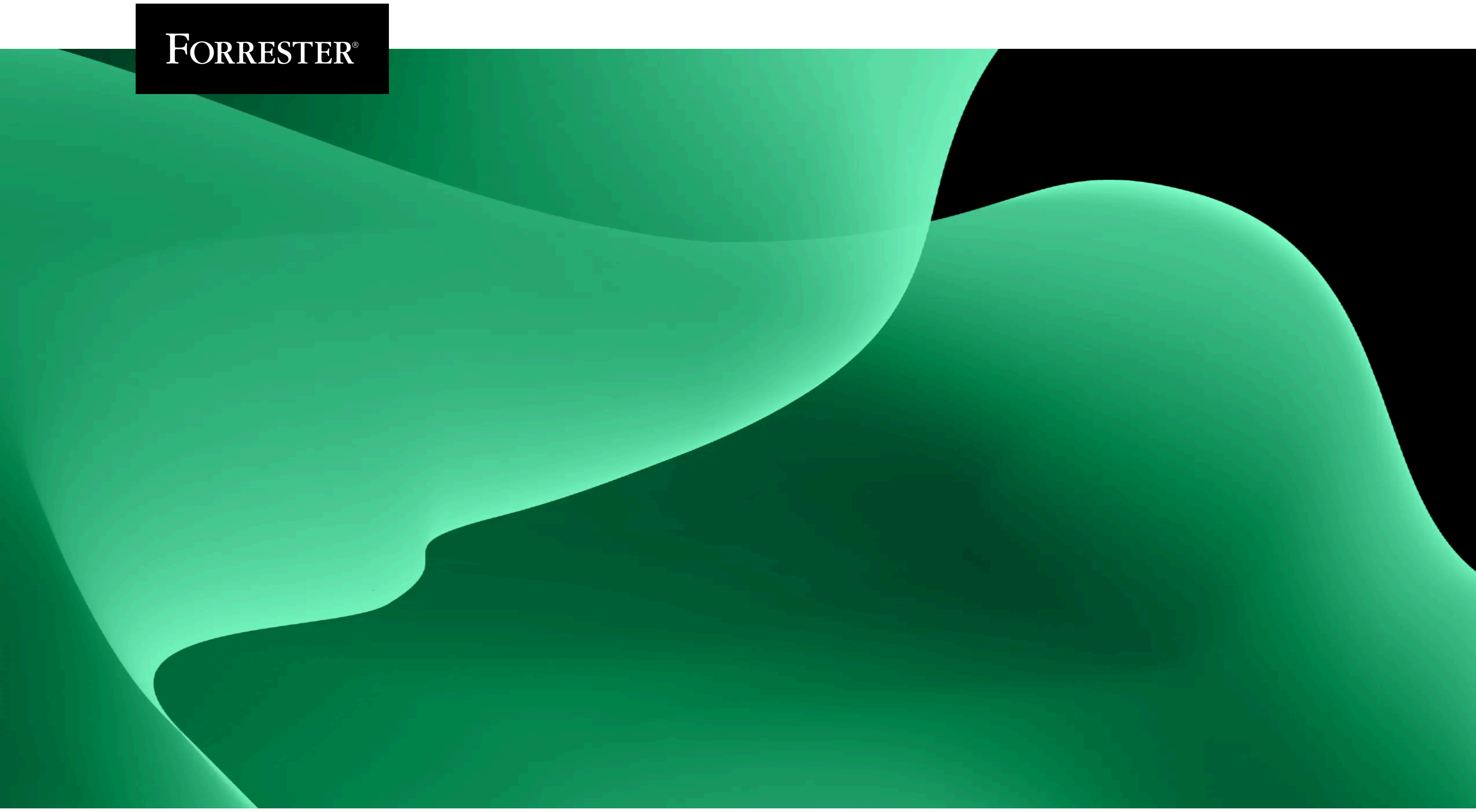
Total Economic Impact

The Total Economic Impact™ Of AppGate ZTNA

Cost Savings And Business Benefits Enabled By ZTNA

A FORRESTER TOTAL ECONOMIC IMPACT STUDY COMMISSIONED BY APPGATE, NOVEMBER 2025



Executive Summary

Organizations shift to decentralized, cloud-first environments to grow, innovate, and reduce costs. As they lean into modern cloud and AI technologies, they increasingly face sophisticated cyberthreats from these same opportunities. Firms must ensure secure, compliant Zero Trust network access (ZTNA) across hybrid infrastructures without relying on legacy perimeter-based models. Modern infrastructure built on secure and resilient network access helps organizations reduce risk, simplify identity and entitlement management, and adapt to dynamic threat landscapes.[1]

AppGate ZTNA delivers a secure, purpose-built ZTNA solution that enables organizations to protect critical resources and achieve measurable business outcomes that are often left unserved by multifunction or cloud-routed platforms. Its low-latency, contextual access for explicit authorization creates direct, encrypted connections between users and resources. With a software-defined perimeter and the use of single-packet authorization (SPA), AppGate ZTNA confers unique cloaking and network obfuscation capabilities, avoids vendor-controlled cloud routing, and minimizes exposure to shared infrastructure risks. Its Zero Trust architecture, distributed enforcement model, and API-first design streamlines network complexity; enables scalable, resilient access across hybrid environments; reduces attack surfaces; and supports automation, integration, and dynamic policy control.

AppGate commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying ZTNA and to demonstrate the value of choosing a vendor that is exclusively focused on secure access.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of ZTNA on their organizations.

210%	$11.6M
Return on investment (ROI)	**Net present value (NPV)**

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four decision-makers with experience using AppGate ZTNA. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization that is a multibillion-dollar, globally distributed organization with advanced workloads, including agentic AI.

Interviewees said that prior to using ZTNA, their organizations struggled to maintain costly, hardware-laden network architectures. Their organizations previously faced frequent disruptions and security risks due to complex routing environments and legacy access models, while managing secure access often demanded significant manual effort from dedicated resources. Downtime resulted in measurable efficiency losses while scaling limitations hindered business growth.

After their investment in AppGate ZTNA, interviewees reported that their organizations reduced the potential impact of insider and other internal threats by putting into practice foundational principles of least-privilege, separation of duties, and segmentation. These efforts improved their security and compliance posture, even when scaling protection across large numbers of users. The solution's ease of use and responsiveness enabled the interviewees' smaller teams to maintain large technology estates more efficiently than their prior environments. This increased end-user productivity and lowered labor costs while ensuring a resilient security and compliance posture across highly distributed, hybrid, and mobile scenarios.

Key Findings

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **A 50% reduction in networking technology and management costs.** With AppGate ZTNA, the composite organization eliminates routing inefficiencies, reduces hardware dependency, and decommissions unnecessary software and SaaS solutions. This optimized network infrastructure leverages an approach that lowers capital expenses and simplifies administration for total network infrastructure and management cost savings of $4.2 million.

- **A 75% improvement in end-user productivity.** With AppGate ZTNA, the composite supports high-performance secure access at scale. It enables direct, encrypted tunnels between users and resources on demand, reducing latency and complexity. This streamlines the remote-user experience and reduces the amount of time users spend onboarding and seeking support for user issues, helping the composite increase end-user productivity by $4.1 million.
- **An 80% reduction in exposure to costly data breaches.** The composite organization strengthens its cyber defenses with AppGate ZTNA in part by making networks invisible to unauthorized users and automatically adjusting access based on device compliance and risk posture. By delivering secure, adaptive access across diverse and constantly changing environments with AppGate ZTNA, the composite organization reduces its exposure to costly data breaches by $3.1 million.
- **An 80% increase in uptime hours from improved network availability and resilience.** With AppGate ZTNA's modular architecture and controller-based failover, the composite organization minimizes downtime disruption, keeping infrastructure operating more smoothly with higher availability for more remote users. As a result of the improved availability and resilience, the composite saves $955,000.
- **A 50% reduction in effort needed to secure and scale network access across environments.** With AppGate ZTNA, the composite organization automates onboarding and provisioning workflows, streamlines policy and entitlement management, and reduces labor effort for security and operations (SecOps), NetOps, infrastructure, and user management. The cumulative labor savings for IT resources amount to $1.7 million over three years.
- **A 90% increase in speed for time to revenue opening and integrating new sites.** Due to the on-demand AppGate ZTNA's direct-routed architecture, the composite organization shortens previously lengthy planning hardware procurement cycles and resource-intensive infrastructure deployments when opening new sites. AppGate's flexible, API-first architecture provides IT teams with full programmability to automate, integrate, and scale new sites. This improved agility and enhanced scalability helps the composite organization improve profit by over $3.0 million over the investment period when compared to the prior environment.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified for this study include:

- **Improved regulatory compliance and cybersecurity insurance posture.** AppGate ZTNA strengthens compliance and cybersecurity insurance posture for the composite by providing flexible, software-defined controls, detailed access visibility, and dynamic tunneling capabilities that supports evolving regulatory needs and improves cyber risk management.
- **Improved product quality.** AppGate ZTNA improves the composite's product quality by enabling developers to maintain uninterrupted, secure access to their work environments, allowing faster task completion and a more responsive development cycle.
- **Increased remote work-related benefits.** AppGate ZTNA enables secure remote work at scale for the composite by allowing employees to access critical systems from any location while maintaining strong access controls, improving workforce flexibility without compromising security.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **AppGate ZTNA.** The composite organization supports 25,000 users per month for total AppGate ZTNA costs of $5.5 million over the investment period.
- **Deployment and management.** The composite organization dedicates 240 IT resource hours within a five-week period to stand up its AppGate ZTNA environment. It requires approximately one-tenth of one FTE to manage the AppGate ZTNA environment. Deployment and management costs total $58,000 for the composite.

The financial analysis that is based on the interviews found that a composite organization experiences benefits of $17.1 million over three years versus costs of $5.5 million, adding up to a net present value (NPV) of $11.6 million and an ROI of 210%.

146,000 hours

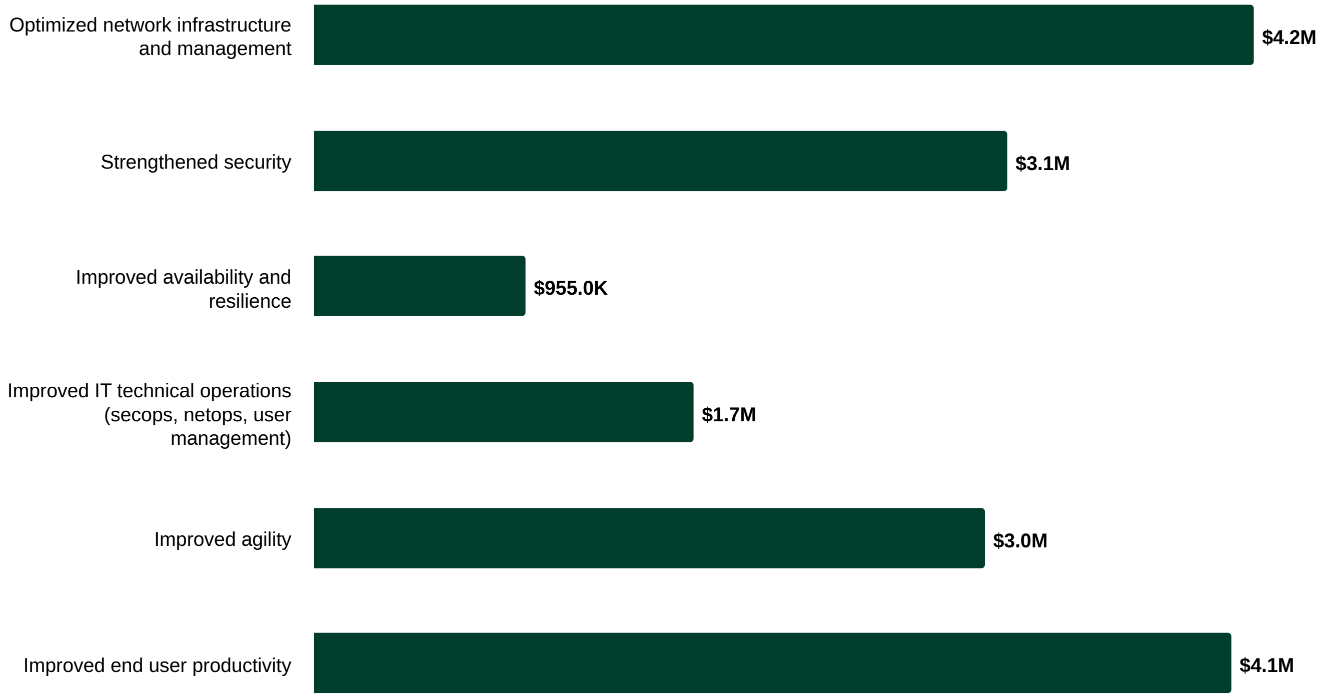
Productive end-user hours recaptured over three years

> *"[With AppGate ZTNA], we have these individual microsegments. [Our attack surface] used to be the whole of the network, and now it is one data center or one section of a data center or one VM [virtual machine]. I think it's 70% to 80% safer than it was in the past and 100% easier. There is no more excuse for not having microsegmentation because it's so easy to do [now]."*
>
> **Network security architect, technology**

Key Statistics

210% **Return on investment (ROI)**	**$17.1M** **Benefits PV**
$11.6M **Net present value (NPV)**	**<6 months** **Payback**

Benefits (Three-Year)



The AppGate ZTNA Customer Journey

Drivers leading to the ZTNA investment

Interviews

Role	Industry	Region	Number Of Users
Network manager	Technology services	Mostly US	>100,000
Network security architect	Technology	Global	5,000 to 10,000
Cybersecurity manager	Manufacturing	Global	10,000 to 20,000
Head of information security	Financial services	US	<500

Key Challenges

Prior to their investment in AppGate ZTNA, interviewees described how their organizations struggled to deliver secure access to core network resources. Whether their organizations were coming from remote-access environment secured by a traditional VPN solution or by a more modern, cloud-routed networking solution, interviewees lamented IT labor inefficiencies, inherent security risks, and rigid, overly permissive access models.

Interviewees noted how their organizations struggled with common challenges, including:

- **Network infrastructure and management complexity and inefficiency.** Interviewees said their organizations previously faced several network and infrastructure challenges, including limited granularity in access control, which restricted the ability to tailor user privileges effectively. Their VPN environments were fragmented and complex, with multiple overlapping configurations and inconsistent IP access across teams. Data residency requirements further constrained flexibility by mandating on-premises storage in specific regions. Legacy multiprotocol label switching (MPLS) architectures added to operational complexity and overhead for the interviewees' organizations, who also operated under tight budget constraints.
  - The network security architect in the technology industry shared: "The big thing is we had VPN concentrators. There was some automation in the client automatically picking the closest entry point. But once you were in, it was a case of routing across the whole of the infrastructure. Everything had to be interconnected to provide access, and you have to be very careful with IP allocations to prevent overlaps."
  - The network manager in the technology services industry said that their organization's complicated MPLS infrastructure made it difficult for IT teams to manage: "We had several VPNs used by different teams. We had different support groups and different IP access by different associates, duplication and all. We were using the MPLS connection model … so we had to have separate [but interconnected] gateways."
- **Costly risks of a cybersecurity breach.** Interviewees said their organizations previously struggled with overly permissive legacy VPN environments that lacked granular access controls, making them vulnerable to threats such as brute force, DDoS, and ransomware attacks. Their infrastructure was difficult to manage, with overlapping routes, outdated software versions, and long maintenance windows that hindered timely updates and increased operational risk. Data residency requirements and fragmented access policies further complicated network design. Additionally, reliance on shared cloud platforms introduced concerns around availability and continuity, especially during major outages.

  The network security architect in the technology industry shared: "[The network] was too open, allowed too much excess, and then patching, adding the additional sites, introducing or injecting routes that could overlap or now route others, requiring lots of planning and huge downtime and maintenance windows. It was difficult to sell to the business, so a lot of it never happened."
- **Poor availability of key network services.** The interviewees' organizations previously encountered significant network and performance challenges that disrupted developer workflows and remote user experiences. Development was often constrained to local machines or exposed to public networks, raising privacy concerns. VPN configurations lacked split tunneling and sufficient bandwidth, leading to performance degradation and congestion at data centers. Interviewees said remote desktop

users experienced latency issues such as delayed input and screen freezes, which impacted productivity and reliability.

The cybersecurity manager in the manufacturing industry stated: “[Our network] was suffering under the weight of being a nonsplit tunneled policy. It was a full tunnel and VPN devices were not connected to sufficient bandwidth to support the user load, so we had performance complaints. Then, we also had issues where too many people on VPN would start to impact business traffic at those data centers, so it was a struggle, and we only had about 400 remote VPN workers at that time.”

- **Inefficient, manual technical operations in SecOps, NetOps, and user management.** Interviewees reported that their organizations previously operated under strained and reactive network environments, where legacy VPN systems required extensive manual provisioning and round-the-clock support across multiple gateways. Their infrastructure was resource-intensive, with large teams dedicated to maintaining outdated systems, leaving little room for innovation or strategic upgrades. Operational efforts at the interviewees’ organizations were focused on patching issues and maintaining stability, often at the expense of forward-looking initiatives. This constant firefighting created a sense of fragility and limited the ability to pursue next-generation solutions.

  The network manager in the technology services industry said that their organization faced so much complexity that it was unable to consolidate down to a single VPN in the prior environment, leading to significant labor redundancies and troubleshooting efforts. They said: “We had around 30 resources supporting just these two VPNs. We had multiple gateways that needed [multilayered] support 24/7, and provisioning was not automated. We had to do a lot of manual provisioning.”

- **Limited business agility.** The interviewees’ organizations previously faced significant challenges during mergers and acquisitions due to complex network integration issues making necessary upgrades risky and impractical due to legacy systems and limited operational knowledge. Technical teams were typically brought in post-acquisition without dedicated onboarding processes, forcing them to devise custom solutions under pressure. Connectivity delays at the interviewees’ organizations were exacerbated by reliance on private hardware-dependent networking models that required long lead times, further slowing integration and operational readiness.

  The cybersecurity manager in the manufacturing industry stated: “Because our connectivity model was private MPLS, we had a minimum 90-day lead time to order one of those circuits. [Then] we would need an address to install it at, so we could get connectivity there eventually, but it took six months to get a circuit in there to actually connect directly to the private network.”

- **Impediments to end-user productivity.** Interviewees said their organizations previously dealt with fragmented VPN environments that required users to manually switch between multiple gateways based on application location, leading to confusion and inefficiency. This setup created a poor user experience for their users, interrupted workflows, and often required full reconnection cycles.

  The network manager in the technology services industry said: “If someone is developing something, they want uninterrupted connection. [In our prior legacy] developer environment, the developers connected to a jump server, and from there they connected to their environment. So if they lost connectivity to the jump server, they needed to [start over and] reconnect from the beginning.”

> *“We would often be on average five to 10 releases behind. … [Our legacy ZTNA solution] was almost too self-service, making it confusing to manage [updates without impact]. We were either increasing our risk, impacting our operations, or both.”*
>
> **Head of information security, financial services**

Investment Objectives For AppGate ZTNA

The interviewees explained how their prior organizational limitations collectively drove the need for more secure, scalable, and manageable solutions like Zero Trust network access and performance-optimized infrastructure to support modern work environments. These challenges highlighted the need for a more seamless, automated, and resilient access model to support both end-user productivity and technical operations.

Interviewees indicated that their organizations invested in AppGate ZNTA in part due to its flexibility, protocol support, and scalability. Unlike other tools that were designed primarily for web and SaaS applications, the interviewees appreciated that AppGate ZTNA closed gaps in coverage for traditional IP-based protocols and legacy systems.

The interviewees' organizations integrated AppGate ZTNA across hybrid environments to automate and modernize their approach to secure access. Interviewees shared how they leveraged AppGate ZTNA to enable their organizations' rapid shift to remote work. Taking advantage of its easy-to-implement split tunneling policies, the interviewees' organizations sought to streamline and improve the remote user experience by increasing performance and connection speeds while introducing improved, granular access policies.

The cybersecurity manager in the manufacturing industry stated: "We have 159 policies [with AppGate]. When we were [in the legacy environment], we had one single policy: you connect, you get access to the entire network. It was a wide-open, full-tunnel situation."

> *"We did evaluate [cloud-routed solutions] and chose to [conduct a proof-of-value exercise] with AppGate specifically because they were not cloud-routed. AppGate is a self-routed ZTNA, which makes them very unique in the space. It's all my infrastructure. Everything is running over my wires, so I'm not dependent on a cloud service for my solution to work."*
>
> **Cybersecurity manager, manufacturing**

Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the interviewees' organizations, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

- **Description of composite.** The composite organization is a globally distributed technical organization with advanced workloads including agentic AI. Of its 25,000 total FTE users, 60% require secure remote access to network resources. The composite is subject to several compliance regimes and is growing both organically and through mergers and acquisitions at a rate of two companies or sites integrated each year.
- **Deployment characteristics.** The functions of network operations, security operations, infrastructure management, and user management are distributed across the IT team, equating to 12 FTEs. The composite organization replaces its cloud-based or traditional VPN and hardware-driven network infrastructure with AppGate ZTNA to public, private, self-hosted workloads and sensitive data across its 40 sites in five weeks. It onboards all 300 corporate applications and 50,000 devices in that timeframe.

KEY ASSUMPTIONS

- $5 billion in annual revenue
- 25,000 total FTE users, 60% of whom require secure remote access
- 12 FTEs on IT team covering networking, security, infrastructure, and user management
- 11% operating margin

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Optimized network infrastructure and management	$1,686,112	$1,686,112	$1,686,112	$5,058,336	$4,193,111
Btr	Improved end-user productivity	$1,657,500	$1,657,500	$1,657,500	$4,972,500	$4,121,957
Ctr	Strengthened security	$1,249,372	$1,249,372	$1,249,372	$3,748,116	$3,107,004
Dtr	Improved availability and resilience	$384,000	$384,000	$384,000	$1,152,000	$954,951
Etr	Improved IT technical operations	$688,896	$688,896	$688,896	$2,066,688	$1,713,182
Ftr	Improved agility	$1,218,461	$1,218,461	$1,218,461	$3,655,382	$3,030,132
	Total benefits (risk-adjusted)	$6,884,341	$6,884,341	$6,884,341	$20,653,023	$17,120,337

Optimized Network Infrastructure And Management

Evidence and data. Interviewees' organizations previously faced high network costs and operational complexity due to reliance on perimeter-based security, legacy VPNs, and hardware-intensive infrastructure. The shift to AppGate's software-defined solutions helped reduce interviewees' organizations infrastructure costs while simplifying administration. Interviewees emphasized how AppGate ZTNA helped their organizations:

- **Reduce network infrastructure cost and complexity.** Interviewees described how their organizations simplified network architecture by eliminating unnecessary infrastructure, hardware, software, and SaaS solutions while also eliminating routing inefficiencies and associated operational costs.
  - The network manager in the technology services industry reported that their organization safely consolidated from two legacy VPNs to a single AppGate ZTNA environment. In the process, their organization eliminated redundant VPN licensing costs. It also shifted away from costly and hardware-intensive MPLS architecture to a software-defined network that required fewer physical machines: "[With AppGate ZTNA], we can easily scale up by spinning additional VMs. We don't need hardware devices. I just need to place a request with my hosting team and they're able to quickly spin up a VM for me to scale."
  - The cybersecurity manager in the manufacturing industry stated: "We were looking at one of our data centers having to go from a 1 gig circuit to a 10 gig circuit but we didn't have to do that [when we went to AppGate]. Once we took the VPN traffic off, the 1 gig was more than enough. … I know the current circuit is $3,000 a month [in connectivity costs] but the 10 gig circuit could have been 10 times that. Once we took the load off there, the network team reported that the usage on that circuit went from 105% down to like 66%."
  - The network security architect in the technology industry shared: "We use [AppGate ZTNA] now for replacing our NAC solution, because … it led to a situation where the office really didn't require any managed network to an extent. You could create a fully open public internet network that gives you internet access only, and the overlay of AppGate onto that network superimposes your defined per-user network, which was really simple."
- **Streamline networking administration costs.** Interviewees also noted how their AppGate environments streamlined network administration across distributed environments with fewer FTEs required for networking infrastructure technology management compared to legacy VPNs and modern, cloud-routed solutions.
  - The cybersecurity manager in the manufacturing industry stated that their organization investigated cloud-routed ZTNA solutions that would have required additional staffing: "Looking at having to hire somebody just to manage my secure access is a little crazy. I know most companies probably already have that but we've never needed it and so AppGate is a big part of why we don't need it."

- The head of information security in the financial services industry shared how their organization was able to avoid the internal administrative effort and risk of patching and updating systems with AppGate ZTNA: "Basically, it's delivered as like a SaaS-type of tenant, so we don't have to think about upgrades, deployment path, or anything like that. They just maintain all that for us, even though we deployed gateways on-prem, they also maintain those. They maintain our entire environment, so they keep things up to date and they will give us a change log."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization's networking infrastructure costs totaled $4 million in the prior environment.
- The composite organization's legacy networking infrastructure required 1.5 FTEs to manage in the prior environment.
- The average fully burdened annual salary for a technical resource is $143,520.
- AppGate ZTNA lowers networking infrastructure technology and management costs by 50% through eliminating routing inefficiencies and unnecessary infrastructure, hardware, software, and SaaS solutions while preventing further associated operational costs.

Risks. The following risks may impact this benefit:

- The number of remote-access users.
- The number of legacy tools and internal labor effort needed to manage them.
- Required capabilities and existing contractual terms.
- Prevailing labor rates and the skill sets available.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $4.2 million.

More than 4,600 hours

Technology management labor effort reallocated to higher-value activities

> *"No more dark fiber, no more $180,000 a year. Over three years it's like $540,000 in savings [with AppGate ZTNA]. That doesn't even take into account outages and upgrades and, you know, a squirrel biting the line."*
>
> **Head of information security, financial services**

Optimized Network Infrastructure And Management

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Networking infrastructure costs in the prior environment	Composite	$4,000,000	$4,000,000	$4,000,000
A2	FTEs required for networking infrastructure technology management in the prior environment	Composite	1.5	1.5	1.5
A3	Fully burdened annual salary for a technical resource	Composite	$143,520	$143,520	$143,520
A4	Percentage reduction in networking infrastructure technology and management costs with AppGate	Interviews	50%	50%	50%
At	Optimized network infrastructure and management	(A1*A4)+ (A2*A3*A4)	$2,107,640	$2,107,640	$2,107,640
	Risk adjustment	↓20%			
Atr	Optimized network infrastructure and management (risk-adjusted)		$1,686,112	$1,686,112	$1,686,112
	Three-year total: $5,058,336		**Three-year present value: $4,193,111**		

Improved End-User Productivity

Evidence and data. Interviewees discussed how AppGate ZTNA made it easier for their users to get onboarded and productive quickly and consistently, giving them secure and consistent access to the tools they need without frustrating delays or performance issues.

- **Faster, more performant and resilient connectivity.** Interviewees said that AppGate ZTNA delivered faster, more resilient, and secure connectivity for their organizations by enabling direct, encrypted tunnels between users and resources, reducing latency, and supporting high-performance secure access at scale.
  - The network manager in the technology services industry explained how their organization enhanced end-user productivity by reducing latency and improving network performance with less interruption than in the prior environment: “We don’t have MPLS connectivity [anymore]. It’s all internet access. It’s point to point. I establish a direct tunnel to the data center, so I have a reduced latency and a faster login as well. [AppGate ZTNA also] improved session availability … and AppGate does its own internal certificate management, and we don’t have to worry about the certificates expiring. … We send a survey to all the users once every six months and we receive a lot of positive feedback about AppGate. Our users are very happy with the way we transformed from the legacy VPN to the new VPN [with AppGate].”
  - The head of information security in the financial services industry reported that prior to AppGate ZTNA, 60% their remote users were experiencing impacts of up to 15 minutes per week. With AppGate ZTNA, all users gained quick and reliable access to network resources leading to measurable productivity improvements: “[The] remote desktop use cases [no longer experienced a] delayed keyboard, a delayed mouse, total screen lockups, or disconnection [altogether. Now with AppGate], users can travel freely and expect high productivity through the system.”
  - The cybersecurity manager in the manufacturing industry noted how AppGate’s demand-based full tunneling helped foster more direct connections between users and resources when needed: “Under the old model, we were struggling to get 300 people connected simultaneously. On AppGate [now], I routinely have [up to] 5,000. … [And] the nice thing with AppGate is you can full tunnel if you want. We have a gateway dedicated to a full-tunnel connectivity … [so users] can flip their AppGate profile to a full tunnel and now they’re egressing out of [a closer data center] for all their traffic … then flip their profile back to their standard profile and they’re back to normal.”
- **Quicker user onboarding with fewer troubleshooting issues.** Interviewees reported that their organizations’ users experienced up to 70% faster onboarding with AppGate ZTNA with fewer access issues and reduced failure rates.
  - The network manager in the technology services industry shared that their users experienced faster onboarding with fewer issues and shorter troubleshooting SLAs with AppGate ZTNA compared to their prior environment. Users, including developers, had more consistent connectivity and fewer steps to access critical resources like the internal development environment: “We have achieved up to 70% faster onboarding because it’s all automated. Users don’t have to wait for a resource to pick the ticket — [they can] get access right now.”

- The cybersecurity manager in the manufacturing industry shared how AppGate neutralized many of the issues impeding remote-end-user productivity at their organization: “File times to load spreadsheets off of the file shares [dropped] from 2 to 3 minutes down to 15 to 20 seconds [for some users]. We had about a 25% connection failure in Australia just due the timeouts. They never have login failures anymore. That’s a non-issue.”

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Sixty percent, or 15,000 of the composite organization’s users require secure remote access to core network resources.
- In the prior environment, remote desktop users experienced additional login steps, slower connection speeds, high latency, frequent session reboots, and other productivity impediments, causing each remote user to waste an average of 4 minutes per day on secure access issues.
- With AppGate ZTNA, the composite can support high-performance secure access at scale. It enables direct, encrypted tunnels between users and resources on demand, reducing latency and complexity. This streamlines the remote user experience and reduces the amount of time users spend onboarding and seeking support for user issues, helping the composite reduce the amount of time users waste on remote desktop issues by 75%.
- The fully burdened hourly rate for an end user is $40.
- End users recapture 25% of the hours that would have otherwise been lost to lengthy remote desktop procedures.

Risks. The following risks may impact this benefit:

- The performance of an organization’s legacy VPN solution.
- The size of organization, employee base, and breadth of AppGate ZTNA adoption.
- Prevailing labor rates and each user’s ability to recapture time savings toward productive activities.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $4.1 million.

More than 146,000 hours

Productive hours recaptured for remote end users over three years

> *“With AppGate ZTNA, logins became much faster, and connections became more reliable and more performant because we were connecting closest to [the user with] more connection points in AppGate than we did [prior]. Because of that, [user] experience got way better and a lot of people got faster access to their core applications.”*
>
> **Cybersecurity manager, manufacturing**

Improved End-User Productivity					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Total users requiring remote access	Composite	15,000	15,000	15,000
B2	Time per day spent loading remote desktop in the prior environment (minutes)	Composite	4	4	4
B3	Percentage reduction in time to load a remote desktop with AppGate	Interviews	75%	75%	75%
B4	Fully burdened hourly rate for an end user	Composite	$40	$40	$40
B5	Productivity recapture	TEI methodology	25%	25%	25%
Bt	Improved end-user productivity	(B1*B2*B3*B4*B5*260)/60	$1,950,000	$1,950,000	$1,950,000
	Risk adjustment	↓15%			
Btr	Improved end-user productivity (risk-adjusted)		$1,657,500	$1,657,500	$1,657,500
	Three-year total: $4,972,500		**Three-year present value: $4,121,957**		

Strengthened Security

Evidence and data. Interviewees shared how their organizations' investments in AppGate ZTNA helped address significant security challenges in the prior environment that stemmed from broad network access, limited policy granularity, and legacy VPN architectures that exposed infrastructure to unnecessary risk. The shift to a Zero Trust model with dynamic, identity-based policies, cloaked infrastructure, continuous risk assessment, and just-enough-access (JEA) with AppGate ZTNA offered the following benefits:

- **Delivered resilient security across complex environments.** The interviewees shared how AppGate ZTNA's direct-routed architecture established encrypted, point-to-point connections between their organizations' users and resources. This design eliminated centralized traffic bottlenecks and reduced exposure to intermediary infrastructure, ensuring consistent security enforcement occurred locally regardless of user location or device type. By maintaining persistent identity verification and dynamic policy evaluation, interviewees noted that AppGate helped prevent unauthorized access and limited the opportunity for attackers to exploit shifting network conditions.

  The cybersecurity manager in the manufacturing industry stated: "The cloaked infrastructure is also another really cool piece of AppGate because [the] infrastructure is invisible to the internet unless you know the right secret code to get in. … We don't have to worry [as much about our] gateways getting attacked because nobody knows they're there. It's unique [to AppGate]. I've yet to experience another solution that does it that way."

- **Improved monitoring capabilities with more precise access controls.** Interviewees' organizations enhanced their access control by replacing legacy VPNs with AppGate's identity-centric, policy-driven architecture. Instead of broad network access, users were granted least-privilege access to only the specific resources they needed, down to individual IP addresses and ports. Interviewees said that access policies were continuously evaluated every 15 minutes, allowing for real-time enforcement based on user status, device posture, and risk scores. This dynamic monitoring meant that if a user's account was disabled or their device became noncompliant (e.g., missing antivirus or outdated patches), access was automatically revoked without manual intervention. These capabilities extended to third-party users and contractors, who were given highly restricted access, minimizing exposure and risk.

  The cybersecurity manager in the manufacturing industry stated: "The user simply can't laterally move anymore unless I have a policy that says they can. They can't scan the network, so if an attacker were to try to get into my AppGate, they would have to get through multifactor first, and even then, they're going to be stuck with an access policy that's based on that user. They're not going to be able to sweep the network. They're not going to be able to do discovery. They're not going to be able to do enumeration, so yeah, it does a lot."

- **Reduced attack surface and breach impact radius.** Interviewees appreciated AppGate's support for private IP provisioning, which eliminated the need for publicly exposed endpoints while reducing complexity and risk of misconfiguration. They also described how AppGate significantly reduced their organizations' attack surfaces, including by cloaking their organizations' network infrastructures and enforcing microsegmentation. Most network appliances became invisible to unauthorized users through techniques like single packet authorization (SPA), making it nearly impossible for attackers to scan or enumerate the environment. Interviewees further noted that their internal organizational systems, including sensitive "crown jewel" assets, were placed behind additional AppGate gateways, requiring explicit policy-based access even from within the corporate network. This approach blocked lateral movement and ensured that attackers could not explore or exploit the network beyond their limited entitlements, even if they had compromised credentials.

- The network security architect in the technology industry shared: "Before AppGate, in public cloud, everything had to be provisioned on public IPs, and you had an entry point that that could potentially be open to the world. With AppGate, you have your single packet authorization requirements, so no one gets in unless you've got you qualify for it. … Everything can happen on private IPs, whether it's on-prem or in the public cloud anywhere in the world. It is just as simple as that."
- The cybersecurity manager in the manufacturing industry stated: "We have certain crown jewel systems … sitting behind a gateway on a nonroutable subnet on a network that you can't get to even if you're on the [our company's] network. You can't get to this network unless you connect to AppGate and you have a policy that says you're allowed to talk to those crown jewel systems."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The cumulative cost of breaches for the composite totaled nearly $3.6 million per year in the prior environment.[3]
- The composite has a 68% likelihood of experiencing one or more breaches.[4]
- Eighty percent of breaches targeting the composite organization originate from external attacks with high potential for lateral movement.[5]
- With AppGate ZTNA, the composite organization tightens network access with expanded policy granularity and decommissions legacy VPN architectures that exposed infrastructure to unnecessary risk. As a result, the composite organization gains the native ability to enforce contextual access control and apply segmentation, reducing infrastructure risk inherent in the prior environment. This minimizes the composite's exposure to breach costs from addressable attacks by 80%.

Risks. The following risks may impact this benefit:

- The size and industry of the organization, which can impact the likelihood and associated costs of security breaches annually.
- An organization's legacy security capabilities and level of AppGate ZTNA coverage and adoption.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $3.1 million.

80%

Reduced risk of exposure to breach costs from addressable attacks with AppGate

> *"With AppGate ZTNA, the attack path is invisible. You have to have the profile installed on your computer to even know where to look, so from that perspective, it's like a 90% reduction in visibility [for the attacker]."*
>
> **Cybersecurity manager, manufacturing**

Strengthened Security

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Cumulative cost of breaches for the composite	Forrester research	$3,588,500	$3,588,500	$3,588,500
C2	Likelihood of experiencing one or more breaches for the composite	Forrester research	68%	68%	68%
C3	Percentage of breaches originating from external attacks targeting organizations, internal incidents, attacks or incidents involving the external ecosystem	Forrester research	80%	80%	80%
C4	Annual risk exposure addressable with AppGate	C1*C2*C3	$1,952,144	$1,952,144	$1,952,144
C5	Reduced risk of exposure to breach costs from addressable attacks with AppGate	Interviews	80%	80%	80%
Ct	Strengthened security	C4*C5	$1,561,715	$1,561,715	$1,561,715
	Risk adjustment	↓20%			
Ctr	Strengthened security (risk-adjusted)		$1,249,372	$1,249,372	$1,249,372

Three-year total: $3,748,116 **Three-year present value: $3,107,004**

Improved Availability And Resilience

Evidence and data. Interviewees reported that their organizations' shift to cloaked infrastructure and dynamic, user-specific routing significantly reduced disruption risk, regardless of user location, device characteristics, and access requirements. Correspondingly, their investments in AppGate ZNTA resulted in improved uptime, speed, and performance.

- The network security architect in the technology industry noted that AppGate's cloaked infrastructure helped improve network performance while also strengthening security: "With AppGate ZTNA, you don't have to deny traffic — the network just doesn't exist if you don't qualify for it, so everything is dark unless you qualify to get access. … You can represent with a VPN solution to an extent but the fact that [with AppGate], in real time, your machine could become uncompliant based on some foreign effect and then your access would automatically be reduced based on your risk score. That was phenomenal, a game changer."
- The network manager in the technology services industry said that AppGate ZTNA made it easier to maintain more up-to-date versions, mitigating disruption both during the patching process and through improved uptime for everyday operations: "When a new version is released, we test that in the development platform and then deploy to the production environment, and it just happens. We do that every six months. [Before AppGate], we had to do more upgrades [than we actually] could because [in] the complex [legacy] environment … had outages [when we tried]. Now it's a smooth process because we can just do it one controller at a time so there is no impact for the end users. [T]here are fewer major incidents. … It's designed in such a way that we have backups across countries or regions, so the outages are very minimal, and end users are also very happy."
- The cybersecurity manager in the manufacturing industry stated: "Under the old model, we were struggling to get 300 people connected simultaneously. On AppGate [now], I routinely have [up to] 5,000. … [Prior to AppGate], we were spending 30 to 40 hours a month troubleshooting [legacy] VPN problem, mainly around bandwidth and performance. Ultimately, not being able to solve it was the biggest reason … why we jumped over to AppGate and just went full steam with it. The performance at those sites where the VPN headends were got much better after AppGate was deployed because we took the load off of them of having to support all the VPN users."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization has 15,000 users requiring secure remote access to network resources.
- In the prior environment, the composite organization's legacy VPN experienced 1 hour of downtime per month due to outages and severe performance degradations.
- With AppGate ZTNA, the composite organization decommissions its legacy VPN, eliminates routing inefficiencies, and increases the number of high-performance users it can support. As a result, it reduces the total annual hours of downtime due to VPN outages by 80%.

- The fully burdened hourly rate for an end user is $40.

Risks. The following risks may impact this benefit:

- Organizational size, geography, industry, and revenue mix.
- Average availability and performance in legacy environments.
- Prevailing labor rates.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $955,000.

80%

Increase in uptime hours from improved secure access availability and resilience

> *"In the time we've had [AppGate ZTNA], we have not had any incidents because everything is so redundant there, everything is at least in duplication, and you have tremendous fail over possibilities and endless configuration management options."*
>
> **Network security architect, technology**

Improved Availability And Resilience

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Total users requiring secure access	Composite	15,000	15,000	15,000
D2	Downtime per month for remote users due to VPN outages in the prior environment (hours)	Composite	1.0	1.0	1.0
D3	Percentage reduction in hours of downtime due to VPN outages with AppGate	Interviews	80%	80%	80%
D4	Fully burdened hourly rate for an end user	Composite	$40	$40	$40
Dt	Improved availability and resilience	D1*D2*D3*D4	$480,000	$480,000	$480,000
	Risk adjustment	↓20%			
Dtr	Improved availability and resilience (risk-adjusted)		$384,000	$384,000	$384,000

Three-year total: $1,152,000 **Three-year present value: $954,951**

Improved IT Technical Operations

Evidence and data. Interviewees highlighted many ways in which AppGate ZTNA improved IT workflows for security, infrastructure, and network operational teams, as well as provided efficiencies for user and access management teams. Interviewees described how this eliminated manual onboarding processes, decreased ticket volumes, and improved the ability to segment critical assets without increasing risk or administrative burden. This helped the interviewees' organizations deploy smaller teams to support more agile and cost-effective IT operations. In particular, interviewee shared how AppGate ZTNA:

- **Enhanced networking and infrastructure operations.** Interviewees reported that their organizations' transition to automated workflows with AppGate ZTNA helped automate workflows related to networking and microsegmentation.
- **Improved security operational efficiency across hybrid environments.** Interviewees shared how AppGate ZTNA platform's flexibility allowed security teams to maintain consistent policies across diverse environments, improving agility while

strengthening overall security posture.

The cybersecurity manager in the manufacturing industry stated: “Different use cases have different requirements, so we have close to 600 different applications [requiring secure access policies] plus 50 to 60 vendors, each of them connecting to maybe one or two servers each. … [Without AppGate, I] would probably need to double the team. We couldn’t do it with a six-person security team for 12,000 employees. It’s just too much, there’s just too much to do.”

- **Streamlined identity and access management workflows.** Interviewees reported many ways in which AppGate ZTNA helped IT resources enable fast, secure access in dynamic environments. They noted how policies were very dynamic in nature, making it easier for their teams to rapidly adjust and easily update policies as well once they were created.

  The head of information security in the financial services industry shared how their organization used AppGate ZTNA to manage
  entitlements: “Entitlements are easy to create with or without Application Discovery Service. Application Discovery Service helps you do it at scale but just even creating entitlements [was] something that would take maybe anywhere from like 4 to 8 or more labor hours for a senior or higher network architect [before AppGate ZTNA]. Now, I can have any one of our engineers easily work on it [and] deploy in 15 minutes or so to make a major policy change versus a day [in the prior environment].”

- **Reduced ticket volumes and streamlined secure access troubleshooting.** Interviewees reported many ways in which AppGate ZTNA helped IT resources enable fast, secure access compared to the prior environment.

  The network manager in the technology services industry also explained: “The volume has reduced drastically. … I see daily volume of around 15 tickets and in the past it was probably around 70 tickets per day. … In the past, because the volume of tickets was higher, we were taking around on an average 8 hours for a ticket reservation on an average. But now the SLA is less than 4 hours.”

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- In the prior environment, the composite organization dedicated approximately 25,000 labor hours, or the equivalent of 12 IT resources, to technical workflows related to security, networking, infrastructure, and user and access management.
- With AppGate, the composite organization automates workflows across the onboarding and provisioning lifecycle, manages policies and entitlements more easily and consistently across diverse environments, and integrates with key third-party security and identity solutions. This reduces the labor effort needed to secure remote network access at scale by 50%.
- The fully burdened hourly rate for a technical resource is $69.

Risks. The following risks may impact this benefit:

- The number of users.
- The size of the IT team covering SecOps, NetOps, infrastructure, and user management.
- Legacy processes and solutions required to add, secure, and manage users and networking infrastructure in the prior environment.
- Prevailing labor rates, the skill sets available, and the extent to which IT resources can recapture time savings toward productive work.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.7 million.

50%

Reduction in technical resources required to achieve ZTNA with AppGate

> *"Our AppGate portion is handled by a small team of probably three, so we've scaled down our requirement tremendously, and I wouldn't say necessarily our [staffing] requirement. There's been a lot of cost savings across the business, so we're maximizing the abilities of our teams in keeping them small."*
>
> **Network security architect, technology**

Improved IT Technical Operations

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Internal technical resource time needed to achieve ZTNA in the prior environment (hours)	Composite	24,960	24,960	24,960
E2	Percentage reduction in technical resources required to achieve ZTNA with AppGate	Interviews	50%	50%	50%
E3	Fully burdened hourly rate for a technical resource	Composite	$69	$69	$69
Et	Improved IT technical operations	E1*E2*E3	$861,120	$861,120	$861,120
	Risk adjustment	↓20%			
Etr	Improved IT technical operations (risk-adjusted)		$688,896	$688,896	$688,896

Three-year total: $2,066,688 **Three-year present value: $1,713,182**

Improved Agility

Evidence and data. Interviewees discussed how the shift to dynamic, software-defined network access with AppGate ZTNA enabled rapid gateway deployment and accelerated business operations. Customer-reported value drivers for this newfound business agility included:

- **Shortened planning cycles with fewer requirements.** Some interviewees described how their legacy, hardware-driven network architecture required months of coordination, hardware procurement, and manual configuration. With AppGate ZTNA, they described how their organizations were able decrease time to market with less resource planning and capital expenditure planning required to integrate newly acquired companies into their parent structure or to set up new offices or data centers.
  - The network security architect in the technology industry shared: "Everything is simple to do. You don't need to plan as much anymore. In the past, when we set up a new location or we had a big project going, we had months and months of planning and with a lot of logistics involved. Now, [we have] the ability to just spin up something to get you into an isolated area with no access from outside other than the gateway. It was really a game changer that made everything easier and quicker [to scale]."
  - The head of information security in the financial services industry said: "[Prior to AppGate], a new office setup would easily take six months just to order private lines, build out the architecture, and enable end-to-end connectivity. Now, we're basically just installing high-speed internet everywhere and letting things connect directly, which is ideal. [Without AppGate], my head of infrastructure would probably have his two senior most architects working on every aspect of that [with] hundreds of man hours [spread over] long nights and weekends."
  - The cybersecurity manager in the manufacturing industry stated: "[It's nice] to know that I'm not going to have to run around and buy a bunch of gear if we announce an acquisition tomorrow. I can wait until the next cycle and incorporate that into the major purchase plan because we've got that AppGate capability we can deploy nearly instantly."
- **Accelerated integration and deployment workflows.** With AppGate, interviewees indicated that their organizations were able to deploy infrastructure rapidly. Some noted that their organizations transformed their rigid legacy access models and onboarding processes to be more flexible and were able to quickly adapt to changing business needs. This allowed them to

onboard thousands of users within days with minimal internal resources during periods of high M&A growth.

The cybersecurity manager in the manufacturing industry stated: “[AppGate ZTNA] speeds up the time to integrate, which just speeds up everything. It speeds up the ability to [achieve] synergies and cost [savings] and collaboration. Everything moves faster when everybody has access to what they need when they need it. [The business user] is never frustrated by waiting on security [because] they don’t have to wait.”

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- In the prior environment, the composite organization:
  - Earned 1% of its annual revenue, or $961,000 per week, from growth activities like organically opening new sites and through mergers and acquisitions.
  - Grew by an average of two sites annually, either by organic growth or M&A activity.
  - Took eight weeks to open a new site or integrate an acquired company.
- With AppGate ZTNA, the composite organization avoids lengthy planning hardware procurement cycles when opening new sites due to the on-demand nature of AppGate infrastructure provisioning. The flexible, API-first architecture empowers IT teams with full programmability to automate, integrate, and scale new sites. This reduces the integration timeline and increases time to revenue by 90%.
- The composite organization’s operating margin is 11%.

Risks. The following risks may impact this benefit:

- The number of users.
- The number of companies acquired and/or new sites opened throughout the investment period.
- Legacy processes required to absorb a new company and/or open a new site in the prior environment.
- Prevailing labor rates and the skill sets available.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $3.0 million.

90%

Reduction in time to integrate an acquired company and/or open a new site with AppGate ZTNA

> *“Accommodating changes is much cheaper because there’s no extra cost [to scale with AppGate ZTNA]. Everything is dynamic now and so therefore I don’t have to plan as much anymore. There are no hardware costs and stuff like that. The flexibility is tremendous, and it helps in every way.”*
>
> **Network security architect, technology**

Improved Agility					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
F1	Revenue from acquisitions	Composite	$50,000,000	$50,000,000	$50,000,000
F2	Revenue per acquisition per week	F1/52	$961,538	$961,538	$961,538
F3	Acquisitions per year	Composite	2	2	2
F4	Time to integrate an acquired company in the prior environment (weeks)	Composite	8	8	8
F5	Reduction in time to integrate an acquired company with AppGate	Interviews	90%	90%	90%
F6	Operating margin	Composite	11%	11%	11%
Ft	Improved agility	F2*F3*F4*F5*F6	$1,523,076	$1,523,076	$1,523,076
	Risk adjustment	↓20%			
Ftr	Improved agility (risk-adjusted)		$1,218,461	$1,218,461	$1,218,461
	Three-year total: $3,655,382		**Three-year present value: $3,030,132**		

Unquantified Benefits

Interviewees mentioned the following additional benefits that their organizations experienced but were not quantified for this study:

- **Improved regulatory compliance and cybersecurity insurance posture.** Interviewees shared how AppGate supported their organizations in navigating evolving regulatory demands by offering flexible security controls, detailed access reporting, and continuous visibility. They noted how this strengthened their organizations' compliance efforts while also improving cyber insurance outcomes.
  - The network security architect in the technology industry shared how their organization was able to enhance the security of their development and production environment while also enriching the information needed for auditors and compliance requirements: "Because of the reporting that we can get from the system on every single access attempt and all network flows, it has really enriched what we can provide as evidence for compliance. … And because you have that ability to test it on a single user or a block of users, it's easy to prove a concept before moving to production. That's another thing that frequently comes up in our compliance reviews, the fact that … the production system can be split into dev if you like for a short amount of time, for a short a small space, or for a small project because everything is software defined."
  - The cybersecurity manager in the manufacturing industry shared how their organization's demand-based full tunneling capabilities improved their ability to reach compliance: "Our insurance company loves the fact that we're on AppGate. They love the Zero Trust of it. They love our policy granularity. They love the invisible infrastructure, the continuous risk evaluation. … One of our compliance standards states that when you're accessing certain government data, you cannot be simultaneously connected to a secure and nonsecure network, so when users need to access that data, they have to flip to a full tunnel VPN profile. … AppGate is definitely a key piece of the compliance puzzle for us. We're leveraging it to satisfy multiple controls."
- **Improved product quality.** Some interviewees shared how AppGate helped improve product quality by ensuring developers stayed securely connected to their work environments without interruption, allowing them to focus on tasks and complete them more efficiently. As a result, they noted that their software development lifecycle was shorter and more responsive to customer feedback.

  The cybersecurity manager in the manufacturing industry stated: "They don't have to worry about getting access to what they need because AppGate will provide that access when they need it … and I think that enables the business to move faster just in general. Safety is obviously number one but then running fast and doing things quickly is also key. On the secure access side of things, we're never the bottleneck. We can get you access as fast as you need it. You're not going to be waiting on AppGate to get anything done. The moment you ask, it's going to happen, and it's going to work the first time. It just enables the business to run at the speed that they need to do great things."

- **Increased remote work-related benefits.** AppGate enabled secure remote work at scale by allowing employees at the interviewees' organizations to access systems from any location, which improved hiring flexibility, supported workforce mobility, and ensured compliance with location-based access restrictions.
  - The network security architect in the technology industry shared how AppGate enabled a secure remote work by allowing employees to relocate freely while maintaining controlled access based on location policies, improving flexibility without compromising compliance or visibility. They noted, "The flexibility really does bring a lot of ease to the [remote user] base."
  - The cybersecurity manager in the manufacturing industry stated that AppGate enabled secure access for employees regardless of location, allowing their organization to hire the best talent without geographic limitations and ensuring reliable connectivity to necessary resources: "I think the success of AppGate has accelerated our ability to hire remotely, so instead of restricting our hiring to just geographic regions where we have offices, we're able to look for the best candidate irrespective of where they're located and we know that the AppGate solution will get them access to their data that they need to do their job no matter where they are in the world."
  - The network security architect in the technology industry shared: "The massive overall impact has been on end users because no one has to be anywhere to do their work — the idea that you don't have to get to an office because you need access to critical resources. Everyone can be available 24/7 and there's no excuse for you not to be able to get to your work wherever you are."

> *"I think we'd be paying significantly higher premiums if we were still on a traditional VPN, probably in the order of 20 to 30% and also possibly would have to go to a higher-risk vendor for our insurance. [With AppGate], we're able to get a better policy from a better policy provider because we evaluate quite low on the risk register."*
>
> **Cybersecurity manager, manufacturing**

Flexibility

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement ZTNA and later realize additional uses and business opportunities, including:

- **Cloud transformation enablement.** Interviewees also discussed how they leveraged AppGate's flexible deployment capabilities to support cloud transformation across global sites. Even in environments with legacy infrastructure and limited historical documentation, AppGate facilitated smooth transitions and modernization efforts.

  The cybersecurity manager in the manufacturing stated that AppGate was a critical part of their organization's cloud transformation strategy due to its extensibility into private cloud infrastructures located in other geographical regions and ability to deploy gateways closer to users and their workloads.
- **Integrations.** Interviewees shared how their organizations integrated AppGate ZTNA seamlessly into their evolving technology stacks with identity and endpoint security platforms to enforce conditional access policies at the network layer, enhancing compliance, reducing risk, and improving overall security posture through real-time device and user validation.

  The head of information security in the financial services industry said that their organization integrated AppGate with Microsoft Entra ID to enforce conditional access policies at the network layer, creating a tightly coordinated system of identity, device compliance, and Zero Trust network controls: "[We like] its ability to be interoperable with other best of breed [solutions] like CrowdStrike… [And] one of the things that AppGate does really well is it pulls in Entra ID, Microsoft telemetry, and it could basically enforce those conditional access policies, but at the network layer. … So, it's multifactor with numbers matching plus compliant device, plus being enrolled in our CrowdStrike system with full enforcement. And so, if all of those things don't match, you're not getting in. It's the perfect symbiosis of all of those things."
- **Zero Trust initiatives.** For interviewees whose organizations were in the process of integrating Zero Trust principles into their environments, AppGate ZTNA was noted as an enabling factor.
  - The cybersecurity manager in the manufacturing industry stated: "AppGate ZTNA was the first product we put in at [our company] that followed the Zero Trust model. … Over the last five years, we've ratcheted [our] policies down using the data

  within AppGate … by [using it to] look at where they actually are going. We use the AppGate data to reinforce the AppGate policy and now, probably 90% of the policies would qualify as a Zero Trust [compliant] policy."

  - The head of information security in the financial services industry stated that AppGate ZTNA's ability to thwart lateral movement provided an important additional layer of security: "We [can] achieve full universal ZTNA with AppGate, which we couldn't achieve with [our legacy cloud-routed ZTNA solution] because we can never fit into that old funnel. … [By governing all of those 594 devices versus just 200 laptops, basically we've increased our ability to protect to 100% of our endpoints versus a subset of our endpoints in the past. It's a huge net improvement."

- **Agentic AI enablement.** Interviewees indicated that AppGate facilitated ongoing collaboration and feature development aligned with their organizational needs, enabling more responsive support and integration of emerging technologies like agentic AI workloads and systems.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Total Economic Impact Approach).

> *"I feel like we're in a really comfortable place from a conditional access perspective. And yeah, AppGate is a gigantic part of that. [With its key integrations], it's an additional layer of symbiosis between our conditional access policies, our identity controls, and our Zero Trust Network Access control."*
>
> **Head of information security, financial services**

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Gtr	AppGate ZTNA	$0	$2,200,000	$2,200,000	$2,200,000	$6,600,000	$5,471,074
Htr	Deployment and management	$18,216	$16,698	$15,939	$15,787	$66,640	$58,430
	Total costs (risk-adjusted)	$18,216	$2,216,698	$2,215,939	$2,215,787	$6,666,640	$5,529,504

AppGate ZTNA

Evidence and data. Interviewees described how their organizations' respective AppGate ZTNA costs were configured on a per-user per-month basis. Total number of sites and IP addresses were noted as additional cost drivers.

- The cybersecurity manager in the manufacturing industry stated: "They never charged us a dime [to scale up]. We pay for the licenses and then they do whatever it takes to make us successful. It's amazing. They're fantastic."
- Pricing may vary. Contact AppGate for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes the composite organization licenses 25,000 users per month.

Risks. The following risks may impact this cost:

- The number of AppGate features deployed.
- The size, coverage, and adoption of AppGate ZTNA deployment.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $5.5 million.

> *"Accommodating changes is much cheaper because there's no extra cost [to scale with AppGate ZTNA]. Everything is dynamic now and so therefore I don't have to plan as much anymore. There are no hardware costs and stuff like that. The flexibility is tremendous, and it helps in every way."*
>
> **Network security architect, technology**

AppGate ZTNA						
Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Total users	Composite	0	25,000	25,000	25,000
G2	Cost per user	Interviews	0	$80	$80	$80
Gt	AppGate ZTNA	G1*G2	$0	$2,000,000	$2,000,000	$2,000,000
	Risk adjustment	↑10%				
Gtr	AppGate ZTNA (risk-adjusted)		$0	$2,200,000	$2,200,000	$2,200,000
	Three-year total: $6,600,000			Three-year present value: $5,471,074		

Deployment And Management

Evidence and data. Interviewees' organizations across industries successfully deployed AppGate with limited resources, rapidly onboarding thousands of users and applications through strong internal execution and responsive vendor support. Once deployed, AppGate required minimal ongoing management with small teams handling maintenance through largely automated processes.

- **Deployment.** The interviewees' organizations deployed AppGate with limited resources, onboarding users and applications. Interviewees also noted receiving highly responsive support from the AppGate team.
  - The cybersecurity manager in the manufacturing industry stated that their organization was able to rapidly onboard their AppGate environment with limited resources within two weeks: "We got 5,000 remote users onboarded in less than two weeks. … I personally deployed 90% of the AppGate infrastructure in seven days."
  - The network manager in the technology services industry told Forrester that their complex organization onboarded approximately 1,000 corporate applications within a six-month deployment period: "It was a great experience and terrific teamwork. I have to thank our AppGate team there because they're part of the squad. They helped us in all aspects. [Our team] included the architect and engineering team and operations support team."
  - The cybersecurity manager in the manufacturing industry stated: "We did not leverage any third-party consulting with AppGate; we did it all in-house, [but] we could not have had the success we had without AppGate's help. They have been the most responsive company I've ever worked with in security, probably by a factor of five."
- **Management.** Interviewees emphasized that AppGate required minimal ongoing effort to manage, with small teams and largely automated processes handling policy updates and access entitlements.

  The cybersecurity manager in the manufacturing industry indicated that the minimal ongoing labor costs was a primary selling point for their organization's investment in AppGate: "Now that we're fully deployed and we've been there for a while, maybe one-tenth of one FTE is dedicated to the maintenance and management of AppGate. It's not much."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization dedicates 240 IT resource hours within a five-week period to stand up its AppGate ZTNA environment.
- The composite organization dedicates approximately one-tenth of one FTE to managing the AppGate ZTNA environment over the three year-period, with slight management efficiencies gained year over year as administration workflows mature and reach a steady state.
- The fully burdened hourly rate for a technical resource is $69.

Risks. The following risks may impact this cost:

- The size, scope, and complexity of deployment and legacy environment.
- Prevailing labor rates, internal skill sets, and training requirements for IT resources and end users.
- Implementation requirements, organizational priorities, and change management efforts.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $58,000.

1/10 of an FTE

Ongoing management costs for the composite organization

> *"It's very low maintenance once it's up and running. It's just policy updates and system upgrades. We don't have to go in there every day and do things. Once it works, it just works."*
>
> **Cybersecurity manager, manufacturing**

Deployment And Management

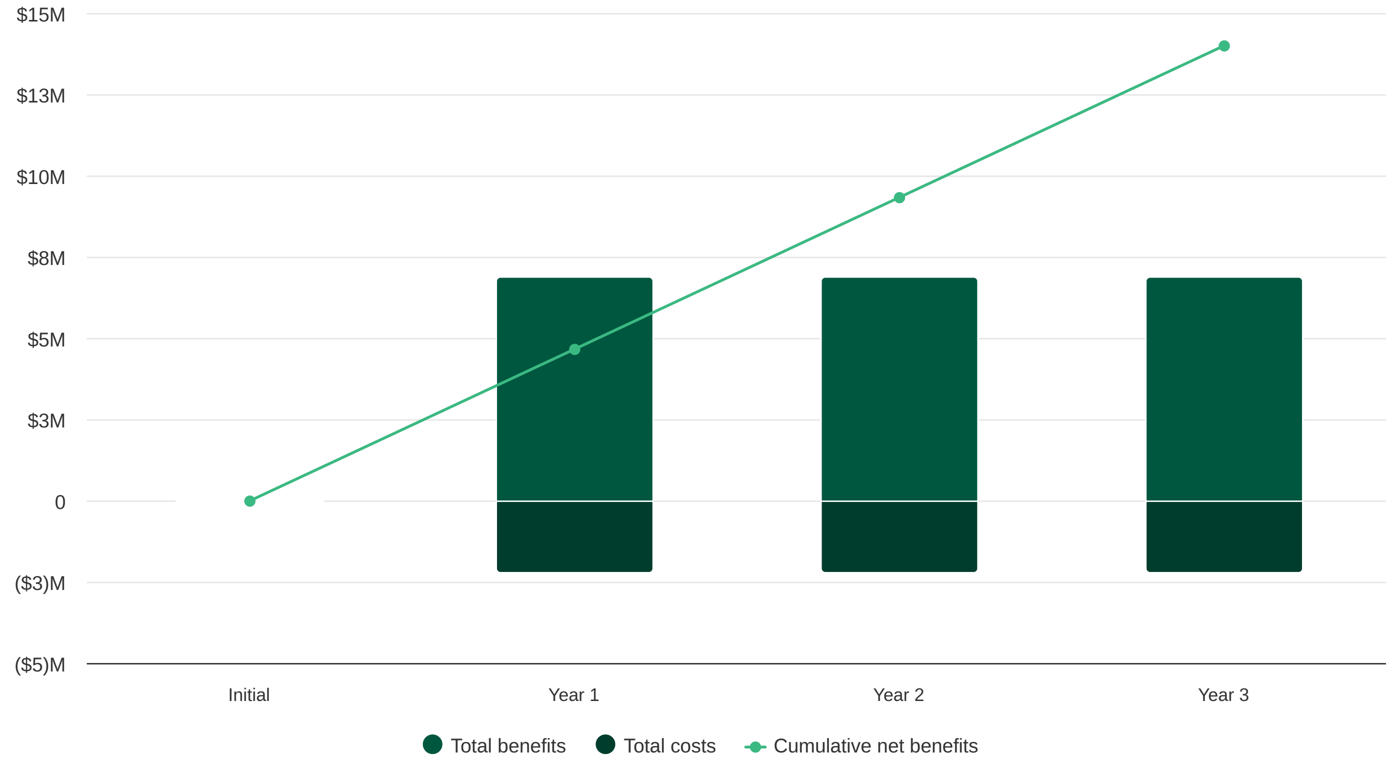
Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Total time necessary for AppGate deployment (hours)	Interviews	240	0	0	0
H2	Total time of ongoing AppGate administration (hours)	Interviews	0	220	210	208
H3	Fully burdened hourly rate for a technical resource	Composite	$69	$69	$69	$69
Ht	Deployment and management	(H1+H2)*H3	$16,560	$15,180	$14,490	$14,352
	Risk adjustment	↑10%				
Htr	Deployment and management (risk-adjusted)		$18,216	$16,698	$15,939	$15,787

Three-year total: $66,640 **Three-year present value: $58,430**

Financial Summary

Consolidated Three-Year, Risk-Adjusted Metrics

Cash Flow Chart (Risk-Adjusted)



Cash Flow Analysis (Risk-Adjusted)						
	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($18,216)	($2,216,698)	($2,215,939)	($2,215,787)	($6,666,640)	($5,529,504)
Total benefits	$0	$6,884,341	$6,884,341	$6,884,341	$20,653,023	$17,120,337
Net benefits	($18,216)	$4,667,643	$4,668,402	$4,668,554	$13,986,383	$11,590,833
ROI						210%
Payback						<6 months

Please Note

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

TEI Framework And Methodology

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in ZTNA.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that ZTNA can have on an organization.

Due Diligence

Interviewed AppGate stakeholders and Forrester analysts to gather data relative to ZTNA.

Interviews

Interviewed four decision-makers at organizations using ZTNA to obtain data about costs, benefits, and risks.

Composite Organization

Designed a composite organization based on characteristics of the interviewees' organizations.

Financial Model Framework

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

Case Study

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

Glossary

Total Economic Impact Approach

Benefits

Benefits represent the value the solution delivers to the business. The TEI methodology places equal weight on the measure of benefits and costs, allowing for a full examination of the solution's effect on the entire organization.

Costs

Costs comprise all expenses necessary to deliver the proposed value, or benefits, of the solution. The methodology captures implementation and ongoing costs associated with the solution.

Flexibility

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. The ability to capture that benefit has a PV that can be estimated.

Risks

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

Financial Terminology

Present value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

Net present value (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made unless other projects have higher NPVs.

Return on investment (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

Discount rate

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

Payback

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendixes

APPENDIX A

Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

APPENDIX B

Endnotes

[1] Source: Global Cybersecurity Market Forecast, 2024 To 2029, Forrester Research, Inc., September 9, 2025.

[2] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

[3] Cumulative breach costs are computed using the composite organization's size (revenue or number of employees) as an input to a regression analysis of reported total cumulative costs for all breaches for organizations that experienced at least one breach in the past 12 months. Source: Forrester's Security Survey, 2025, "Using your best estimate, what was the total cumulative cost of all breaches experienced by your organization in the past 12 months?" Base: 1,740 global security decision-makers who have experienced a breach in the past 12 months. The cumulative breach cost is then multiplied by a 67% likelihood for organizations to experience one or more breaches in a given year. Source: Forrester's Security Survey, 2025, "How many times do you estimate that your organization's sensitive data was potentially compromised or breached in the past 12 months?" Base: 2,643 global security decision-makers. Regression analysis of the reported total cumulative costs of all breaches experienced by security decision-makers' organizations in the past 12 months. The composite organization's revenue is used as the input to the regression formula. Source: Forrester's Security Survey, 2024, "Using your best estimate, what was the total cumulative cost of all breaches experienced by your organization in the past 12 months?" Base: 1,660 global security decision-makers who have experienced a breach in the past 12 months.

[4] Regression analysis of the likelihood of experiencing one or more breaches, using the frequency that organizations experienced breaches in the past 12 months as reported by security decision-makers. The composite organization's revenue is used as the input to the regression formula. Source: Forrester's Security Survey, 2025, "How many times do you estimate that your organization's sensitive data was potentially compromised or breached in the past 12 months?" Base: 2,643 global security decision-makers

[5] Percentage of breaches by primary attack vector, as reported by security decision-makers whose organizations experienced at least one breach in the last 12 months. Source: Forrester's Security Survey, 2025, "Of the times that your organization's sensitive data was potentially compromised or breached in the past 12 months, please indicate how many of each fall into the categories below." Base: 1,766 global security decision-makers who have experienced a breach in the past 12 months.

Disclosures

Readers should be aware of the following:

This study is commissioned by AppGate and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in ZTNA. For any interactive functionality, the intent is for the questions to solicit inputs specific to a prospect's business. Forrester believes that this analysis is representative of what companies may achieve with ZTNA based on the inputs provided and any assumptions made. Forrester does not endorse AppGate or its offerings. Although great care has been taken to ensure the accuracy and completeness of this model, AppGate and Forrester Research are unable to accept any legal responsibility for any actions taken on the basis of the information contained herein. The interactive tool is provided 'AS IS,' and Forrester and AppGate make no warranties of any kind.

AppGate reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

AppGate provided the customer names for the interviews but did not participate in the interviews.

Consulting Team:

Courtenay O'Connor

Alyssa Dolan

PUBLISHED

November 2025