Pulse Secure®

IDG CONNECT

2019 STATE OF ENTERPRISE SECURE ACCESS

ENABLING APPLICATION AND DATA ACCESSIBILTY IN A WORLD OF MULTI-CLOUD AND ZERO TRUST

A report based on exclusive research by IDG Connect on behalf of Pulse Secure

Sponsored by Pulse Secure®

Survey conducted by IDG CONNECT

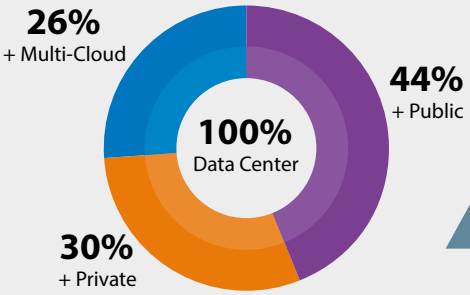
Highlights

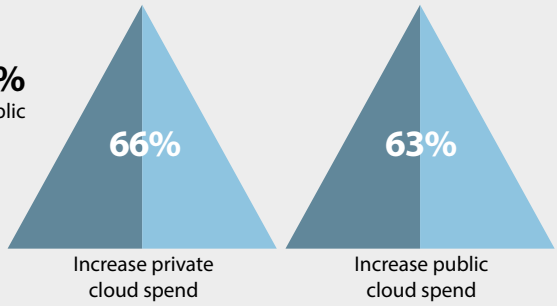
Secure Access spending is on the rise

91%	41%	29%
increased budget through 2021	increasing budget by 5-15%	increasing budget by 15-25%

91% see an increase in Secure Access budgets over the next 18 months, with the majority (41%) seeing 5-15% growth and 29% seeing an increase between 15 and 25%.

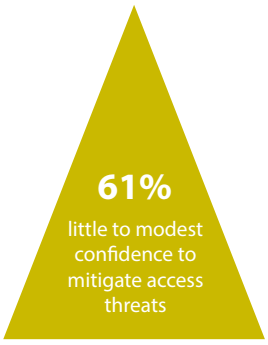
Hybrid IT gains multi-cloud push
44% of enterprises use data center in conjunction with public cloud, 30% in conjunction with private cloud, and 26% utilize all three IT environments. Near-term planned data center spend going down 66%, private cloud going up 63%, and public cloud up 20%.



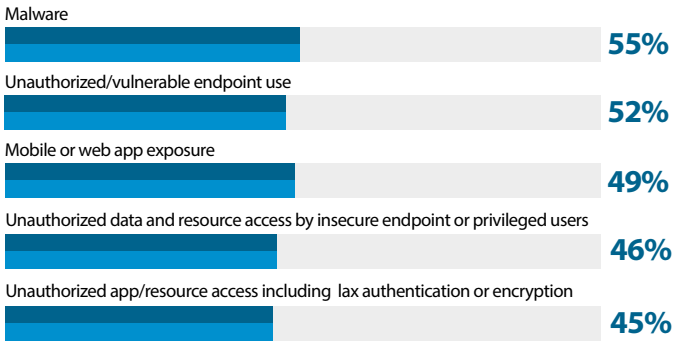


Endpoint exposures among impactful access security incidents

Lack of confidence



Top 5 access security incidents with significant to high impact

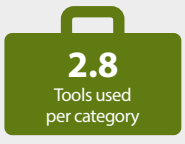


Top IT priorities

Improve endpoint security, remediation prior to access	48%
Enhance IoT discovery, isolation and access control	46%
Fortify network and cloud access visibility and resource segmentation	44%
Refine privileged user or service account-based access	42%
Augment app workload delivery and protection	42%

A case for Secure Access tool consolidation

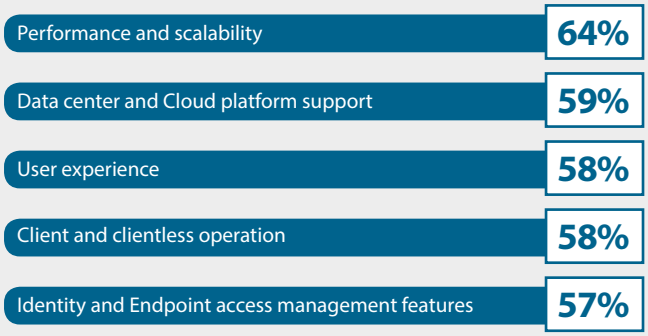
Companies use nearly 3 tools in each secure access category: VPN, MFA, NAC, NGFW, NAC, MDM



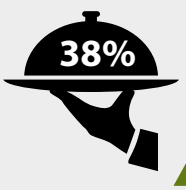
IT open to reduce number of tools and explore suites

Enterprises jumpstart Software Defined Perimeter (SDP)

Top valued Secure Access tool capabilities

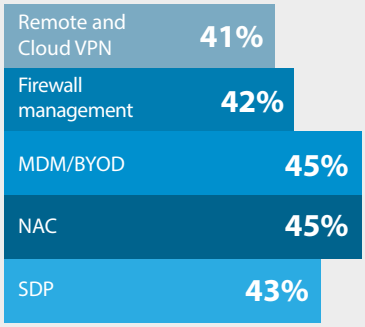


Outsourcing more



Use MSSP for Secure Access

Increased spend in next 24 months



Top Secure Access capabilities outsourced within 18 months

Introduction

IT is more complex than ever today as organizations accelerate digital transformation and broadly adopt public and private cloud infrastructure. At the same time, more enterprises become increasingly reliant on mobile workers, flexible working lifestyles and consumer-like tools, there is a demand for simpler, faster and safer access to data, applications and services from wherever users are located and from any device or platform.

But this demand for accessibility comes at a time when IT departments have never been under so much pressure to defend their brands, intellectual property and the sensitive data of their customers and employees. This has led to a need for increased visibility and oversight as the network perimeter becomes more porous and elastic, and as endpoints grow in number thanks to BYOD schemes and a panoply of devices from desktop PCs to notebooks, tablets, smartphones, kiosks, wearables and the Internet of Things (IoT)-enabled objects.

Given consistent and mounting news of breaches and private data theft, companies are fortifying their security capabilities to prevent and contain cyberattacks. One security model that is gaining momentum is that of Zero Trust. While not trusting anyone or anything is a misnomer, Zero Trust is about "verifying before granting trust". A Zero Trust model authenticates, authorizes and verifies users, devices, applications and resources no matter where they reside. It encompasses proving identity, device and security state before and during a transaction, applying least privilege access controls closest to the entities, applications and data, and extending intelligence to allow policies to adapt to changing requirements and conditions.

A critical component for companies to enable mobile workforce productivity while stemming the tide and scope of security breaches is the use of Secure Access technology. Secure Access, which applies Zero Trust tenets, aims to safeguard data, assets and services by controlling who and what is authorized to use them and how that access is protected. This umbrella category covers a wide range of tools from Firewalls (NGFW), Virtual Private Networks (VPN), Network Access Control (NAC), Cloud Access Security Brokers (CASB) and Mobile Device Management, to Multi-factor Authentication (MFA), Privileged Access Management (PAM), Software Defined Perimeter (SDP) and others.

To gain sharper insight into this changing and growing area of IT security, IDG Connect conducted a survey on behalf of Pulse Secure to gauge activity and perceptions across industries. This report illustrates the current landscape and extent of enterprise Secure Access challenges, practices and risks, as well as the application of technologies to reduce exposures due to endpoint and IoT security threats, unauthorized access, and inconsistent data protection controls.

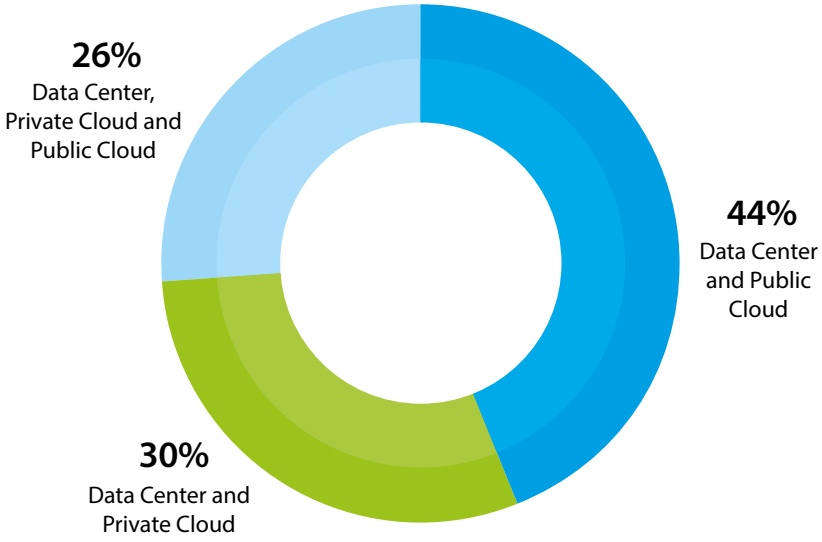
We surveyed over 300 senior security decision makers and influencers across midsize and large organizations in the US, UK and DACH (Germany, Austria and Switzerland) countries to understand:

- Current IT deployment models
- Access challenges, issues and impact
- Practices, controls and tools used to address access exposures
- Secure Access tool usage and value
- The degree of confidence respondents have in their ability to mitigate risks
- How companies plan to invest to fortify access defenses and capabilities

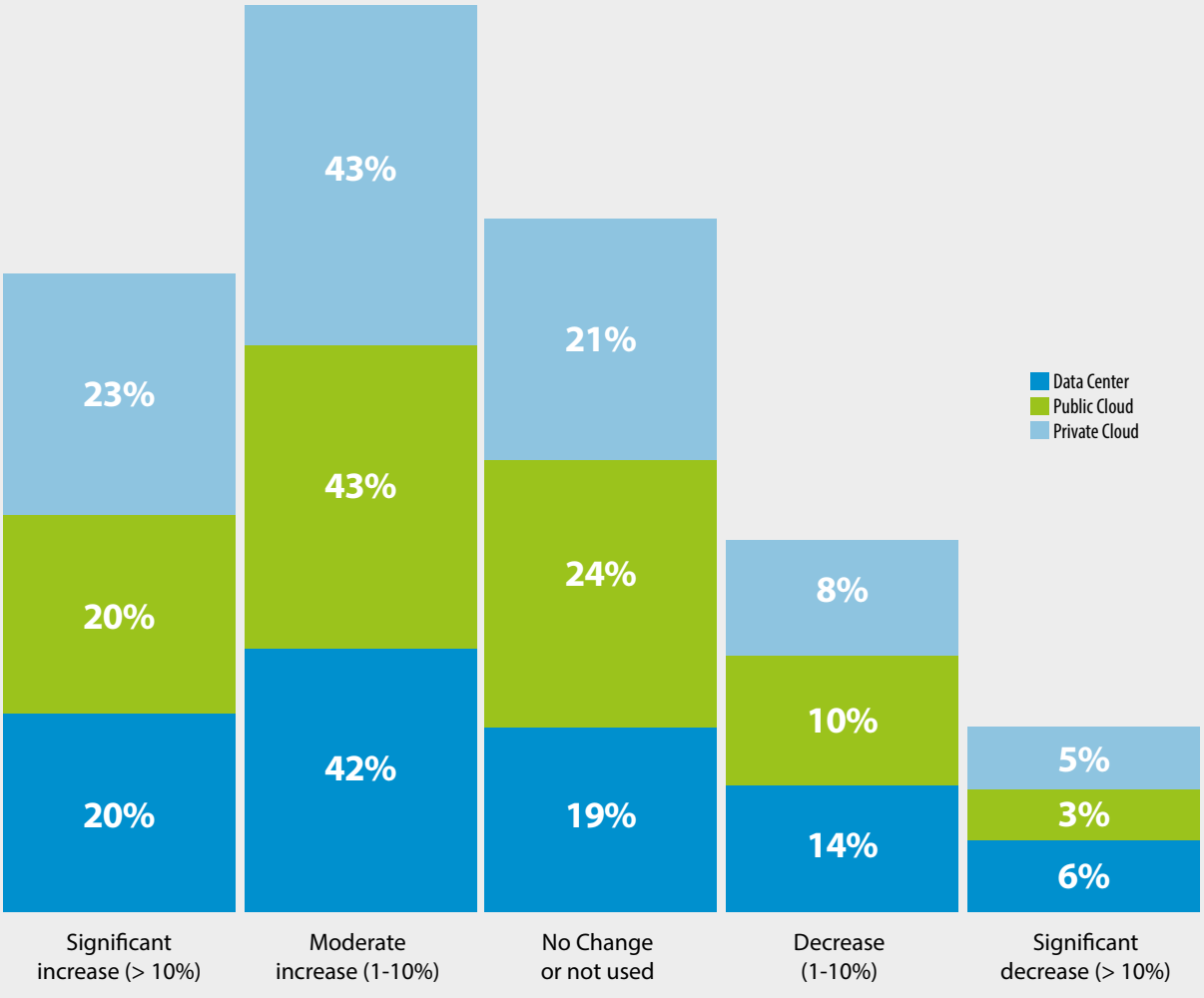
The survey findings and related insights aim to empower corporate leadership and IT security professionals to examine how their organizations are enabling accessibility while mitigating security risks.

Hybrid IT

Preferred IT service delivery model



Planned IT delivery investment



IT's a Hybrid World

To understand our audience's operating environments, we first asked about their organizations' preferred IT service delivery models. The resounding answer that came back was that they live in a hybrid world with every single respondent saying they have a combination of on-premise data center and some form of cloud delivery capability – be that in the form of private cloud or public cloud platform with SaaS applications.

The highest percentage of respondents came from organizations with data center and public cloud as their preferred IT service delivery model (44%). Nearly a third cited data center and private cloud use, with the remainder using all three environments.

The numbers indicate that, despite consistent growth in cloud usage, the notion of the "network perimeter" being a thing of the past is quite wrong. Clearly, there are many applications and resources that reside within corporate networks, and for good reasons.

The research also confirms our assumption that most enterprises today select IT delivery models on a 'horses for courses' basis. They may often choose public cloud for speed of deployment, agility, elastic capacity and a preference for operating expenditure over capital expenditure. Others will stay with conventional, on-premise deployments for complete control over applications, infrastructure and resources, or to have access to optimal performance and governance compliance. Others yet may opt to use private cloud to gain something of each advantage.

While enterprises operate hybrid IT environments, they are investing heavily in multi-cloud support. Over 60% of respondents say they will increase spending over the next 18 months across data centers, private clouds and public clouds. On average, 40% indicate increasing public and private cloud investments up to 10%, and 20% plan to decrease data center spend in the same range.

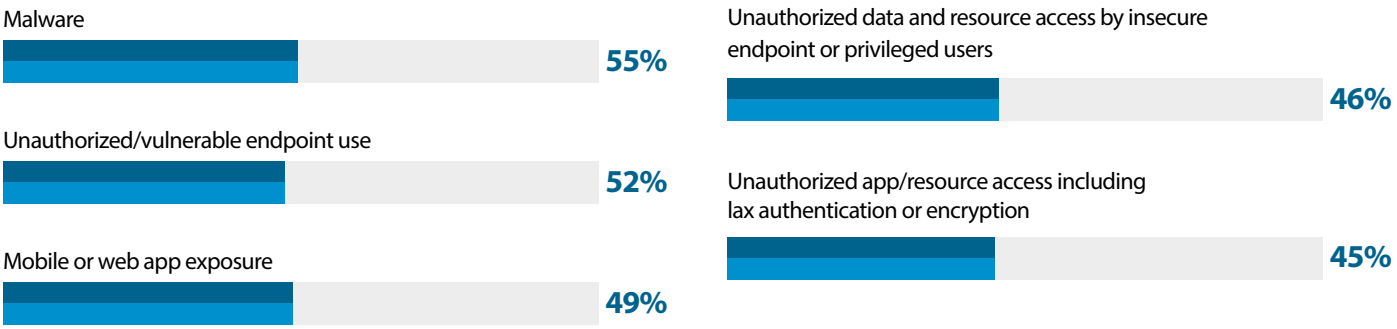
All of this reinforces that Secure Access must support distributed environments and cover all service delivery models.

In detail

US respondents were relatively more likely than other regions to say their preferred model is a combination of data center, private cloud and public cloud (32%). Respondents in the **Finance** sector (32%) and in the **UK** (42%) were more likely to say data center and private cloud was their preferred combination (42%). The **smallest companies** we surveyed preferred data center and public cloud (54%) and the **largest** preferred data center and private cloud (46%), perhaps suggesting the latter's relative sophistication and bigger budgets. **DACH** respondents were relatively the more likely to cut spending across all three areas and **US** respondents were more likely to spend more on public cloud (76%) with the **UK** least likely (43%).

Incidents

Top 5 access security incidents with significant to high impact



Fallout from access security incidents is big and broad

Security breaches are so common today that conventional wisdom states that it's no longer a case of if you get breached but when. But what are the common contributors to access security incidents, and is the problem getting worse?

When we asked about the net impact of access security incidents compared to a year ago, we found that all impact areas saw the large majority of respondents saying they had increased impact. Malware (55%), unauthorized/vulnerable endpoint use (52%) and mobile or web app exposures (49%) had the highest number of respondents reporting significant to high impact. As endpoint vulnerabilities, threats and inadequate security hygiene are among the most prevalent of access security issues, the data suggests a need for better end user education and the use of more automated means to contain or prevent these threats before allowing access to sensitive resources and data.

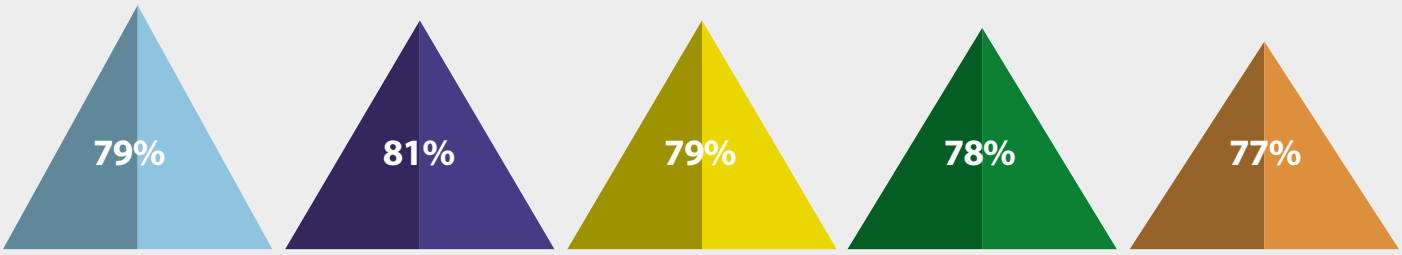
The findings also indicate that issues with poor access authorization (46%) and resource access protection (45%) through lax authentication and encryption are among prominent factors contributing to security incidents impacting organizations today.

In detail

In **DACH** countries, unauthorized resource access by privileged or service user/account had the highest mean relative impact on organizations. In **Finance**, application unavailability, outages and unauthorized data access and data leakage had a higher relative impact on organizations than in other organizations. In **Health/Pharma**, mobile or web application security exposure had a higher relative impact.

Control Gaps

Top access control gaps with significant to high impact



Poor user and device discovery, and mobile computing exposure

Application availability

Uncoordinated authorization

Inconsistent, incomplete enforcement, Weak device access, configuration compliance

Security gateway sprawl, and inconsistent, incomplete remediation

Plenty of access security gaps

Searching for weaknesses in defenses, we asked our audience to highlight the access security control gaps they had recognized recently as being significant and impactful. A large majority said they could identify with the range of access security gaps, and when we narrowed down the field to 'significant' and 'impactful', priority areas became clearer.

Our survey suggests that the majority of respondents are experiencing issues in application availability (81%) in terms of ensuring responsiveness and reliable access for users. This may suggest a need to improve application usage analytics and load balancing automation. Clearly, to reduce access security blind spots requires more automated, granular visibility of users, endpoints and mobile devices – a gap expressed by more than 3/4 of respondents.

Another notable element here is inconsistent enforcement. While enterprises have progressed access policies, endpoint access compliance (8%) and enforcement (78%) controls appear to have waned. This suggests it would be wise to reassess coverage for user and device discovery, as well as authentication and monitoring technologies to mitigate endpoint and access security issues.

The findings also suggest a need to improve processes tied to directory services (6%), which serve as a cornerstone for application and resource access control. Enterprises that do not revisit access security administration and controls will be prone to increased unauthorized access, privacy compliance and sensitive data leakage risks.

In detail

The **smaller** companies in our survey said they have a tougher time than larger companies with maintaining directory services and inconsistent or siloed policy management. **Large enterprises**, on the other hand, indicated they have issues with user and device discovery, mobile computing exposure and inconsistent enforcement. In the **UK**, inconsistent, incomplete enforcement received the highest mean rating. In the **DACH** countries, poor user and device discovery and poorly maintained directory services received the highest mean ratings.

Operational Capacity

Top 5 threat mitigation areas with little to no confidence

Defining app, data and resource access and protection requirements — 22%

Defining, implementing and enforcing user and device access policy — 22%

Provisioning, monitoring and enforcing BYOD and IoT device access (22%) — 22%

Orchestrating dynamic access authentication and protection — 20%

Automating DevOps app delivery — 19%

Define and enforce network segmentation — 19%

Confidence in ability to mitigate access threats is unacceptably low

Despite their having taken many steps and invested quite heavily in tools and preventative measures (as we shall see later), there are low levels of confidence from our respondents in their ability to effect access threat mitigation. Fewer than half of respondents indicated modest confidence in their security processes, human resources, intelligence and tools to mitigate access security threats – while under 35% expressed significant confidence. With stakes so high in information security, organizations can ill-afford to allow operations that yield such paltry levels of confidence.

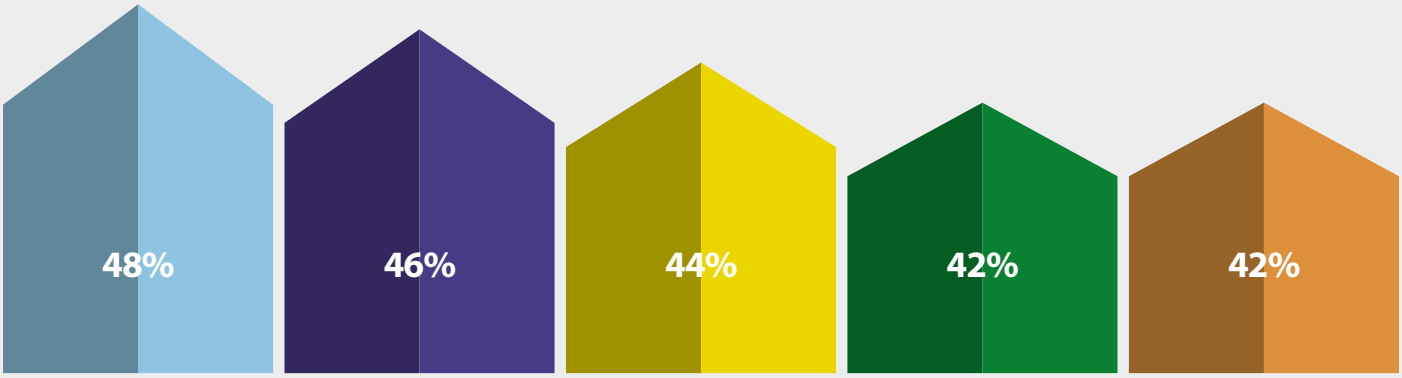
Access policy scope and requirements development (22%), user and device access controls and enforcement (22%), as well as BYOD and IoT access security (22%) compromise the top three concerns where security leadership can focus. Given today's limited budgets for IT and security personnel and increased demand for more responsive services, it makes sense that organizations are looking to explore how to further automate access security. Nearly a fifth of respondents cited low levels of confidence in orchestrating authentication and protection, including DevOps app delivery.

In detail

The **largest enterprises** had more confidence, than that of smaller organizations, in their ability to orchestrate dynamic access authentication, enforce IoT access protection and perform network segmentation.

IT Priorities

Top 5 Secure Access priorities



Improve endpoint security, remediation prior to access

Enhance IoT discovery, isolation and access control

Fortify network and cloud access visibility and resource segmentation

Refine privileged user or service account-based access

Augment app workload delivery and protection

Endpoint compliance leads top priorities in access security initiatives

Where is our audience placing most emphasis on Secure Access initiatives? Improving endpoint security appears to be a top priority across companies of all sizes, but there is a wide range of areas our respondents view as important, perhaps most notably, Internet of Things (IoT) access control. Nearly half of respondents are seeking to be better equipped to discover, contain and provision access for IoT devices, despite this being an area that is still very far from being mature.

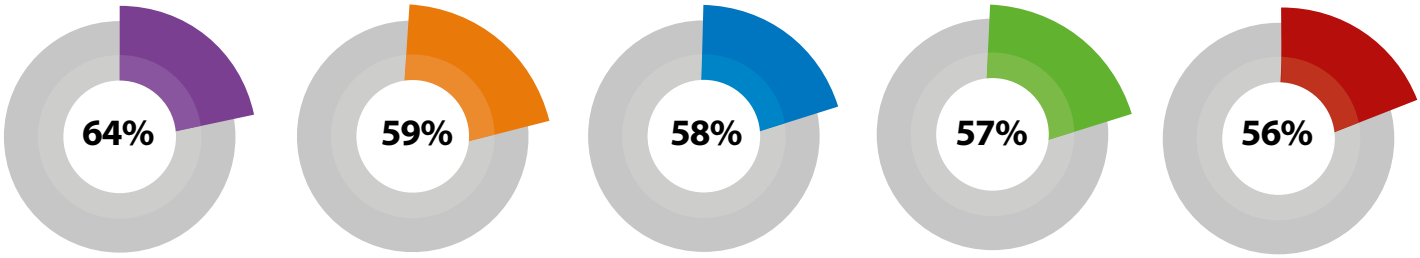
Similarly, the third most popular response – fortifying network and cloud access visibility – illustrates how hybrid IT adoption has also driven the need to consolidate oversight and enable segmentation of applications and resources across data centers and multi-cloud. The more complex, dynamic and distributed the hybrid IT environment, the greater the need to improve access security capacity. This is reflected by initiatives to refine privileged user and service account access management (42%), and to automate access provisioning of respective applications, network, systems and data that comprise a hybrid IT app workload (42%).

In detail

Automate and Invoke Behavior-Based Access Enforcement (40%) and Enable Access Control Consistency Across Hybrid IT Environments (39%) were also cited as top interests among respondents. In the **UK**, improving identity access management orchestration received a relatively significant mean rating as a priority whereas in **DACH** countries, automating and invoking behavior-based access enforcement received the highest mean priority rating. In **Finance**, refining privileged user or service account-based access received a relatively significant mean priority rating.

Tool Considerations

Most valued tool attributes



Overall performance and scalability

Data center and cloud platform support

End user experience and client and client-less operation

Identity and endpoint access management features

Price and ease of administration

Buyers have a need for speed in Secure Access tools

What do buyers want from Secure Access tools? Plenty. But among 14 suggested desirable attributes of these tools, which do they value the most? They're seeking everything from access ecosystem interoperability (49%) and hybrid IT deployment flexibility (59%) options to an unfettered user experience, and identity and endpoint access management features (58 and 57% respectively). However, one answer that stood out was the fact that they demand performance and scalability (64%). Clearly, decision makers are unwilling to trade off speed of authenticated and protected access when it comes to security services.

On a related note, as security decision makers have become more engaged with their business peers, it is not surprising that end user experience made a top five priority (58%). Similarly, ease of administration (56%) is a key consideration for efficient operations. The support for agentless client support also aligns to ease of administration, scale and deployment flexibility. Not surprisingly, value pricing (56%) also made the top five of desired tool attributes.

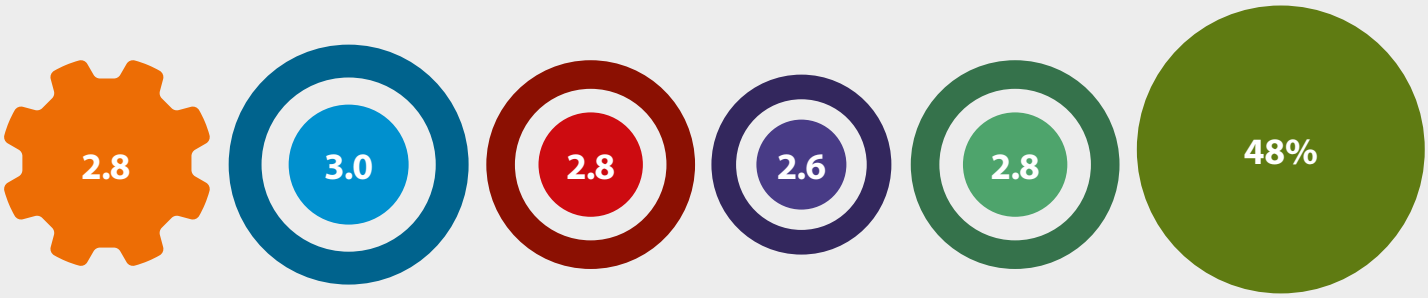
According to respondents, secondary desired tools features include: end-user platform coverage, breadth of authentication and SSO options, and depth of access context visibility and anomaly intelligence. The least important feature cited by respondents, or perhaps the one that buyers feel is a standard, is access ecosystem interoperability.

In detail

Hybrid IT coverage, end-user computing coverage, as well as performance and scale are deemed of relatively higher importance to **smaller** companies in our panel. **Larger enterprises** worry more about breadth of authentication and single sign-on options for hybrid IT, depth of access context visibility and anomaly intelligence, and protected connectivity options – perhaps indicating that performance and scale are understood requirements.

Tool Consolidation

Number of Secure Access tools in use by sector



Companies use nearly 3 tools in each secure access category: VPN, NGFW, NAC, MDM

Health/Medical/ Pharmaceuticals

Hi-Tech/ Manufacturing

Finance/Banking/ Insurance /Investment

Others

Enterprises open to reduce number of tools and explore suites

Multiplicity of tools leads to complexity

Of more than 13 types of Secure Access tool presented to the survey participants, on average, companies use at least two of each type, and large organizations use more than three of the top five tools: VPNs, next-generation firewalls, CASBs, NACs and MDM suites.

This underlines the way that enterprises have amassed a variety of duplicate Secure Access tools or capabilities by way of addressing new threats, feature activation, decentralized purchasing authority, compliance requirements or acquisition. The resulting tool smorgasbord leaves enterprises to cobble together a piecemeal access security strategy in order to support their distributed environment and business needs.

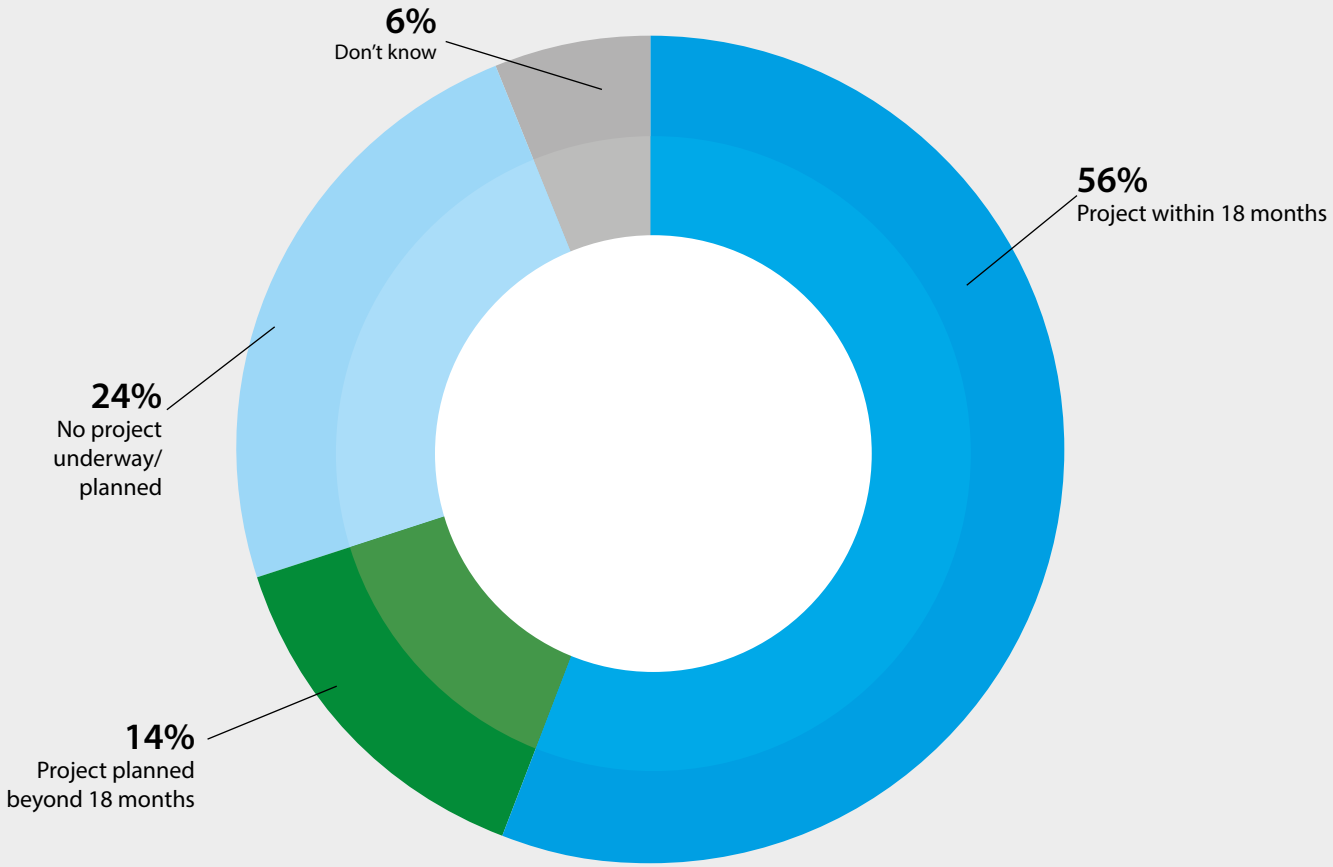
This scenario contributes to complexity for users and administrators, visibility, audit and security gaps, delayed threat response, and increased costs. Unsurprisingly, the issue of 'tool sprawl' is particularly applicable to larger companies that have about 30% more tools than SMEs. As indicated in the IT priorities section (above), where the response 'enable access control consistency across Hybrid IT environments' was cited by more than a third of respondents as a top interest, it's time for enterprises to consider tool consolidation and standardizing on integrated platforms. Nearly half of respondents indicated that they would explore Secure Access platforms/suites.

In detail

Large companies with over 20,000 staff will use over five tools on average for cloud access security. Smaller companies with 1,000-2,500 staff will use five or more tools for VPN access. In **High Tech / Manufacturing** the highest number of tools used (four) comes in mobile security.

Software Defined Perimeter

Growing plans for SDP projects (or pilots)



Software Defined Perimeter technology gaining interest

Interest in Software Defined Perimeter (SDP) technologies for multi-cloud access is clearly growing. SDP enables secure access directly between the user and their device to the application and resource. Like perimeter-based VPN technology, SDP invokes user, device and security state authentication controls before and during an authorized, protected connection.

When asked to what extent their organizations anticipate implementing SDP technologies, more than half of respondents indicated they will commence or pilot an SDP project within the next 18 months; an additional 24% said they anticipated plans in the future. A quarter had no plans and only a small minority were unfamiliar with the technology.

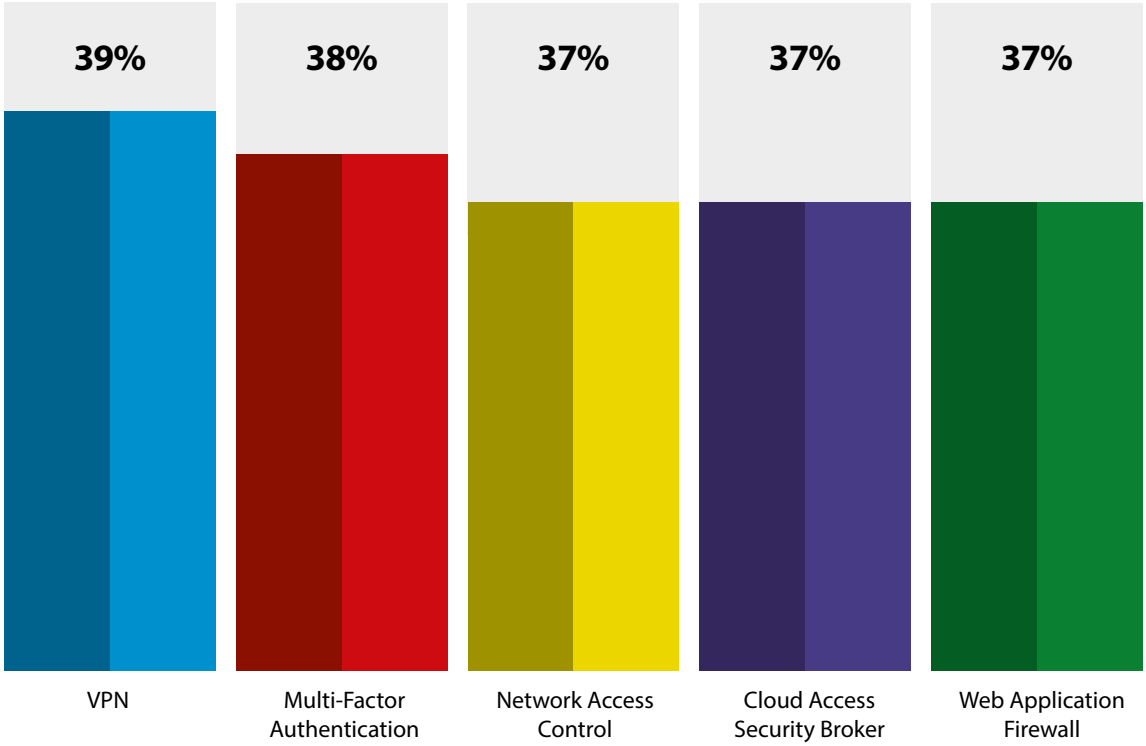
As indicated earlier, the interest and anticipated growth of SDP likely reflects IT adoption and investment in multi-cloud environments.

In detail

Smaller companies and those in the DACH region are significantly less likely to have an SDP project planned. 65% of companies with **2,500-4,999** staff have a project planned within 18 months.

Platform Value

Tools considered as best suited for Secure Access Platform



Organizations considering platform advantages

IT organizations are consolidating tools and exploring platforms as a way to gain operational and cost efficiencies. We asked our audience which tools would have greater value as part of a Secure Access platform or suite. The leading answers were VPN (39%), Network Access Control (37%), Cloud Access Security Broker (37%), Multi-Factor Authentication (38%) and Web Application Firewall (37%).

Perhaps surprisingly, privileged access management (30%) and single sign-on (31%) were perceived as offering the least value as part of a platform. Possibly, this is because our respondents felt that these were discrete capabilities or no longer represented a challenge.

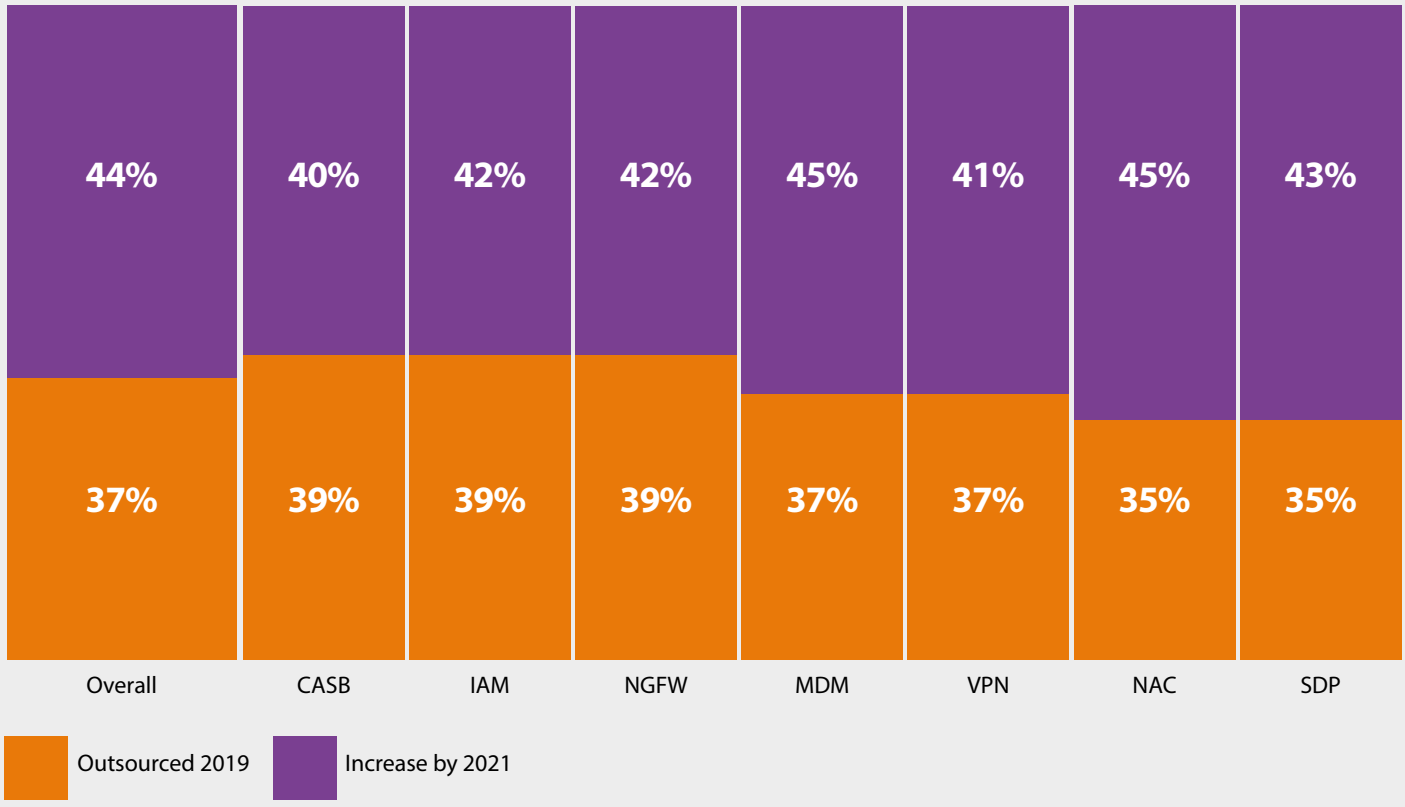
As highlighted in the tools sections, enterprises should assess their current Secure Access tool portfolio: the degree of redundant or limited capabilities of each tool and respective means to satisfy business and audit requirements. Beyond coverage, visibility, control and management functionality, Secure Access suites can yield demonstrable integration, administrative, support and cost benefits.

In detail

In **Hi-Tech/Manufacturing**, mobile security, NAC and Software Defined Perimeter (SDP) received relatively significant mean weights for 'possible value' within platform. In companies with **1,000 to 2,499** employees, a significant percentage of respondents understand the value of VPNs and web application firewalls within a platform.

Outsourcing

Secure access functions outsourced (current and planned)



Secure Access managed services are being used now, and they're growing

Utilizing Managed Security Service Providers (MSSP) is an understandably attractive option to those organizations with limited focus, expertise, time and funds. But to what extent are enterprises turning to managed security service providers to fortify or outsource their access security capacity. To gauge adoption, we asked our audience what types of Secure Access functions they outsource today and what they plan to outsource in the near-term future.

Over a third of those polled outsource some of their access security functionality. The top three outsourced services were CASB (43%) , IAM (39%), and NGFW (39%) then followed by MDM (37%) and VPN (37%). According to our poll, this trend to outsource is likely to increase 7% over the next couple of years.

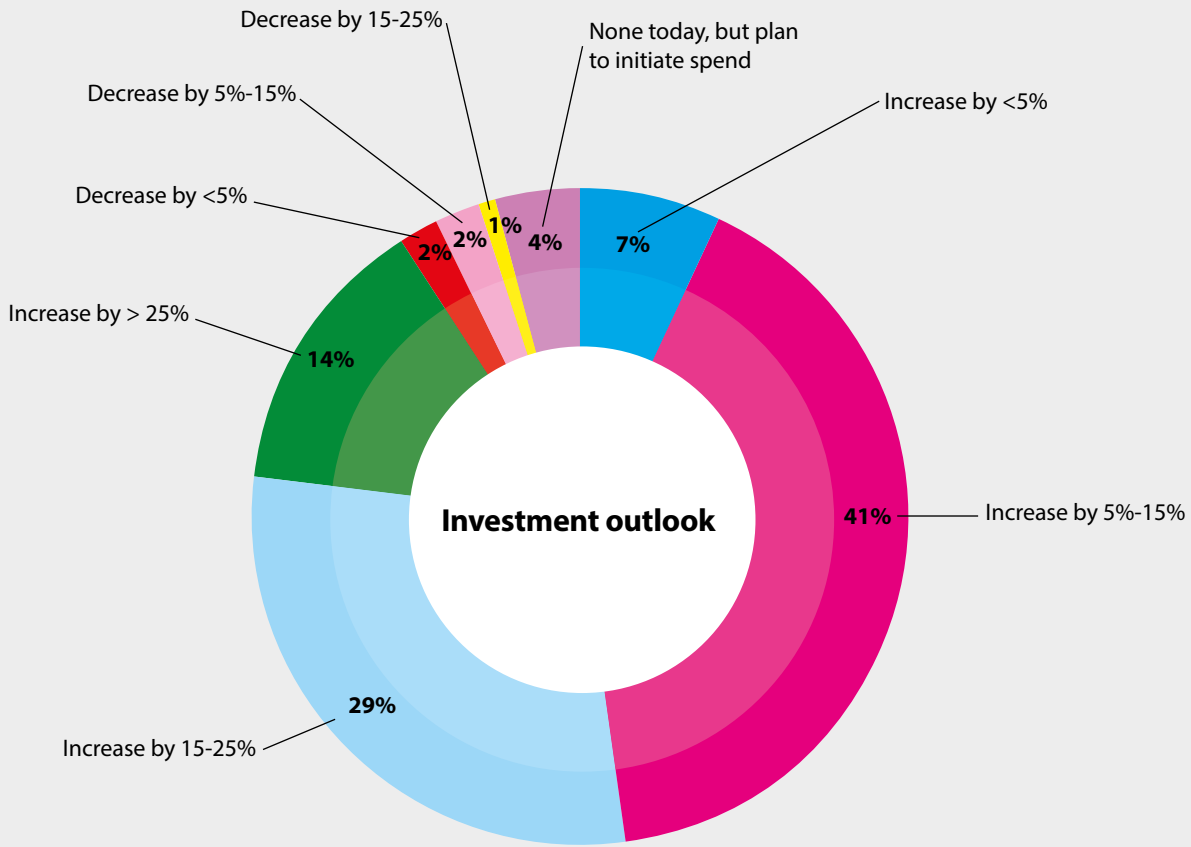
Most organizations are currently outsourcing or plan to outsource firewall protection. Overall, respondents indicated that NAC was highly desired to be outsourced, which may reflect the nature of that technology's perceived complexity. One emerging Secure Access function that is projected to rise sharply over the coming 24 months is that of SDP – given that most commercially available SDP solutions are only offered as SaaS implementation.

In detail

Largest companies with over 20,000 staff are more likely to outsource firewall and mobile device management. **Over half of health/pharma** sector respondents outsource mobile device management and BYOD schemes.

Investment

Enterprises are upping their investments in Secure Access



Percentage of respondents

Spending on Secure Access is northward-bound as enterprises see clear benefits in enabling trusted, protected access to applications, services and data across data centers and multi-cloud. Over 90% of our audience foresee an increase in Secure Access expenditure over the next 18 months, with the highest proportion seeing an increase between five and 15%. A healthy number (14%) is anticipating greater than 25% investment.

Only 5% of respondents see a decrease in spend and 4% indicated no increase. The picture being painted by our audience is one of a security category seeing robust growth, especially as IT budgets are only growing marginally on an annual basis. But organizations' acute need to enable a mobile workforce, the use of IoT devices, and the increase in cloud adoption today is demonstrating renewed investment in Secure Access approaches.

In detail

While a distinctly higher percentage of **US** respondents expect investments in Secure Access tools and services to increase by 5-15%, a higher percentage from other locations expect an increase of over 15%. **Mid-tier and enterprises** appear to have the more significant increase between 5%-25%. Almost a fifth of **Health/Pharma** respondents anticipate and increased of over 25%.

Conclusion

Re-think your Secure Access strategy

The world is not flat, the sky is not falling, and the perimeter is not dead. Our findings to the contrary are that enterprises have made material outlays in perimeter security and remote access capabilities, and as such, access to data center apps and resources will continue to migrate to the cloud. With increased investments in public and private cloud infrastructure, the shift in how organizations deliver hybrid IT services to enable digital transformation initiatives must also take into consideration empowering a mobile workforce; supporting consumer and IoT devices in the workplace; and meeting data privacy compliance obligations – all making it a challenging environment to ensure, monitor and audit access security.

IT organizations at least recognize the need for corresponding investments in access security solutions. The survey showed that over 90% of respondants plan to increase their secure access technology expenditure, with the majority (41%) seeing 5-15% growth and 30% seeing a rise between 15 and 25%. Few (<10%) anticipate flat or declined spend. Even with current and planned investment, fewer than half of respondents indicated modest confidence in their security processes, human resources, intelligence and tools to mitigate access security threats – while under 35% expressed significant confidence.

The research points a clear picture where we see that control gaps are yielding endpoint and access exposures and impactful security incidents. Organizations are experiencing malware (55%), unauthorized/ vulnerable endpoint use (52%) and mobile or web app exposure (49%) incidents. In addition, unauthorized access due to poor endpoint or privileged user issues (46%); or poor authentication and encryption application (45%) are also taking a toll on enterprises.

How can these security issues be addressed? One place to start is to identify what control gaps to focus on. Survey respondents cited lower confidence in application availability (81%). While user experience is an important component of access, you can't manage what you can't see – in this regard, issues on granular visibility of users, endpoints and mobile devices (79%) are apparent. Additional identified control gaps that are material to reducing access incidents are endpoint access compliance (79%) and enforcement (78%).

How did the expressed access incidents and control gaps result in renewed priorities and tool requisites? Improvements in endpoint security and remediation, IOT security, network and cloud visibility, privileged user and service account access, and app workload delivery rose to the top cited priorities (each received over 42% response). When it comes to enterprise toolsets – beyond performance and scalability, respondents focused on interoperability, hybrid IT support, user experience, and identity and endpoint access management as key desired features (each over 56%).

The findings also indicated a clear business case for Secure Access tool consolidation as companies reported use of nearly three tools in each leading product sub-category. As expected, larger companies tend to use 30% more tools than small to medium enterprises. The greater the number of tools, the more likely larger operational complexity, issues and costs.

This scenario contributes to complexity for users and administrators; visibility, audit and security gaps; delayed threat response; and increased costs. For those looking to take advantage of consolidation, respondents incidated that likely candidates for platform offerings would comprise VPN, MFA, NAC, CASB and WAF (37% or higher response). One relatively new cloud access technology of particular interest is Software Defined Perimeter (SDP), where over half (56%) of respondents plan to start an SDP project within 18 months.

Another opportunity for enterprises to augment their access security capacity is the use of managed services: outsourcing is in with 37% of Secure Access functions being outsourced today employing MSPs, and more growth is expected to follow of at least 7% anticipated over the next 24 months.

We also saw some differences across geographies in both deployments and in security measures. To give just a few illustrative examples, in the US, we observed high levels of using a combination of data center, private cloud and public cloud. Americans were more likely to worry about inconsistent or incomplete remediation and uncoordinated authorization while the British were relatively more likely to fret over mobile computing risks. DACH region respondents were more likely than other areas to reduce IT delivery spending but felt fairly confident in their ability to enable and enforce BYOD access.

The same went for industries, reflecting varied concerns and actions. For example, Finance respondents were, like the US, more likely to rely on all the main deployment options than peers in other sectors. Health respondents saw poorly maintained directory services as a major challenge.

Conclusion Continued...

High-tech/Manufacturing respondents felt more confident than many others in their ability to automate DevOps apps delivery.

But what was consistent across countries, sizes or organization and sector was that access security for hybrid IT is a current and growing concern with requirements and threats emerging from many sources. For organizations that have not recently examined or established more coherent Secure Access initiatives, our research suggests that now is the time to re-assess their business requirements, processes, control coverage, capacity and technology in order to prevent exposures and mitigate risks.

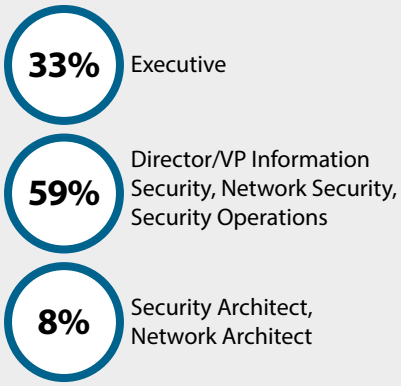
Disclosure

Details of this report

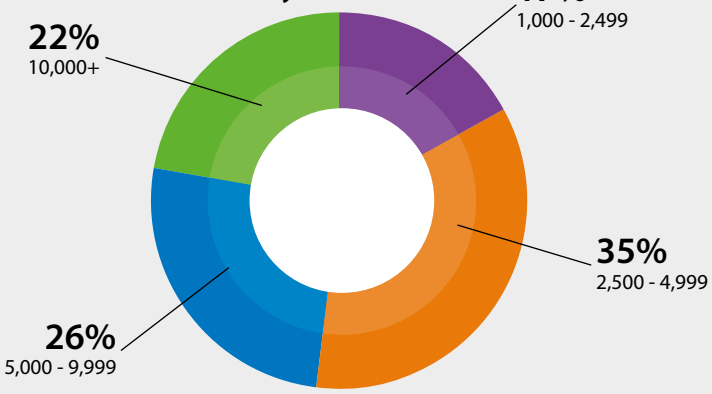
Research was conducted using an online survey which polled over 300 respondents from the US and Europe; 56% of respondents were from the US and 22% each were from the UK and the combined DACH countries of Germany, Austria and Switzerland. The results were collected and analyzed in the spring of 2019. Respondents were information security purchase decision makers within organizations of over 1,000 employees, and spanned industries including financial services, healthcare, technology, and manufacturing.

Demographics

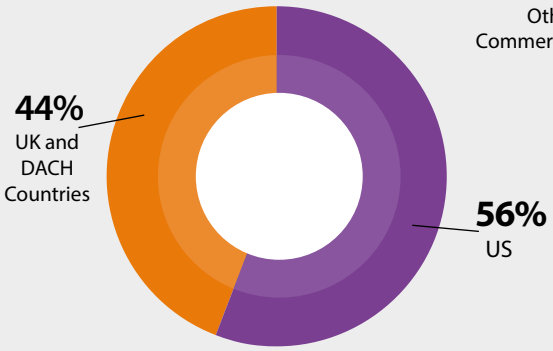
Respondents



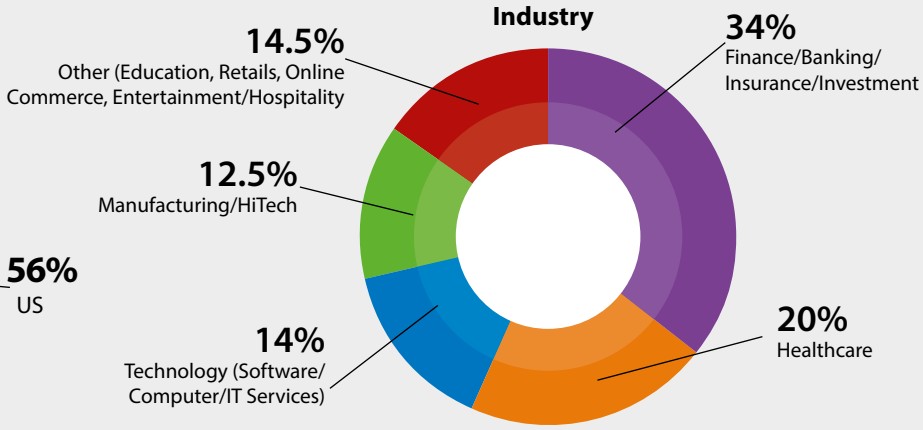
Organization size by headcount



Region



Industry



Sponsor: Pulse Secure, LLC

Pulse Secure provides easy, comprehensive software-driven Secure Access solutions for people, devices, things and services that improve visibility, protection and productivity for our customers. Our suites uniquely integrate cloud, mobile, application and network access to enable hybrid IT in a Zero Trust world. Over 20,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net and follow Pulse Secure on Twitter or visit or visit us on LinkedIn and Facebook.

Research: IDG Connect

IDG Connect is a division of International Data Group (IDG), the world's largest technology media company. Established in 2006, it utilizes access to 44 million decision makers' details to unite technology marketers with relevant targets from 147 countries around the world. Committed to engaging a disparate global audience with truly localized messaging, IDG Connect also publishes market-specific thought leadership papers on behalf of its clients and produces research for B2B marketers worldwide. Visit www.idgconnect.com

Attribution

Use of this report and the respective data, in whole or in part, must be unaltered and must reference the sources as: "2019 State of Enterprise Secure Access" by IDG Connect and Pulse Secure.