built a reputation for creating and leading high performing teams, having lived and worked in Australia, the United Kingdom, Canada and the USA. He holds a B.S. in Engineering and a B.S. in Commerce from the University of Sydney.

1

How has cyber security changed during COVID-19

COVID-19 has dramatically changed the cyber security landscape, highlighting those organisations that were most unprepared for the mass shift to remote working. With the majority of employees still working from home, workforces are more vulnerable than ever before. Not only are people more likely to click on suspicious links when isolated in their own homes, but attacks are also becoming far more sophisticated, targeting VPNs and other exposed areas of the business. For example, we're increasingly seeing attacks over text messages and personal social media accounts. We are looking at a cybercrime gold rush, as remote IT workers without adequate protection are a gift to cyber criminals. In the current age of remote work, traditional defence perimeters can no longer effectively protect the workforce, and therefore the business.

2

With working routines changing (remote/office/blended) – what do companies need to have in place right now? And in the future?

While we've seen success with organisations quickly scaling remote working security tools, for many this short-term firefighting approach isn't sustainable. Now more than ever, with this new dynamic way of working, businesses need to make security a top priority. Organisations should be investing in security skills and cultivating IT teams that can sustain and keep a remote workforce secure. COVID-19 has highlighted the urgent need for businesses to shift their mindsets when it comes to security, and the increase in cybercrime has accelerated the adoption of frameworks such as Zero Trust. Zero Trust throws away the idea of a trusted internal network versus an untrusted external network; instead, we should consider all network traffic untrusted. The core principle of Zero Trust is to "never trust, always verify." In today's security landscape, it's all about the people who access your systems, and the access controls for those individuals. According to recent polls by Deloitte, 37.4% of security professionals say the pandemic has sped-up their organisations' Zero Trust adoption efforts. The Zero Trust model is so important to implement if businesses hope to keep their workforce secure, no matter where employees log in from.

As part of this, employing rigorous security solutions, such as adaptive MFA is critical to ensuring malicious actors are not able to access sensitive information. It is far easier to identify anomalous activity with a system of at least two factor authentication, as it combines passwords with other factors such as physical tokens, contextual information or biometrics. A password is no longer a satisfactory way to make sure someone is who they say they are, and businesses should not rely only on this method of authentication to protect their workforces.

3

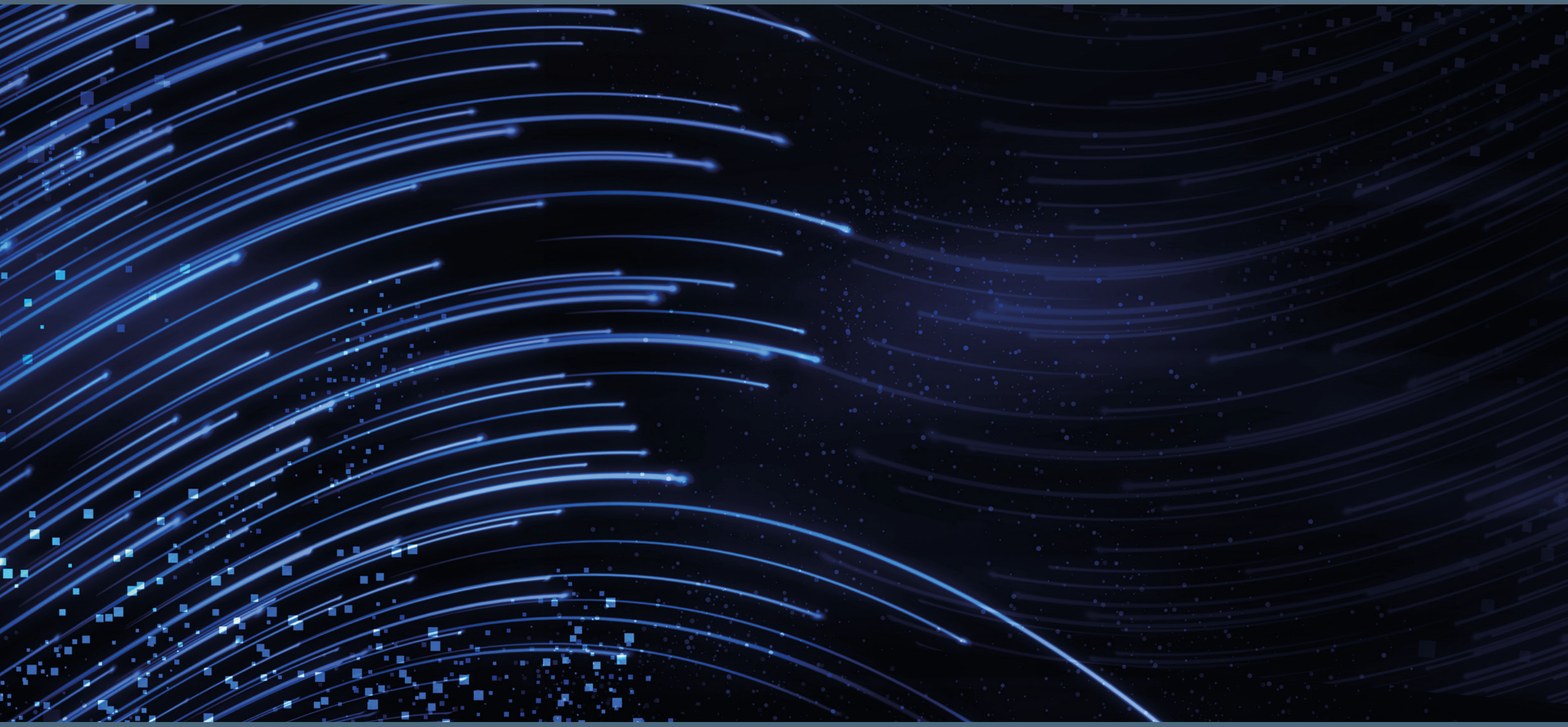
What technologies are needed?

The importance of cloud security skills and secure coding practices will continue to grow at break-neck speed. People thinking of joining the security industry, either from higher education or cross training from other technical roles, should be looking to these areas of learning.

4

What are the best practices for employees to follow?

The importance of cloud security skills and secure coding practices will continue to grow at break-neck speed. People thinking of joining the security industry, either from higher education or cross training from other technical roles, should be looking to these areas of learning.



Do you need help with your Identity and Access strategy?

Bytes Identity and Access Management Workshop

80% of Security Breaches are caused by compromised or weak credentials. Now more than ever, it's important for businesses to understand how to secure user access, balancing the need for 'right now' access to critical resources with business risk and compliance. Working out the correct approach can be complex but is business critical in order to provide yours staff, customers & third parties with just the right access to the right resources in the right place at the right time.

Bytes are here to help. Our Free IDENTITY & ACCESS WORKSHOP is designed to help you map out an Access &Identity strategy for your business which gets the balance between security and convenience right.

We offer guidance on 5 different areas of Identity and Access Management

- Multi Factor Authentication & Single Sign On
- Identity Lifecycle Management
- Identity Access Management
- Privilege Identity & Privilege Access Management
- Identity Governance

Our Methodology:

Our expert engineers work with you to identify your key access challenges and requirements, then walk you through the various options that you have to strengthen your security posture whilst ensuring smooth, simple user access. The result – a clear map of your journey to simple, secure user access at every point of your business – from new staff onboarding to privilege management.

Assess

- ✓ Evaluate current requirements
- ✓ Explore Security roadmap
- ✓ Demonstrate Multi Factor Authentication & Single Sign On

Discover

- ✓ Deliver workshop and knowledge transfer
- ✓ Analyse and discover gaps
- ✓ Consider vendors and offerings

Recommend

- ✓ Align appropriate technologies to create solutions
- ✓ Provide a bespoke solution recommendation report to assist with business cases

What you can expect

- ✓ Interactive 1:1 Session
- ✓ Expert Advice and Guidance
- ✓ Can support multiple stakeholders
- ✓ Sessions run remotely or in person
- ✓ 20+ years experience in Security Optimisation

Enquire about our Identity Workshop today:
tellmemore@bytes.co.uk | 01372 418500 | bytes.co.uk

About Bytes

Bytes provides leading insights, expertise and practical help to over 3,600 organisations nationwide. We enable effective and cost-efficient technology sourcing, adoption, security and management of software, hardware and cloud services.

Our UK business began in 1982 and has grown profitably each year to reach a turnover in excess of £500m, making us one of the largest software services and solutions businesses in the country.

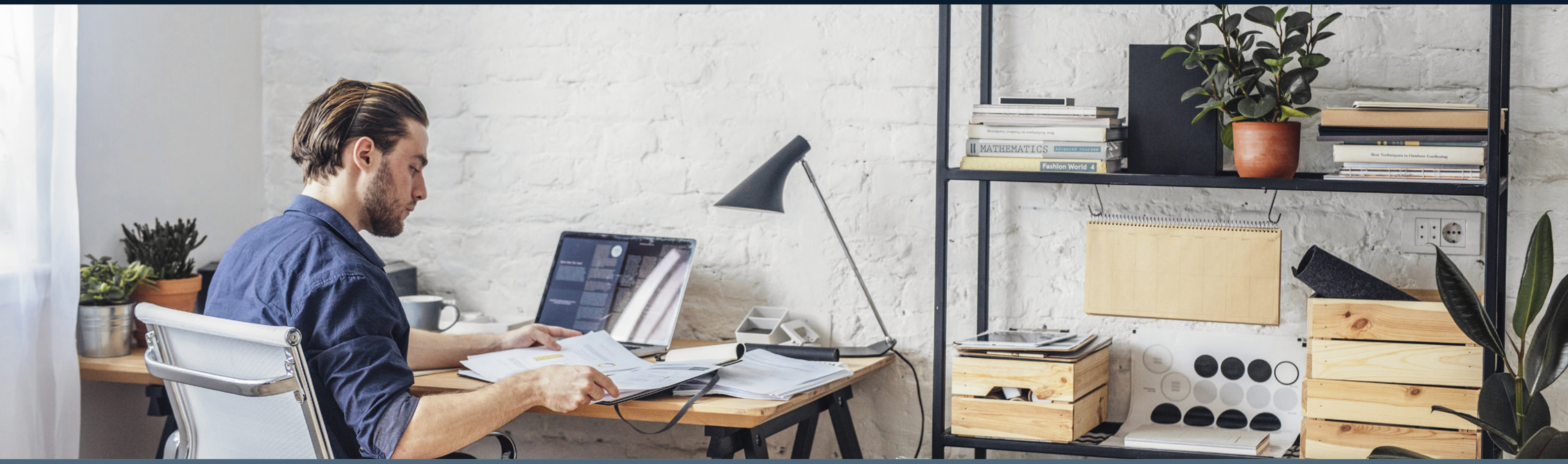
The most important aspect of our business is our people. We value initiative, teamwork and achievement. Together, we focus on providing the highest levels of service so we can deliver our ultimate goal – customer satisfaction and success.

Our customers include leading brands across retail, media, finance, manufacturing, legal, healthcare and the public sector.

We work closely with the majority of IT vendors and are delighted to regularly receive honours from them in addition to being named a Sunday Times Best Company to Work For 2020.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organisations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 8,950 organisations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.



To understand how Bytes can help you develop and enhance your Secure Systems Access Strategy, get in touch and start a conversation today.

BYTES | Smarter together

UK Head Office

Bytes House
Randalls Way
Leatherhead
Surrey
KT22 7TW

T 01372 418 500
E tellmemore@bytes.co.uk
W www.bytes.co.uk