2023

Nemertes

Better data. Better decisions.

Appgate SDP: Driving Value Through ZTNA

Nemertes' Real Economic Value study independently evaluated the business and operational impact of Appgate SDP, a Zero Trust Network Access (ZTNA) solution. Through detailed interviews with technology professionals who use the product to provide granular, dynamic, secure access to organization resources, Nemertes has quantified the real-world benefits and improvements Appgate SDP brings to these organizations.

By John Burke, CTO

Nemertes

April 2023

Table of Contents

1. Executive Summary

This research study was based on interviews with technology leaders at medium to large U.S. and multinational organizations from a broad range of industries. The interviews focused on understanding and detailing their use cases for Appgate SDP, a Zero Trust Network Access (ZTNA) solution, and on quantifying its operational and strategic benefits to the organization.

Overall, we found that Appgate SDP helped these organizations deal effectively with a rapidly evolving, complex, and sophisticated array of cybersecurity threats and requirements, in four important ways:

1. Appgate SDP made organizational security better: using it reduced the number of security incidents and exposure to threats while also providing fine-grain control of access privileges to systems and automatic enforcement of least-privilege Zero Trust access principles.

2. Appgate SDP made better security easier: specifically, it made more precise privileges easy to assign, and made it easier to manage changes to privilege assignments over time.

3. Appgate SDP made better, easier security faster: cybersecurity and operations teams could both set up account privileges and make needed changes faster than before, and were able to automate more account and privilege management operations.

4. Notably, and importantly for beleaguered IT teams, Appgate SDP made better, easier, faster security simpler: it reduced the number of access management tools needed—while providing a higher level of security—and also reduced the amount of hands-on staff time needed to manage access.

Key Operational Impacts

All participants reported measurable improvements in at least one important operational metric, ranging from the number of cybersecurity incidents to time spent modifying cloud users' access rights. We also saw that Appgate SDP was instrumental in advancing Zero Trust initiatives.

- 83% saw significant reduction in security incidents after deploying Appgate SDP
- 62% average reduction in the time to properly provision access rights on new accounts
- 87% average reduction in time to modify access privileges for an account
- 32% average reduction in the staff hours needed to manage remote access
- 55% average reduction in the number of tools used to manage on-premises access (among those not already down to 1)
- 85% of servers (on average) in organizations' Zero Trust environments protected by Appgate SDP

2. About the Study

For this research, Nemertes interviewed technology leaders at U.S. and multinational organizations during a four-month period, October 2022 – January 2023. Nemertes analysts interviewed all participants—there was no use of online surveys or phone-bank interviewers. As needed, interviews were followed up via email to confirm our understandings or gather additional data.

All participants used Appgate SDP in their production environments at the time of the interviews.

The participating organizations were mid-sized to large, with an average employee count of 50,000 and annual revenues (or operating budgets, for non-profits) of $31 billion. Participants came from verticals including retail, manufacturing, financial services, software, professional services, and the federal government.

Participant organizations also tended toward the strategically minded when it comes to technology adoption. (Please see Figure 1.) The majority of the organizations (67%) consistently look at IT as a strategic investment, something they engage to be competitive with their peers. Another 11% go further and look to technology investments to give them a sustained competitive advantage. The remaining 22% are more moderate, seeing only a few specific technology investments as strategic. None identified as technologically conservative, seeing IT strictly as a "cost of doing business" and not strategic.

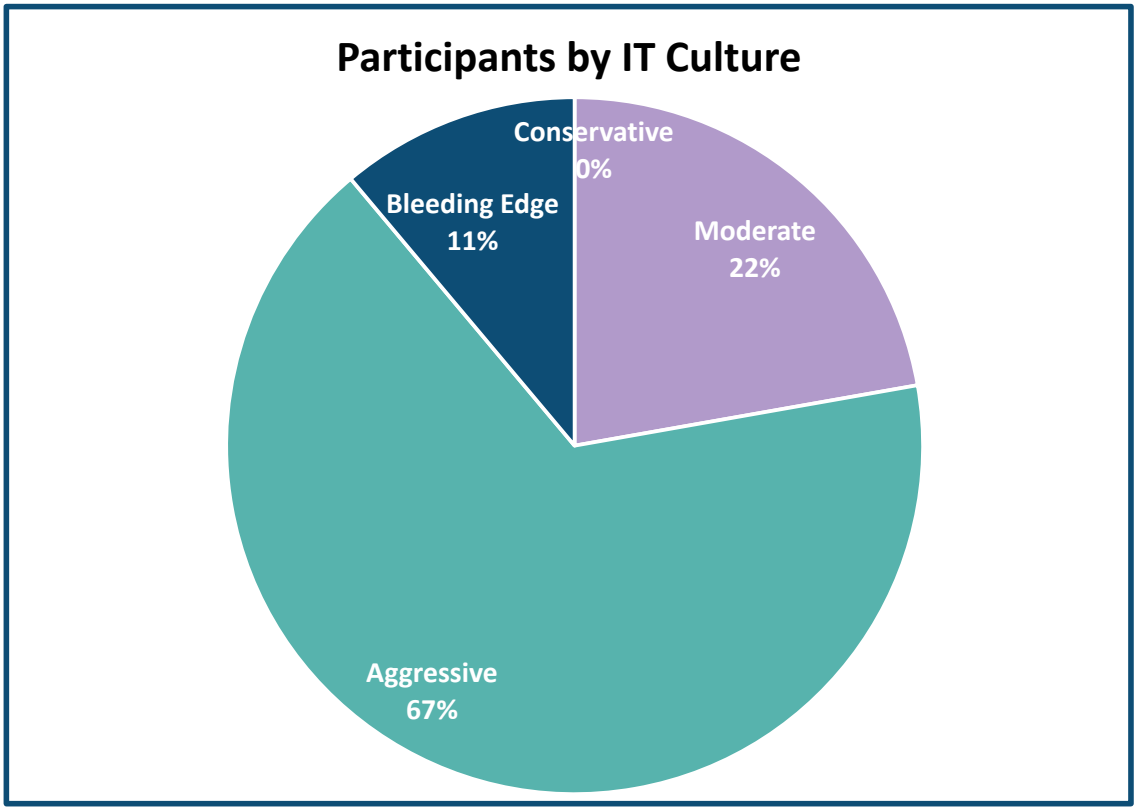


Figure 1: Participants by IT Culture

3. Adoption: Drivers and Use Cases

Appgate SDP controls network access to organizational resources; a person or system not explicitly authorized to use a resource will not be able to see or reach that resource on the network.

Around that fundamental function, organizations deploy Appgate SDP to meet the needs of specific use cases. We say "specific use cases" and not "a specific use case" because every participant had multiple use cases in mind when acquiring and deploying it. (Please see Figure 2.). Bringing in one tool for multiple purposes helped participants simplify cybersecurity operations and toolsets.

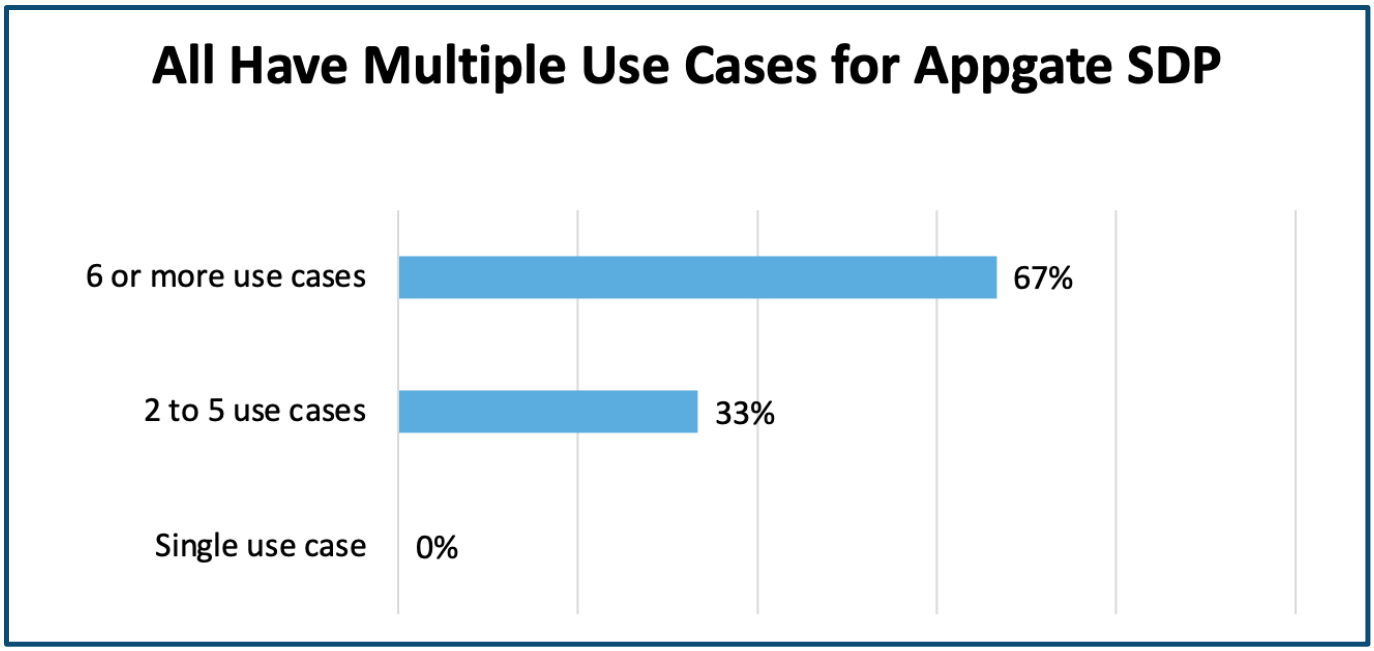


Figure 2: Appgate SDP for Multiple Use Cases

3.1 Use Cases

Given Appgate SDP's core functionality, it is no surprise that half of the use cases participants cited revolve around managing resource access for different sets of users. (Please see Figure 3.) It is also no surprise, given the recent pandemic, that every participant named the problem of managing access for remote employees as a reason they brought Appgate SDP on board. Nearly as many, 89%, were also focused on managing access for cloud users. "We're in the process of shutting down our last data center," said the Principal Enterprise Architect at a midsize software and IT services company, "and Appgate is in front of IaaS and SaaS both. [It] made moving to IaaS easy by providing a seamless access layer for users, and to modularly add new cloud platforms under the hood, transparently."

Looking for leverage on a perennially difficult problem, 78% deployed Appgate SDP to get, or improve, the ability to manage access for third-party users, such as contractors and partners. "[Our] existing remote access solutions did not allow third-party contractors to get access to our assets," said the Cloud Solution Architect at a large professional services company.

The same portion, 78%, were focused on managing access for on-premises employees. “We plan to evolve this as a full ZTNA product, understanding that ZTNA is a journey,” said the Director of Enterprise Infrastructure at a large manufacturer.

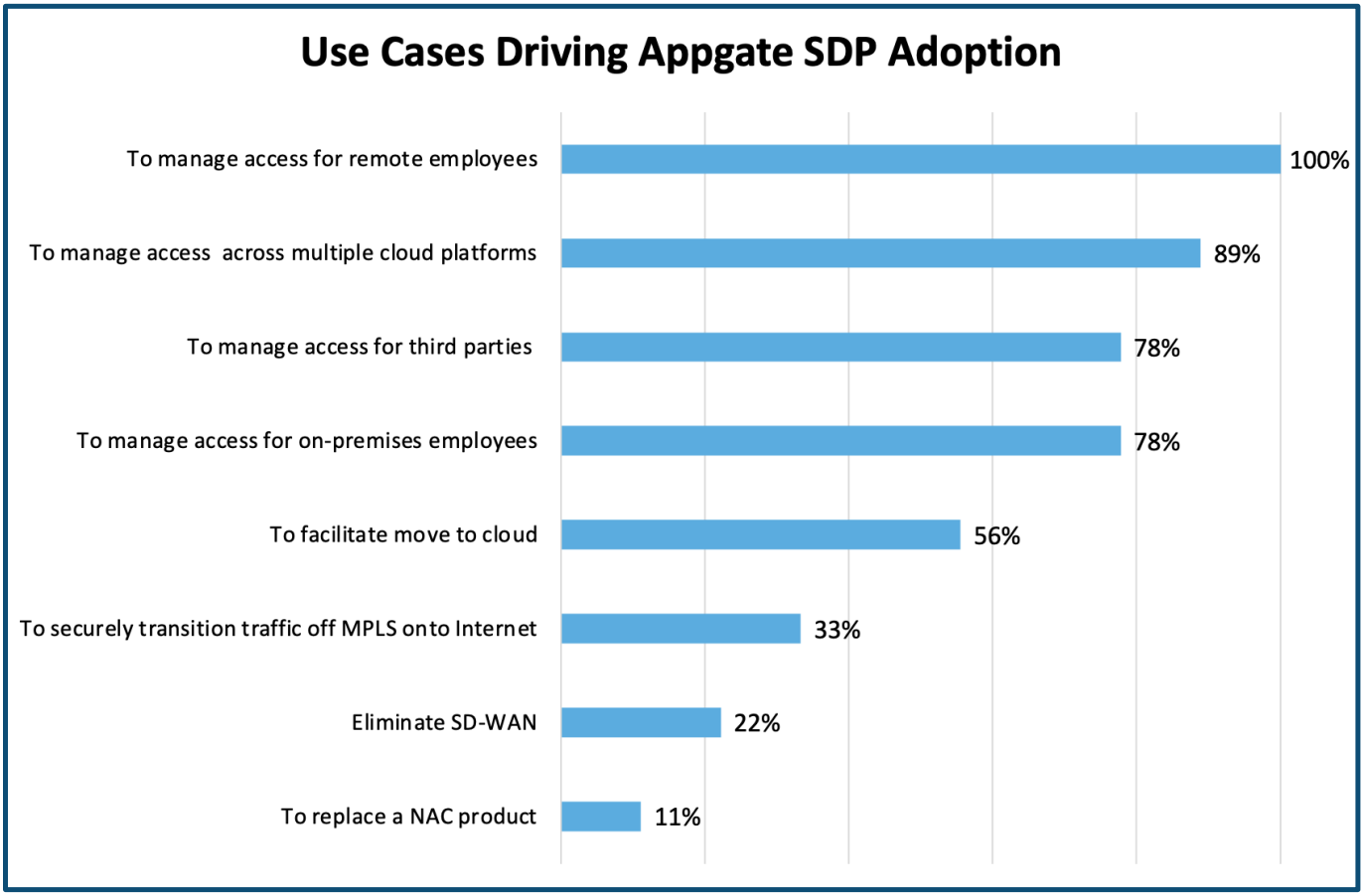


Figure 3: Appgate SDP Use Cases

This set of use cases represents an adoption arc most organizations using Appgate SDP had followed or were in the process of following: most began with remote user management, often driven by dissatisfaction with legacy VPNs, then proceeded to other ZTNA use cases.

Beyond the baseline problems centered on managing user access to resources, organizations have adopted Appgate SDP to serve broader strategic goals in IT and cybersecurity. Over half (56%) adopted it in part to advance their broader strategy of moving more resources to the cloud, allowing them to maintain extremely tight access controls without any change in how users get to resources and simplifying how administrators manage access.

Less commonly but very significantly, participants brought Appgate SDP in to help them transition off older network and security technologies.

- A third brought Appgate SDP in part to help them ease MPLS out the door: they no longer needed an MPLS WAN with all its associated expense if they could use ZTNA to easily and transparently secure all communications among users and systems over the Internet. Given they were rolling Appgate SDP out anyway, they saw no need to continue paying for both.

- Another 22%, having already transitioned to SD-WAN, were similarly using ZTNA to eliminate the need for their SD-WAN solution so they could retire it.

- Lastly, 11% targeted network access control (NAC) replacement. This is a surprisingly small percentage, given NAC systems reputation as difficult to fully deploy; but on the other hand, that same difficulty may mean that not as many of these organizations had an active NAC system to replace.

3.2 Why Deploy Appgate SDP?

ZTNA is a hot topic, thanks to the remote work, cloud migrations, the rapidly expanding universe of cyberthreats, and the ongoing Zero Trust security directives from the U.S. government. There are plenty of other ZTNA solutions to choose from. These organizations selected Appgate SDP chiefly because they saw that it is a comprehensive ZTNA solution, addressing all forms of resource access across a network, not just remote user access or cloud access. At the same time, they saw how it could make flexible access management easier and more consistent across environments:

- "Most products focused on web only, Appgate was network-centric, which we were very interested in," said the Principal Architect at a large IT services company

- "Executive Order 14028 on improving the nation's cybersecurity…outlined in this is the adoption of Zero Trust Architectures. [Appgate serves as] a micro segmentation device—not a lot of true competitors in this space," said the Product Manager, Cloud Native Access Point at a large federal organization. "We were trending this way prior to the EO. I like the combination of micro segmentation and device compliance."

- "Our security providers started talking up ZT, and Appgate looked like a great way to get in that direction. Easy to do things location-specific, unlike with VPNs," said the Director of IT at a professional services company

- "One of the leading ways of providing least privileged access through software mechanisms," said the Associate Director of Security Operations at a large retailer

- "We are a collection of companies, a lot of networks, and we are looking for a single solution to manage access and create a Zero Trust environment," said the Vice President of Major Programs and Networking at a large IT services company

4. Key Benefits: Reduced Security Counts and Attack Surface

Zero Trust principles dictate that no communications with protected resources be allowed without an explicit policy in place allowing them. One of the key corollaries of this requirement in a full Zero Trust environment is that by default, protected resources are invisible to anything else on the network. A protected resource becomes accessible on the network only to those users and systems explicitly granted permission to access it at the moment access is attempted, and only via the prescribed means of access, and only after being authenticated on each attempt to connect. For any user or system not granted that permission when access is attempted, the resource remains invisible.

> ***"Many of our legacy internal systems are unpatched and contain vulnerabilities that are difficult/impossible to remediate. Limiting exposure to these machines to ONLY those with legitimate needs significantly reduced our attack surface."***
>
> ***Associate Director for Security Operation***
> ***Large Retailer***

This is a radical change from a typical data center or IaaS environment, in which a system is by default visible to its neighbors and to any external system able to see through a perimeter firewall. That visibility to neighbors in the environment is what makes lateral attacks such a dire threat: once a foothold is gained inside the environment, all the other systems there can be probed and attacked freely. Appgate SDP blocks unauthorized lateral access to protected resources. "Many of our legacy internal systems are unpatched and contain vulnerabilities that are difficult/impossible to remediate. Limiting exposure to these machines to ONLY those with legitimate needs significantly reduced our attack surface," said the Associate Director for Security Operations at a large retailer.

83% of participants saw significant reductions in the number of security incidents their cybersecurity teams had to respond to.

Combining that kind of reduction in the attack surface with the host of VPN- and access-related security problems obviated by rolling out Appgate SDP, no surprise that 83% of participants saw significant reductions in the number of security incidents their cybersecurity teams had to respond to. "It certainly drastically reduces the security threat landscape/profile," says the Director of Enterprise Infrastructure at a large manufacturer.

Furthermore, thanks to its extensive logging and the deeper visibility into access attempts provided by Appgate SDP, "[w]e definitely have more granular insight [into incidents] now," said the Principal Architect at a large IT services company.

5. Key Benefits: Getting User Provisioning Right

We saw that Appgate SDP consistently delivered major improvements across all use cases centered on provisioning the right access privileges to protected resources. This included both setting up initial access rights at account creation, and the ongoing task of updating privileges as users change positions or roles, or their needs change, or systems change.

With Appgate SDP, organizations saw nearly two-thirds reduction in the time needed to provision user access initially, and nearly 90% reduction in the time needed to modify access privileges. (Please see Figure 4 and Figure 5.)

That is, they saw days or weeks of time shrink to hours or even minutes.

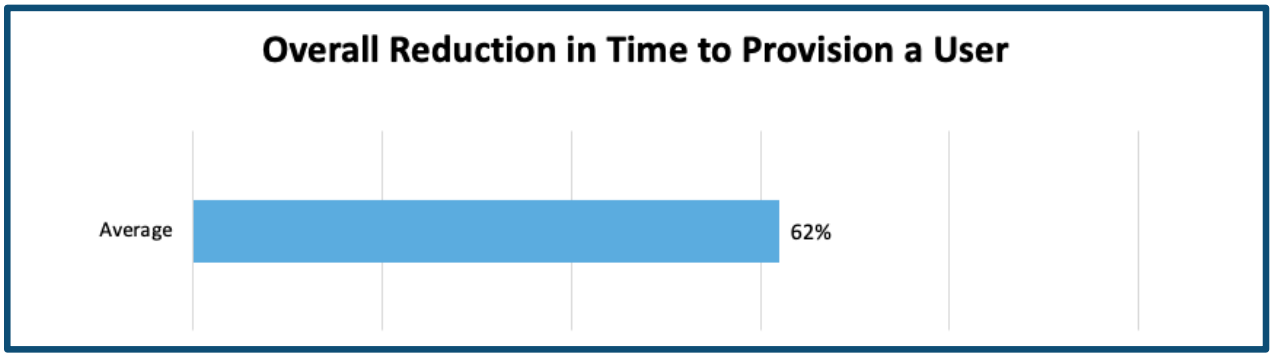


Figure 4: Average Reduction in Time to Provision Access for New Accounts

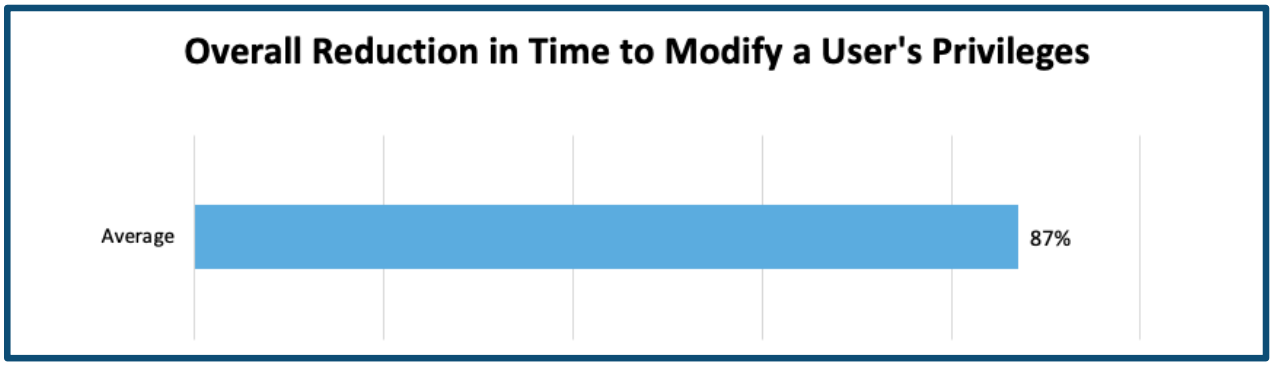


Figure 5: Average Reduction in Time to Modify Access

The improvements were more dramatic in some use cases than in others. (Please see Figure 6 and Figure 7.) On the provisioning side, time savings ranged from just under a third to more than 70%. It was management of third-party access that saw the greatest improvements (71% reduction in time, on average), followed closely by setting up correct access for cloud users.

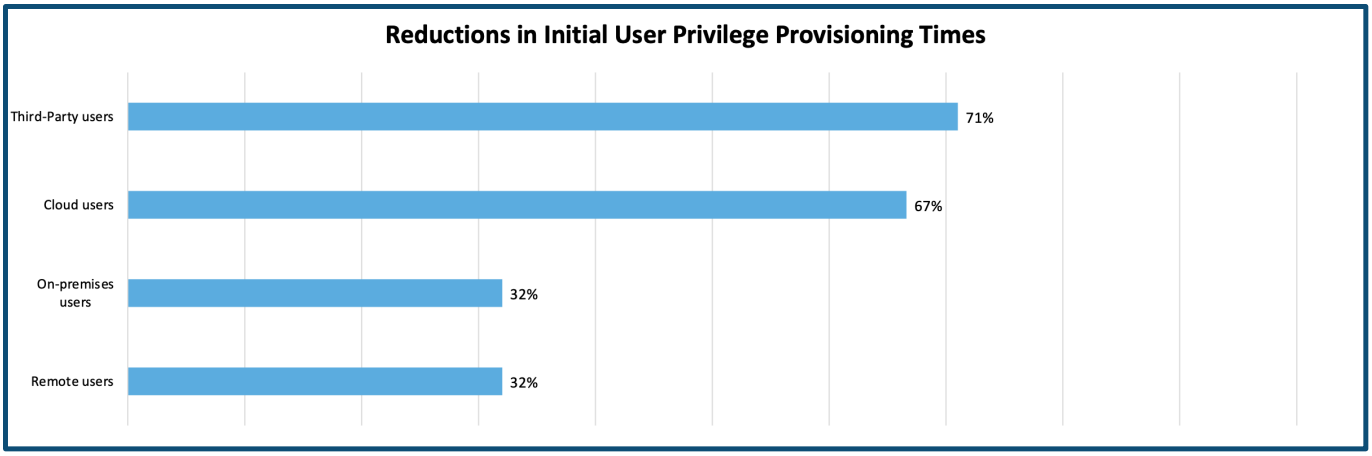


Figure 6: Average Improvements in Initial User Privilege Provisioning Time by Use Case

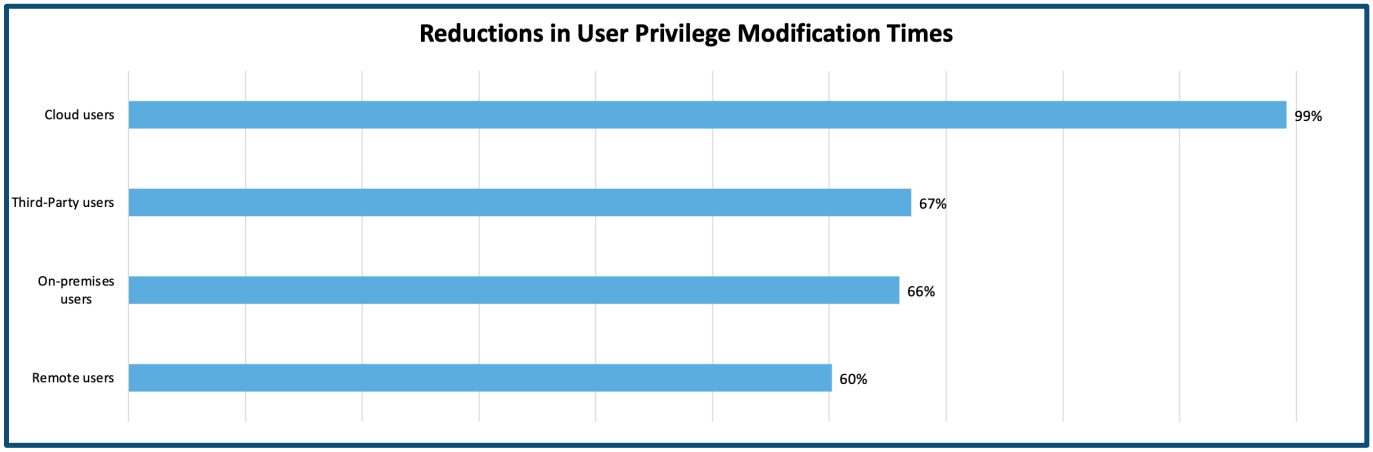


Figure 7: Average Improvements in Privilege Modification Time by Use Case

On the access modification side, every use case saw reductions of 60% or more in average time to modify access rights. The cloud use case had the most dramatic improvements, a jaw-dropping 99% average reduction in the time required, which participants attributed to having a consistent platform with which to address all the access issues, an easier way to set up access policies, and having the ability to automate more of the operations involved.

5.1 Cloud and Remote Users

Appgate SDP administrators saw, on average, a 32% reduction in the time needed to provision remote users, and a 67% reduction in the time needed to provision cloud users. They saw an average reduction in the time needed to modify an existing remote user's privileges of 60%, and a whopping 99% reduction for modifying cloud use privileges.

> ***"Appgate has made the decision to move apps to the cloud easier. Before Appgate, we really couldn't provision users for cloud application access. Now, modifications can in some cases happen automatically."***
>
> ***Principal Architect***
> ***Large IT Services Company***

These kinds of changes had profound impacts. "Appgate has made the decision to move apps to the cloud easier. Before Appgate, we really couldn't provision users for cloud application access. Now, modifications can in some cases happen automatically," noted the Principal Architect at a large IT services company. This sentiment was echoed by the Cloud Solution Architect at a large professional services company: "We couldn't allow access [for field workers to our cloud-hosted applications] before Appgate. Now that we have it, we have a capability that didn't previously exist…we maximize APIs to fully automate the vast majority of our authorization activities."

It is important to remember that the granularity of control possible with Appgate SDP is significantly better than most participants had been used to: "Appgate allows a more granular approach to doing access management," said the Associate Director of Security Operations at a large retailer. "Before Appgate, access was all-or-nothing. Now, with Appgate, we can much more tightly control access details, and the time to do that is a third of the time it took to grant full access."

Appgate SDP users also saw on average a 32% reduction in the amount of hands-on staff time required to do the provisioning and execute the rights changes.

Just as important as the granularity of control is the ease of making changes, including the degree of automation possible (as indicated in the comments above). Notably, and separately from the amount of calendar time user provisioning and right modifications take, Appgate SDP administrators also saw on average a 32% reduction in the amount of hands-on staff time required to do the provisioning and execute the rights changes.

These two things together translate to a lot of time freed up for overburdened and expensive cybersecurity staff. "[Executing an entitlements change] once approved is seconds to 5 minutes. Before Appgate…hands-on infosec time required to implement [was] a week on average," noted the Senior Information Security Engineer at a large financial services company. "The team was oversubscribed."

5.2 On-premises Users

Appgate SDP drove similar improvements in access management for on-premises users: a 32% average reduction in the amount of time needed to provision users' initial access privileges, and a 66% reduction in the time needed to manage modifications afterwards.

Notably, Appgate SDP also made it possible for IT teams to reduce the number of tools involved in provisioning and managing user access. Among the half of organizations that were not already down to a single tool to manage access, introducing Appgate SDP resulted in a 56% reduction in the number of tools in use. (Please see Figure 8.)

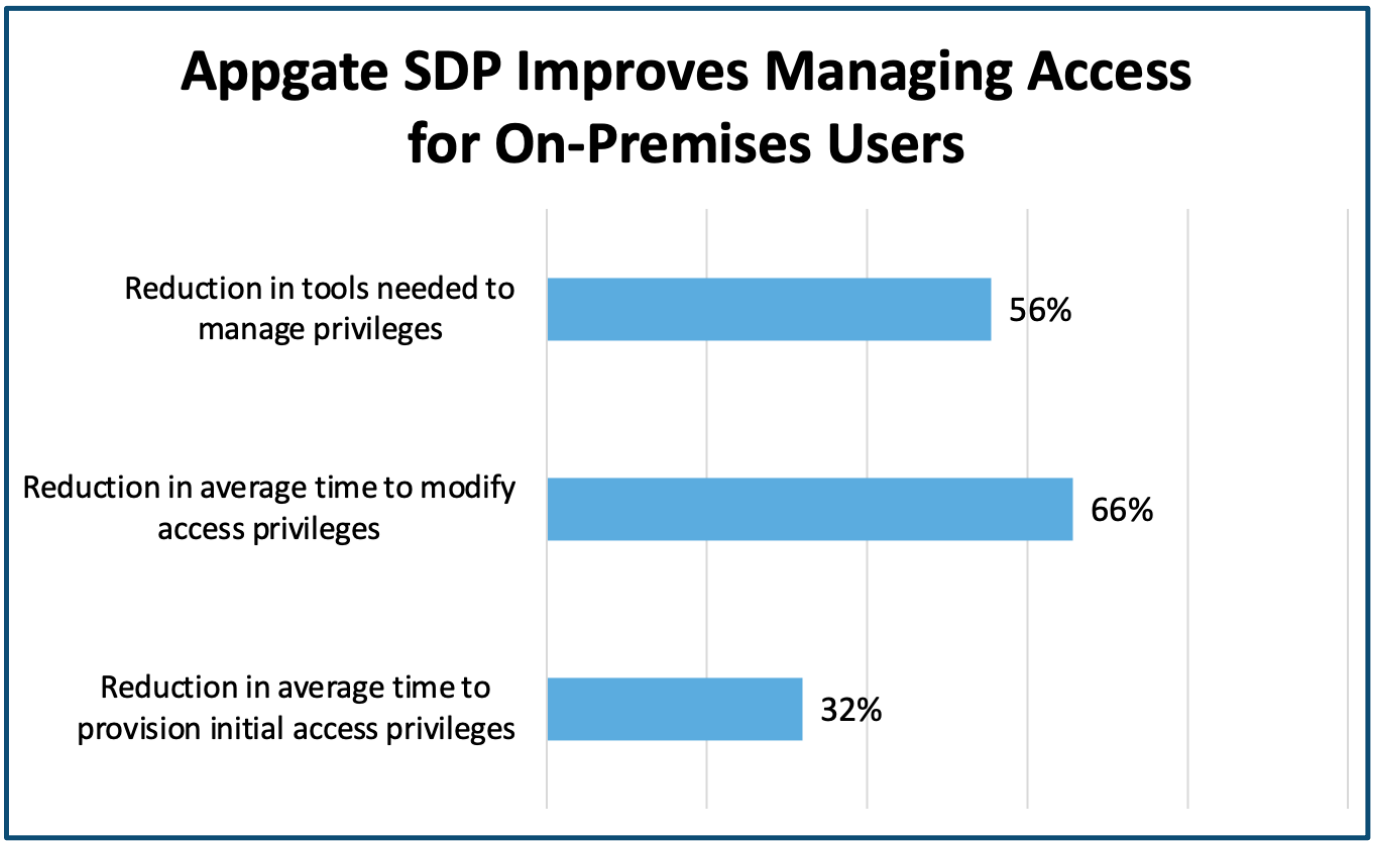


Figure 8: Improvements in On-Premises User Management

Using Appgate SDP to manage on-premises access fulfills most of the key requirements organizations have for NAC: controlling access to the network itself, and coupling access decisions with platform health checks for systems seeking access. "Before Appgate, there was NO provisioning, people just plugged into the network," said the Director of Enterprise Infrastructure at a large manufacturer. "With Appgate, we now establish secure policies for all users."

5.3 Third-Party Users

Third-party access has long been a thorn in the side of IT departments. People working for business and technology partners or contractors often need access to an organization's systems, but that access should not be identical to the access granted to employees. That is, third-party users are ideally granted access only to the systems they need to have access to, and that will be a small subset of the systems employees need access to.

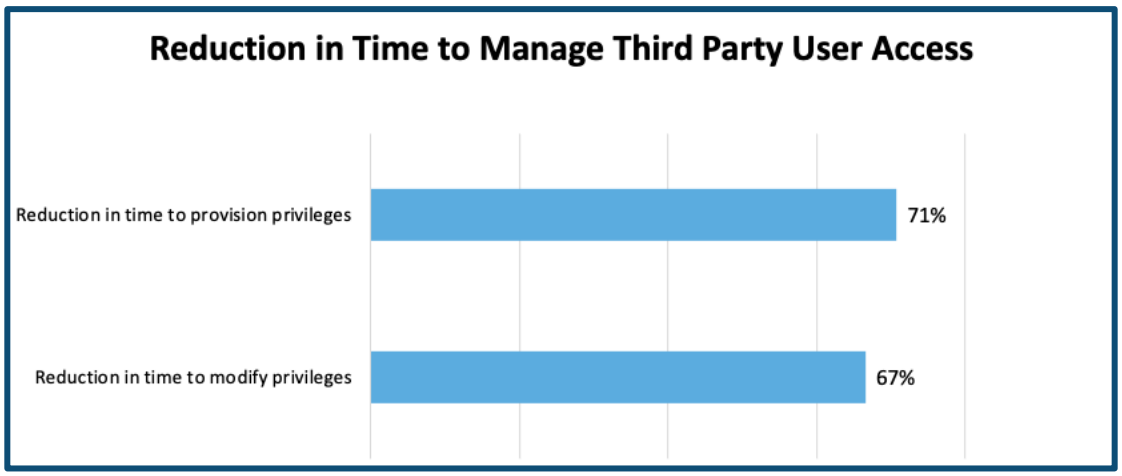


Figure 9: Improvement in Third-Party User Management

Unfortunately, most organizations have not had access management systems in place to make this easy, or even possible. Many have been forced to forbid third-party access to internal systems: "We couldn't allow third-party access before, as we had no tools to do this," said the Principal Architect at a large IT services company. This sentiment was echoed by the Cloud Solution Architect at a large professional services company: "Before Appgate, there was no third-party access. Appgate is allowing this to happen."

Those that could not simply forbid access have mostly instead had to provision accounts for third-party users that are just like anyone else's, with network-level access to all the internal systems anyone else can see. These organizations generally try to track these users as a distinct group so as to keep on top of changes in the access rights they should have, including when they should lose them, e.g., at the expiration of a contract. This is an effort that usually fails, and so stale accounts accumulate, a cybersecurity debt that represents significant risk.

Participants said Appgate SDP has been transformative with respect to third-party access, making it easy to allocate—and set expiration dates on—granular access to just the systems that contractors, vendors, or other third parties required. "Third parties had full access before Appgate. Appgate now allows us to permit access only to apps the third party requires," said the Director of Enterprise Infrastructure at a large manufacturer.

6. Key Benefit: Advancing Zero Trust

As a ZTNA solution, deploying Appgate SDP is itself a step towards implementing a full Zero Trust architecture. Appgate SDP administrators tend to think of their infrastructure as having a Zero Trust environment and a legacy environment, with workloads being migrated from legacy to Zero Trust, or decommissioned in legacy and replaced by new solutions spun up in the Zero Trust environment *ab initio*. On average they use Appgate to control access to 85% of the systems in their Zero Trust environments.

> ***"We are using Appgate for resource access and microsegmentation."***
> ***Principal Architect***
> ***Large IT Services Company***

Importantly, Appgate SDP is not focused solely on user access; it can also manage resource-to-resource access. "We are using Appgate for resource access and microsegmentation," said the Principal Architect at a large IT services company. The Principal Enterprise Architect at a midsize software and IT services company similarly noted, "[We] need to deepen adoption of Appgate for inter-systems [communications] at all levels." On the adoption arc most companies follow, gating user access is the lower-hanging fruit and is pursued first. Managing inter-system access is more complicated to plan and implement, and many organizations did not even have tools available to map out the relationships in amongst their systems—to see which systems communicated with which other systems, and how—until they had deployed Appgate SDP.

Appgate SDP users on average control access to 85% of the systems in their Zero Trust environments with Appgate SDP.

7. Conclusion

Organizations usually deploy Appgate SDP to solve multiple problems in their environments. They tend to start with replacing their VPNs for remote users, but quickly apply the solution to solving all manner of user access issues, and to make it a cornerstone for broader deployment of Zero Trust and an enabler of speedier migration to cloud.

Across all areas, Appgate SDP drives major, and in some cases transformative, reductions in the amounts both of clock time and of hands-on staff time required to manage access. Simultaneously it delivers significant improvements in the granularity of control an organization can exert, enabling both broader and safer extension of access to third parties, be they partners, contractors, or auditors.

And, thanks to its enforcement of Zero Trust principles at the network level, Appgate SDP renders protected resources invisible to anyone and any system not meant to reach them, dramatically reducing the organizational threat surface and reducing the number of cybersecurity incidents these organizations have to deal with.

8. Case Studies

8.1 Summary of Case Studies

Financial services firm improved user access management while tightening controls. Appgate SDP's more granular entitlements capabilities and better automation also help them advance their Zero Trust agenda.

International IT services company implemented deep Zero Trust functionality. Offering the entire spectrum of managed hosting solutions to its customers, they needed a solution that could provide full control of communications within their networks as well as at the access points.

Major international IT outsourcer needed to secure its collection of networks. They needed a single solution to manage access across the whole enterprise and help them create a Zero Trust environment. They chose Appgate SDP.

Federal agency redoubles push for ZTNA after Executive Order on Zero Trust. Years of work had produced little progress—and now more resources were shifting to cloud. Appgate SDP has become a key component of the organization's cloud-native access point architecture.

Global outsourcing company controls secure access to AWS resources. They needed the solution to be better—more secure—than their existing methods, and for it to be applicable to both on-premises and remote users, whether employees or third-party. Appgate SDP addressed their problems.

Software and IT services company deploys agile Zero Trust access to support expansion. This firm pursued Zero Trust to facilitate international expansion, where its legacy VPN and "hard perimeter" approach impeded it. Appgate SDP solved their problems and has led to transformational change in the operating model.

Global manufacturer with a burning need to replace its legacy VPN solution wanted more. More than just a new VPN, it wanted to enhance its security posture. Appgate SDP made them more secure as it replaced legacy VPN technology.

Insurer urges construction management firm to embrace Zero Trust. The obvious first step was access management tools, and they needed a tool that would make it easy to do location-specific things—unlike their legacy VPNs—and also make less work for IT. Appgate SDP was the solution.

Major Internet retailer enables Zero Trust least privilege access. Furthermore, they want one tool across remote and on-premises user bases, and cloud and on-premises resources. Appgate answered the call.

8.2 Financial services firm improved user access management while tightening controls

This financial services firm needed a solution to improve user access management through better control of access entitlements and better automation, and also help them advance their Zero Trust agenda. After evaluating other solutions they chose Appgate SDP.

Staff	19,000
Revenue	$8.3B
Culture	Aggressive

By melding automated execution of entitlement creation via Appgate SDP to a workflow for access entitlement requests and approvals, they accelerated a process that took a week to the point where it takes only a couple of hours, and most of that in the approvals phase rather than the execution. Modifications to entitlements were similarly accelerated, from two days on average to two minutes. Moreover, they now do so with only 40% of the staff hours previously required, and with a third fewer tools in the mix.

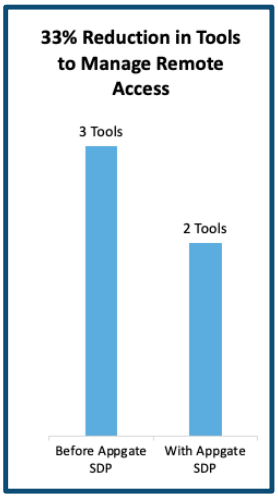
> ***"Actual implementation [of entitlements] once approved is seconds to 5 minutes. Before Appgate, the elapsed time was about the same through the approvals part, but the hands-on infosec time required to implement was a week on average, because the team was over-subscribed."***
>
> ***Senior Information Security Engineer***

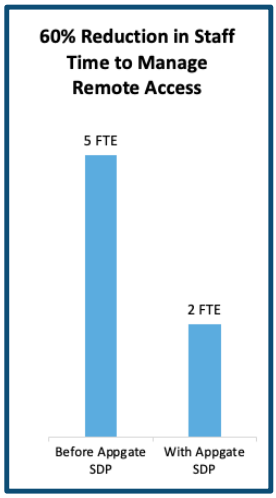
In addition to current management of remote access, the organization is working on deploying Appgate SDP for on-premises users.

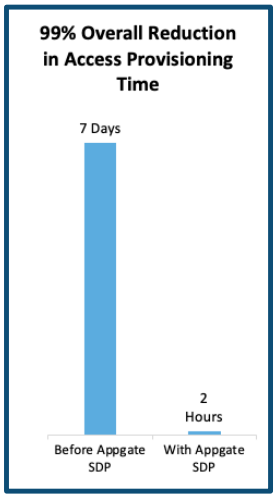
Although the organization had moved only about 9% of its workloads to cloud, they have begun phasing in Appgate SDP management of access to cloud services. Most existing cloud workloads are behind Appgate SDP, and all future deployments will be.

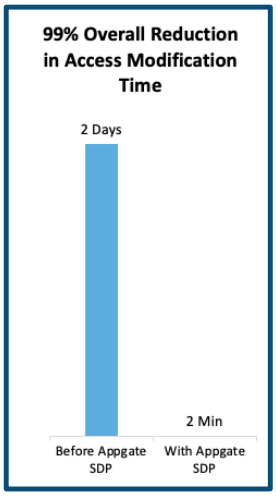
83% of IaaS environments protected by Appgate SDP.

The broad deployment of Appgate SDP for remote access has allowed the organization to phase out VPNs entirely, which they view as a first significant step down the road to true Zero Trust. It has also helped them increase their use of dynamic, context sensitive security policies: pre-Appgate, 40% of their policies were in some way dynamic and context-aware, post-Appgate it is 60%.









8.3 International IT services company implements deep Zero Trust functionality

This company provides the entire spectrum of managed hosting solutions to its customers, from empty racks in a data center to managed public cloud infrastructure. As they evolved from their original roots in basic hosting, they needed a solution that could provide full control of communications within their networks as well as at the access points.

Staff	8,000
Revenue	$1B
Culture	Moderate

They looked to Appgate SDP to control access for both remote and on-premises users, and for both their own and third-party users—in this case, third parties being their customers. They also brought Appgate SDP in to remove barriers and obstacles to them moving their own applications into cloud environments.

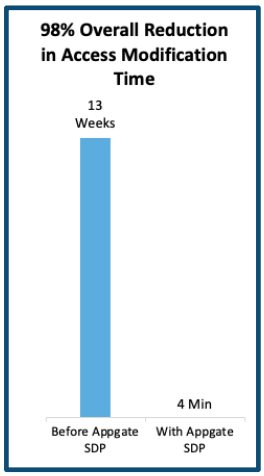
> ***"Most products focused on web only, Appgate was network-centric, which we were very interested in; Couldn't allow 3rd party access before, as we had no tools to do this; [Our] level of security and granularity of access have improved."***
>
> *Principal Architect*

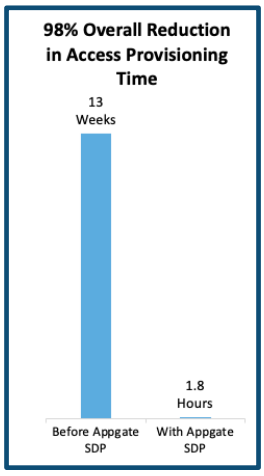
Appgate SDP is providing radical improvements in user provisioning times and user access modification times—98% reduction on each, overall. Cloud user provisioning that used to take three days now takes 10 minutes; cloud account modifications that took an hour now take 30 seconds.

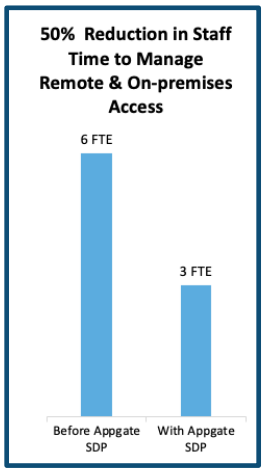
They are also fully engaged in adopting Zero Trust throughout their infrastructures, with Appgate SDP as one of their primary tools, to facilitate microsegmentation. They have moved 30% of their systems into a Zero Trust environment, with 100% of them protected by Appgate SDP. In future, they intend to decommission their standalone NAC solution, it having become functionally redundant given the presence of Appgate SDP. About 60% of their endpoints are licensed under the current NAC solution, and they intend to bring that down to zero.

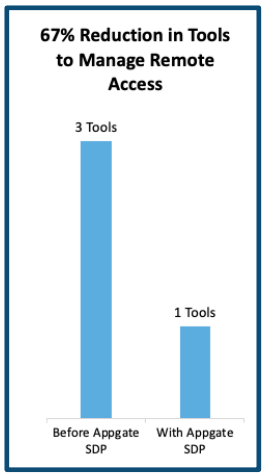
Cloud user provisioning that used to take three days now takes 10 minutes; cloud account modifications that took an hour now take 30 seconds.

Beyond speeding up and tightening down network and system access at all levels, Appgate SDP provides them far more granular visibility than they had before into network access events, including security incidents. Since deploying, they have seen a dramatic reduction in incidents related to unauthorized access to systems.









8.4 International IT outsourcer needed to secure its collection of networks

This very large, international IT outsourcer and application automation company shares a problem with a lot of other companies that grow by acquisition and merger: it is a collection of companies, running a collection of networks. They needed a single solution to manage access across the whole enterprise and help them create a Zero Trust environment. They chose Appgate SDP.

Staff	130,000
Revenue	$16B
Culture	Aggressive

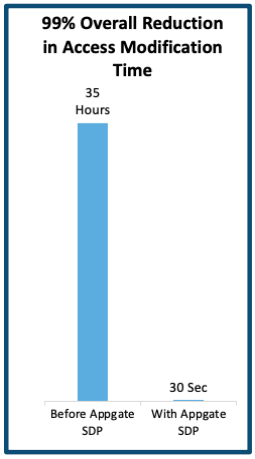
Appgate SDP replaced a mishmash of VPN solutions managed separately from each other and with limited coordination. One result of moving to a consistent and automatable secure access platform has been an enormous speed-up in user provisioning and privilege modifications. Cloud and remote user accounts that took four days to provision on average, pre-Appgate, now take an average of only 30 seconds. Modifying rights on an account previously took four hours, reduced with Appgate SDP to 30 seconds. Third-party users, who number in the tens of thousands sometimes, can now be provisioned and managed just as expeditiously as staff.

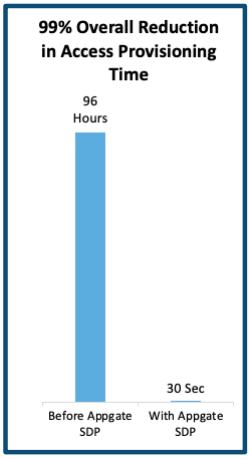
> ***"VPN solutions are a way people get penetrated with known security incidents. We are fully migrated off these VPNs. We have not had a security incident with Appgate at all."***
>
> *Vice President of Major Programs and Networking*

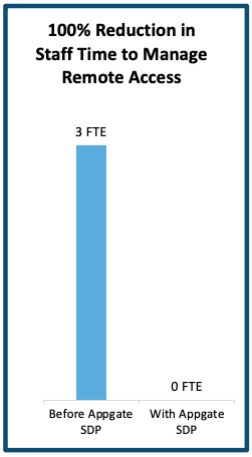
Moreover, where three FTEs worth of staff time went to managing remote access pre-Appgate, that has shrunk to zero with Appgate SDP and workflow automation. The same is true of third-party users: pre-Appgate, it took the equivalent of three full time staff to manage them; post-Appgate, it takes no committed staff time at all.

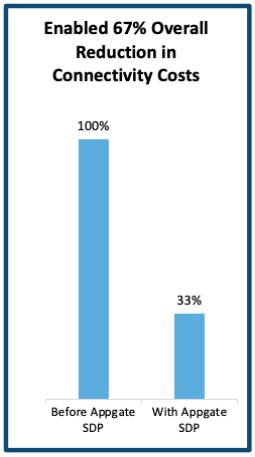
Appgate SDP made it possible to reduce overall connectivity costs by 67%.

Appgate SDP has turned into an important security visibility asset, having helped them spot three ransomware attacks in progress in the past year. In addition to allowing the company to reimagine and unify access control, Appgate SDP is empowering them both to securely transition of off MPLS connections and to pull back from their planned deployment of SD-WAN. Since deploying Appgate SDP they have pulled MPLS from all 600 sites they had it at. And even though they significantly increased the bandwidth to each site, via dedicated Internet access, their overall connectivity costs dropped by 67%. "Our offices now look like Starbucks," noted the principal architect in reference to their open, café-style WiFi networks.









8.5 Federal agency redoubles push for ZTNA after Executive Order on Zero Trust

A branch of the government has been working to implement a Zero Trust architecture for years, and also to shift to making more extensive use of cloud resources. The recent run of Executive Orders around cybersecurity, including EO 14028, created a renewed sense of urgency around making those forays into cloud without compromising the pursuit of Zero Trust. Appgate SDP has become a key component of the organization's cloud-native access point architecture.

Staff	250,000
Revenue	$234B
Culture	Aggressive

By bringing Appgate into the mix, the organization has been able to build an environment in which accounts with only and exactly the access privileges they need are, on average, provisioned within 30 minutes of receiving a request. Modifications to the privilege set for an account will be made within 5 minutes, on average.

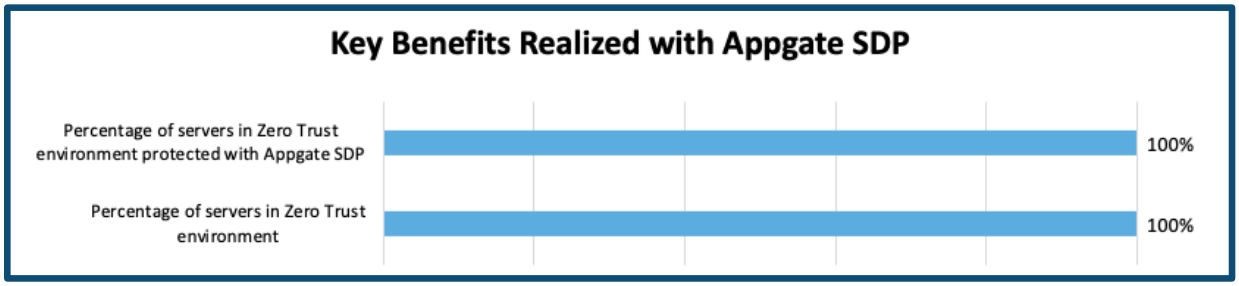
> ***"Micro segmentation [system]—not a lot of true competitors in this space. …I like the combination of micro segmentation and device compliance."***
> ***Product Manager, Cloud Native Access Point***

As the organization continues to expand its use of Appgate SDP, it will be re-evaluating its non-classified environments with respect to their use of MPLS communications and, overall, its recent adoption of SD-WAN. IT teams will be assessing whether either standard use of MPLS or SD-WAN remain necessary given truly secure communications over the Internet.

And, of course, ZTNA for users is only one of the "193 separate activities" being undertaken to shift them to Zero Trust. Implementing microsegmentation and ZTNA for back-end servers and services are others. At this point, 100% of the organization's servers are in its Zero Trust environment—and 100% of them are protected with Appgate SDP.

Percentage of servers in Zero Trust environment: 100%

Percentage of servers in Zero Trust environment protected with Appgate SDP: 100%



8.6 Global outsourcing company controls secure access to AWS resources

To facilitate and accelerate their move to the cloud, this global temp and outsourcing company needed a quick solution to the problem of controlling access to resources in AWS. They needed the solution to be better—more secure—than their existing methods, and for it to be applicable to on-premises and remote users, whether employees or third-party. Appgate SDP solved all these problems for them.

Staff	20,000
Revenue	$7B
Culture	Aggressive

Specifically, they were seeking a solution that would support FIDO-2 MFA incorporating a hardware token, and that would also be able to safely support third-party access to their systems, something their incumbent solutions could not do.

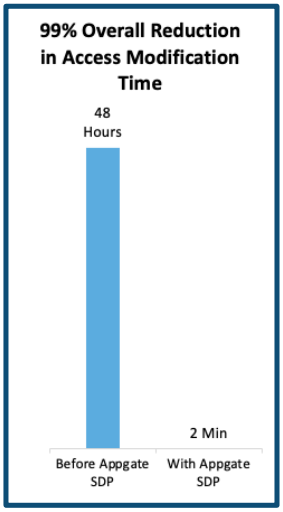
> ***"Once users are in, we maximize APIs to fully automate the vast majority of our authorization activities."***
> *Cloud Solution Architect*

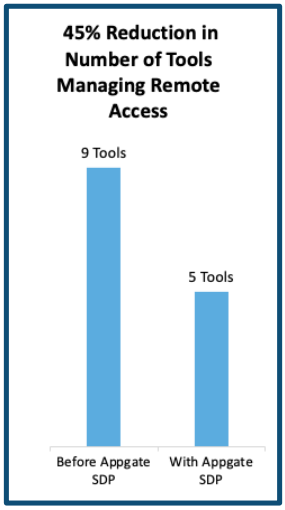
All of this was in support of a cloud migration effort that had already been in motion for 10 years, and had resulted in the movement of 50 applications—about 65% of the total planned migration—and their placement in four separate environments. The difficulty of managing access across these disparate systems and environments was one factor slowing the migration, and there are still many access methods in use. The plan is to continue to consolidate and rationalize control with Appgate SDP.

The company regards the cloud resources as their Zero Trust environment; 100% of the resources there are protected via Appgate SDP. Thanks in part to the improvements in access management Appgate SDP brought with it, they will shut down their EMEA data center, migrating all the workloads remaining in it into cloud environments, and getting them to approximately 85% to 90% migrated.

Another thorny problem Appgate SDP solved was third-party access to corporate resources. Before Appgate SDP, this was simply not allowed; with Appgate SDP, it is now a standard procedure. Accounts can be provisioned in 30 minutes, and modified as needed in just two minutes.

Third-party access to resources can now be allowed, can be provisioned in 30 minutes, and modified in just two minutes.





8.7 Software and IT services company went for agile Zero Trust to support expansion

A midsized software and services firm pursued Zero Trust to facilitate international expansion, where its legacy VPN and "hard perimeter" approach impeded it. Appgate SDP solved their problems and has led to transformational change in the operating model.

Staff	2,350
Revenue	$535M
Culture	Aggressive

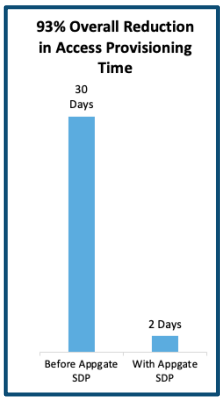
Zero Trust had been a goal for many years prior to Appgate SDP adoption, seen as the only way to ensure secure, properly limited access both for internal users wherever they were, including overseas, and for external users including suppliers and partners. The ideal future environment needed simultaneously to provide granular access controls independent of location, to support international compliance regimes without massive manual effort, and to not get in the way of the company's security services staff as they engaged in "Red Team" activities in the course of assessing customer security.

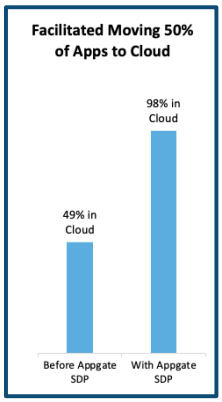
> ***"[Deploying Appgate resulted in] 6% reduction in gross IT spend, 5.7% in security spend."***
> *Principal Enterprise Architect*

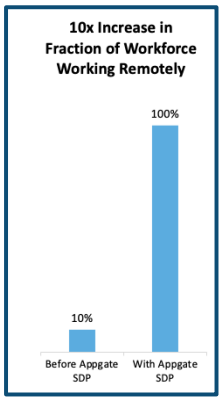
After many disappointments with inadequate solutions, the firm implemented Appgate SDP. Provisioning new users with all the specific access rights they needed went from taking 30 days to 12 hours, and modifying privileges from days to minutes. Moreover, the user experience was vastly improved compared to the VPN: establishing connections was faster, easier, and more reliable. This led initially to a rapid transition away from their legacy VPN solutions—end users actually demanded transition to the new system and encouraged colleagues to do the same. Appgate now controls nearly all access, and for all employees, from the CEO down.

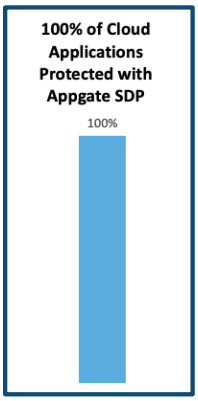
Provisioning new users with all the specific access rights they needed went from taking 30 days to 12 hours, and modifying privileges from days to minutes.

After they decommissioned their many VPN appliances, generating substantial savings, they realized that the ZTNA model had not only transformed how they control access to systems, it had created the possibility of eliminating their private WAN entirely. The WAN had existed primarily to provide secure access to back-end systems, after all, and the shift to ZTNA meant that secure access could as easily be provided over the public Internet, and at roughly equivalent performance for the systems in question. Even as this transformation was in progress, generating even more savings, the pandemic pushed them one step further. The shift to remote work was followed by the realization that there was little need for anyone to work in a company facility anymore. Subsequently nearly all company offices have been shut down in favor of permanent work from home, generating still more savings. So, all users are now remote users, all the time, thanks to Appgate SDP.









8.8 Global manufacturer with burning need to replace legacy VPN solution wanted more

A global manufacturer with a burning need to replace its legacy VPN solution wanted more than just a new VPN: it wanted to enhance its overall security posture. Appgate SDP helped them do both.

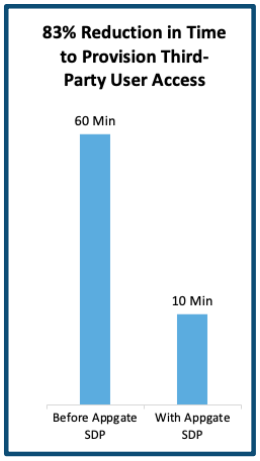
Staff	5,000
Revenue	$1.5B
Culture	Bleeding Edge

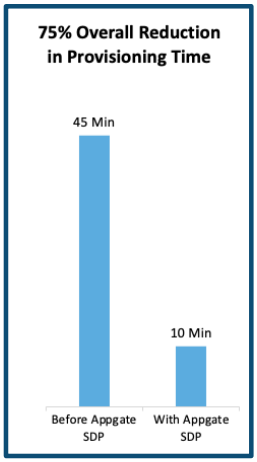
The initial goal was to manage access for remote, on-premises, and third-party users. Beyond this, they plan eventually to manage all access to cloud resources—once they begin migrating workloads to cloud. And, ultimately, they mean to make Appgate SDP a cornerstone on which they will implement a full Zero Trust network access architecture.

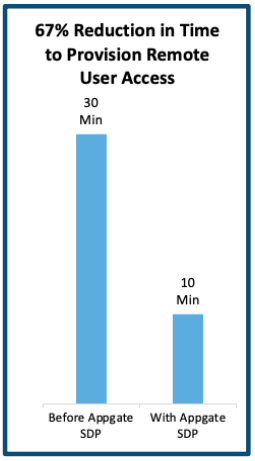
They succeeded in reducing the time it takes them to provision new users' access rights by 75% on average. And, significantly, for remote and on-premises users, they have shifted from an "all access" model under which, if people could reach any resource then they could reach every resource, to a highly granular model. The same applied to third-party users: even if they needed to reach only a single resource in order to do their work, they were able to see all the other resources as well. Now, all three classes of users have access only to the resources they actually have a business need to reach.

> ***"Appgate allows a more granular approach to doing [remote] access management. Before Appgate, access was all-or-nothing. Now, with Appgate, we can much more tightly control access details, and the time to do that is 1/3 the time it took to grant full access.***
>
> ***Before Appgate, there was no provisioning [of access for on-premises users], people just plugged into the network. With Appgate, we now establish secure policies for all users."***
>
> *Director of Enterprise Infrastructure*

As a result of the introduction of differential levels of access to resources with Appgate SDP, they have been able to "drastically reduce" the cybersecurity threat surface of their systems and take a big step towards a Zero Trust environment over all. Their ultimate Zero Trust goal is to "treat the end user the same whether they are on-prem or off-prem" not by making access wide-open, but instead by ensuring that "all people need to be authenticated and authorized for access, regardless of position, company affiliation or location."







8.9 Insurer urged construction management firm to embrace Zero Trust

A small construction management and general contracting firm with a very lean IT operation needed to take steps towards Zero Trust, thanks to a push from their cybersecurity insurance company. The obvious first step was with access management tools, but they needed a tool that would make it easy to do location-specific things—unlike their legacy VPNs—but which also make less work for IT. Appgate SDP was the solution.

Staff	225
Revenue	$700M
Culture	Moderate

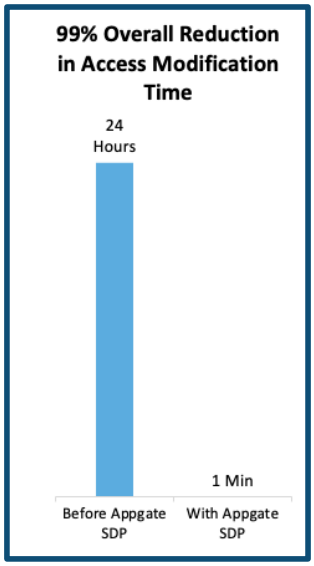
They embraced Appgate SDP first for managing remote users, but with the goal of folding in on-premises users next. Although they have seen no significant savings in account provisioning time, they have seen an enormous improvement in account modification times, with the average time from request to fulfillment down from a full day to approximately 1 minute. And, even though there has been no speed up on provisioning, there has been a significant improvement in the granularity of access controls available.

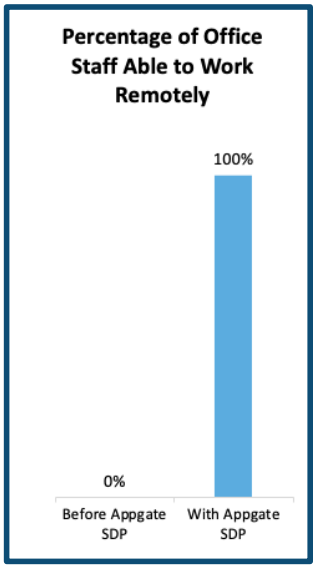
> ***"Our security providers started talking up Zero Trust, and Appgate looked like a great way to get in that direction. Easy to do things location-specific, unlike with VPNs."***
>
> ***Director of IT***

IT had been provisioning site to site VPNs for private communications from remote work sites to on-premises applications. They had also been backhauling cloud-bound traffic through these VPNs. As they proceed with the Appgate roll-out, they saw some application performance improvements in addition to access management improvements. The Appgate SDP agent's intelligent routing of communications points each user's sessions at the ingress points with the best performance for them, eliminating the added latency associated with backhauling everything to a fixed data center before sending it out to its destination.

Saw a significant reduction in security incidents after deployment.

In the wake of the pandemic, Appgate SDP also powered an overall shift in work patterns. As with so many other companies, the pandemic had driven the firm to nearly 100% remote work for a time. However, the nature of the business is that 70% of the team is in the field at any given time anyway. As the pandemic receded and the company contemplated a return-to-the-office for everyone else, they instead decided that since Appgate made it safe and effective to work from home, they should be flexible and allow anyone to work remotely on an ongoing basis.





8.10 Major Internet retailer enables Zero Trust least privilege access

This major Internet retailer was in search of an access management solution that let it implement least privilege access for both on-premises and cloud resources, across remote and on-premises user bases. Appgate SDP answered the call.

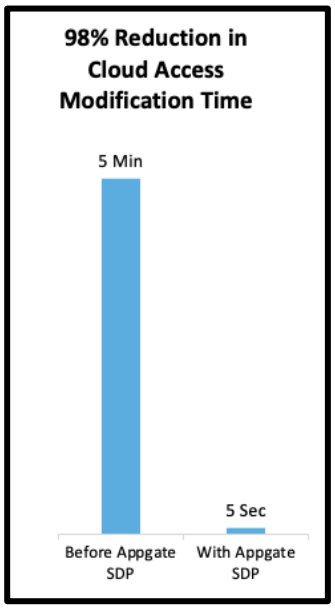
Staff	17,000
Revenue	$8.9B
Culture	Aggressive

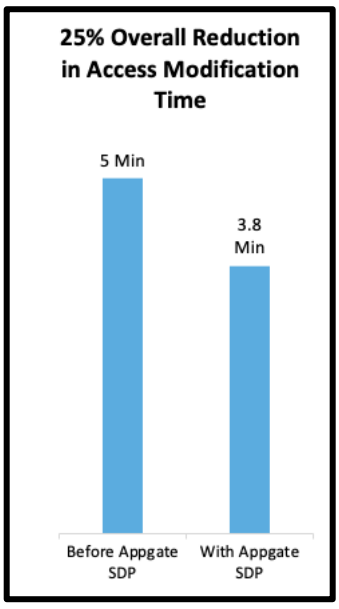
This cloud-native company already had highly automated processes for creating user accounts and assigning them access. Appgate SDP added the ability to be finer grained in the access granted. And, despite their existing sophistication, Appgate SDP was able to drive a further 25% reduction in the time needed to modify privileges after provisioning on average. For cloud user access modifications specifically, the reduction was 98%. And the comparison is all the more compelling because pre-Appgate, cloud users had access to pretty much anything in the same environment; now access is specific to only the systems a user needs to do their job. The same applies across remote access and on-premises access: the quality of control is enormously improved. This is an especially important point for third-party access: fine-grain control has dramatically reduced the level of access non-staff (nearly 2% of the user base) have to non-public applications.

> ***"Many of our legacy internal systems are unpatched and contain vulnerabilities that are difficult or impossible to remediate. Limiting exposure to these machines to only those with legitimate needs significantly reduced our attack surface."***
>
> ***Associate Director, Security Operations***

Applications are developed in the cloud, and access management is now automated as a part of the overall build process. Appgate SDP is an important part of this automated implementation of access management, being integrated into development teams' CI/CD pipelines.

Despite the fact that the company is cloud-native, even it has legacy systems with unpatchable security holes. By providing a mechanism to tightly control who has access to these systems, and how they can reach them, Appgate SDP has helped them reduce their threat surface while also postponing the expense of migration.





9. Methodology

In September 2022, Nemertes developed a customized set of hypotheses and questions focused on uncovering the business value and operational impact of Appgate SDP. We reviewed these hypotheses with Appgate, which provided Nemertes with the names of current, experienced customers to interview. Nemertes scheduled calls with and interviewed participants in October 2022 – January 2023. Nemertes senior analysts interviewed all participants, independently, to gather detailed data on each organization's experience with Appgate SDP. Nemertes then analyzed the data, for each and collectively across organizations. We have kept the names of the organizations confidential to protect their competitive information.

About Nemertes: Nemertes is a research-based advisory and IT consulting firm that analyzes the business value of emerging technologies. Since 2002, we have provided strategic, client-centric recommendations based on data-driven operational and business metrics to help organizations deliver successful technology transformation to employees and customers. Simply put: Nemertes' better data helps clients make better decisions.