FORRESTER®

The Total Economic Impact™ Of Semperis

Business Benefits Enabled By Semperis

A Forrester Total Economic Impact™ Study
Commissioned By Semperis, May 2024

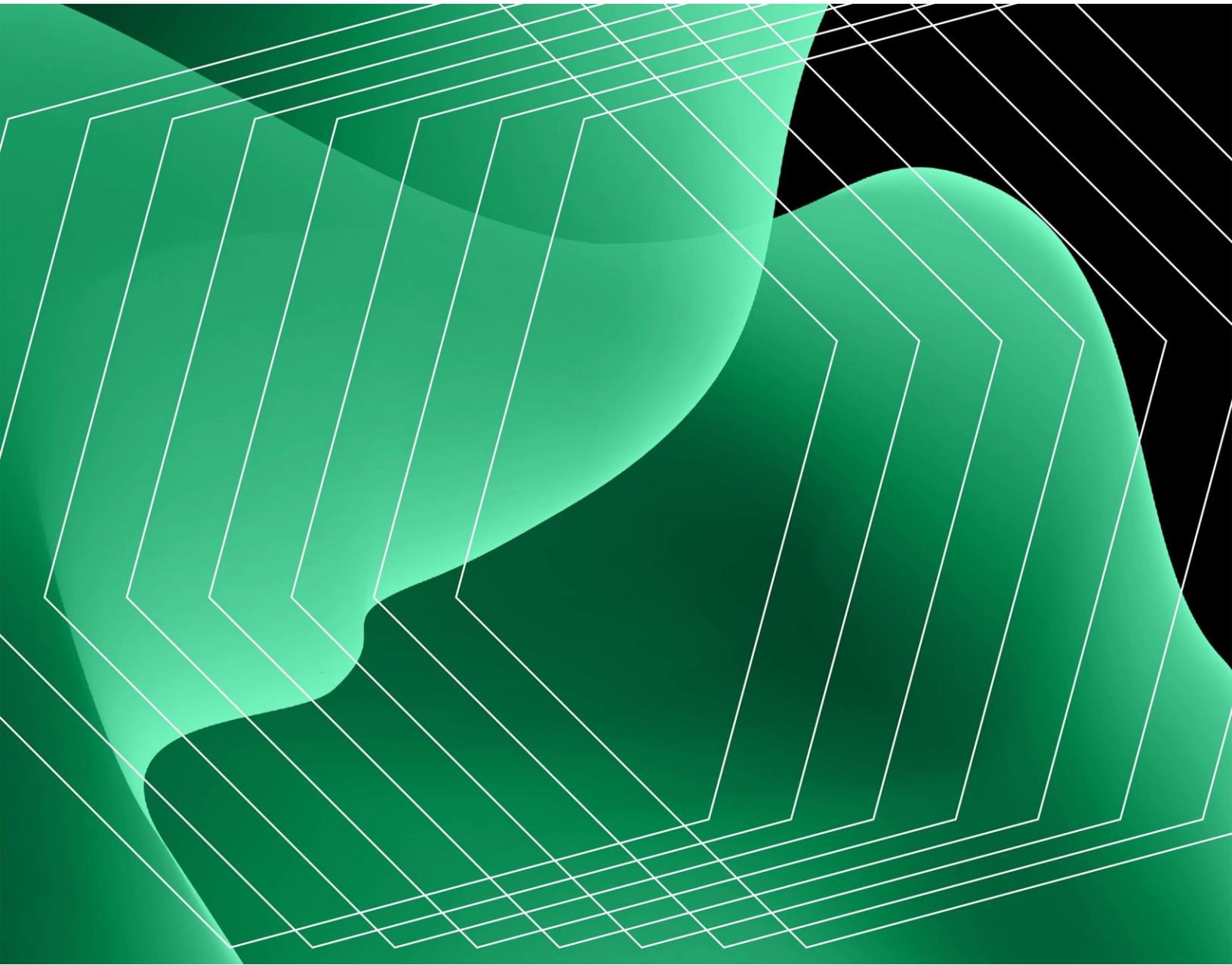


Table Of Contents

Consulting Team:

Sanitra Desai

Zahra Azzaoui

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

The ever-evolving cybercriminal ecosystem continuously poses new and unique security threats to organizations of all shapes and sizes. Most (84%) organizations experienced an identity-related breach in the last year and, with the average total breach costing $3.5 million, organizations must combat this risk by investing in technology that safeguards hybrid enterprise identity systems with on-premises Active Directory (AD) and Entra ID in the cloud.[1] Forrester found that organizations that use Semperis can both recover their AD in the event of a ransomware attack and remediate object- and group-level incidents in AD and Entra ID 90% faster. This translates to millions of dollars in savings and reduces the likelihood of a successful attack.

Semperis protects critical enterprise identity services for security teams charged with defending hybrid AD environments from cyberattacks, data breaches, and operational errors. By offering comprehensive protection for identity environments — including Active Directory, Entra ID, and Okta — Semperis provides a layered defense against identity-based incidents before, during, and after an attack, all supported by an expert, dedicated incident response team.

Semperis commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential benefits and financial impacts enterprises may realize by deploying Semperis.[2]

AD disaster recover
90% faster

Three-year benefits (PV)
$9.5M

Reduction in time spent monitoring the hybrid AD environment
40%

Reduction in average likelihood of a successful hybrid AD-related ransomware attack
25% reduction

Object- and group-level recovery
90% faster

To better understand the benefits and risks associated with this investment, Forrester interviewed six representatives with experience using Semperis. The interviewees' organizations range in size and geography and are from a variety of industry sectors, including healthcare, financial services, energy, and professional services. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is in a highly regulated industry with sensitive data and has 50,000 employees and revenue of $10 billion per year.

Prior to investing in Semperis, interviewees noted their organizations used a mix of identity threat detection, response, and prevention tools, and used generic enterprise backup and/or traditional AD recovery solutions, such as a bare-metal recovery approach, to back up their data. This, in conjunction with the existing tools' inefficient manual processes and subsequent business challenges, put interviewees' organizations at a heightened risk of an AD- and Entra ID-related ransomware attack and AD- and Entra ID-related operational inefficiencies.

After the investment in Semperis, interviewees noted their organizations gained full visibility of their hybrid AD environments and were thus able to efficiently identify and address potential cyberthreats to proactively avoid an identity-based attack. By improving their overall security posture, the interviewees' organizations reduced the likelihood of an identity-based attack and cut down credential abuse. Interviewees stated that in the event of an AD attack, their organizations achieved faster AD recovery with Semperis' Active Directory Forest Recovery (ADFR) solution, reducing end-user downtime and reaping significant labor and revenue savings. The interviewees also noted their organizations also saw additional time savings on AD and Entra ID environment monitoring and object- and group-level remediation through the automation capabilities of Semperis' Directory Services Protector (DSP) solution. Through these improvements, interviewees said their organizations saw added value through improved brand credibility and the ability to maintain a strong security posture as their businesses continued to grow.

KEY FINDINGS

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

- **Improved business continuity due to faster hybrid AD attack recovery yielding $3.9 million in savings.** Semperis' Active Directory Forest Recovery (ADFR) tool reduces the composite organization's AD backup and recovery timeline by 90%. The composite organization also gains the ability to conduct post-breach forensics to close back doors and eliminate persistence. By reducing the recovery timeline and the risk of malware reinfection, the composite limits its revenue and labor losses during downtime, avoiding prolonged business disruption and quickly regaining operational stability by bringing AD back to a trusted state.
- **Improved business continuity through a reduction in the likelihood of a successful hybrid AD attack worth $1.2 million.** In addition to the business continuity savings realized through ADFR, the composite organization reaps additional value with Directory Services Protector (DSP). DSP provides full visibility of hybrid AD environments to close existing security gaps by continuously monitoring for security indicators and identifying potential threats before they manifest into a full-on attack. This risk reduction allows the composite to reduce the likelihood of experiencing successful AD and Entra ID attacks by 25%, further cutting its revenue and labor losses. Note that the security benefit of preventative action is difficult to quantify accurately, so the 25% reduction is intentionally a conservative estimate.
- **Object- and group-level remediation savings worth $4.3 million.** When unintended changes are made to objects and groups in the hybrid AD environment, the composite organization uses DSP's granular rollback capabilities to quickly restore normal configurations of individual attributes, group members, objects, and containers — reducing end-user downtime and improving operational resilience.
- **Hybrid AD environment monitoring efficiencies that save $109,000.** The composite organization realizes substantial IT team time savings for AD environment monitoring with DSP in place. Seamless integration into existing

security operations center (SOC) environments and real-time alerts and automation features, such as automatic rollback of suspicious changes and continuous security assessments to combat configuration drift, allow the composite's IT team to spend less time manually investigating potential threats in AD and Entra ID and more time on high-value work.

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

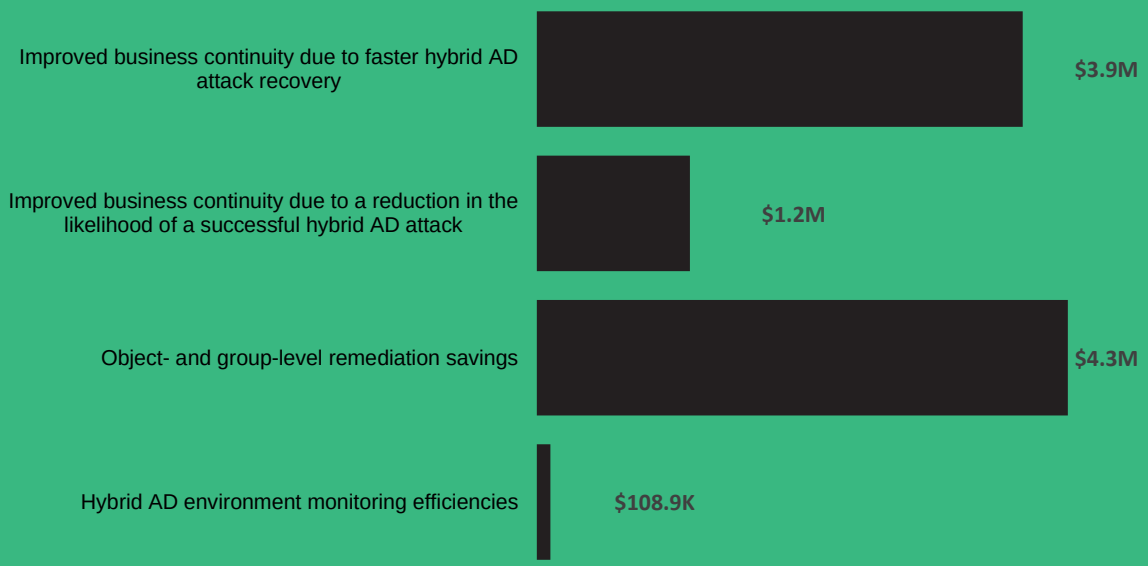
- **Improved brand credibility.** The composite organization experiences improved hybrid AD environment resilience and data integrity through its investment in Semperis. By applying Semperis' AD security expertise and experience in identity attack incident response to achieve a stronger security posture, the composite boosts its reputation among customers and unlocks new avenues for business growth.
- **Improved visibility of the hybrid AD environment.** The composite organization gains a comprehensive view of its hybrid AD environment, improving its threat detection abilities and subsequently reducing its AD attack surface area.

The representative interviews and financial analysis found that a composite organization experiences benefits of $9.5 million over three years.

> "We initially went with Semperis because they are the market leader in the space, but their solution has actually delivered value to our organization. Their patented technology for malware or wiper attack recovery of AD along with our newfound full visibility into our AD environment has delivered great results."
>
> TECHNICAL ARCHITECT, AD, PROFESSIONAL SERVICES

AD disaster recovery	Reduction in average likelihood of a successful AD-related ransomware attack	Object- and group-level recovery	Reduction in time spent monitoring the AD environment	Benefits PV
90% faster	**25% reduction**	**90% faster**	**40%**	**9.5M**

Benefits (Three-Year)



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 Semperis.

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

DISCLOSURES
Readers should be aware of the following:

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

Forrester makes no assumptions as to the potential benefits 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 Semperis.

Semperis 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.

Semperis provided the customer names for the interviews, but Semperis did not participate in the interviews. Only Semperis customers participated in closed-door interviews.

Due Diligence
Interviewed Semperis stakeholders and Forrester analysts to gather data relative to Semperis.

Interviews
Interviewed six representatives at five organizations using Semperis to obtain data about 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 fundamental elements of TEI in modeling the investment impact: benefits, flexibility, and risks. Given the increasing sophistication of financial 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.

The Semperis Customer Journey

Drivers leading to the Semperis investment

Interviews				
Role	**Industry**	**Region**	**Revenue**	**Employees**
Technical architect, AD	Professional services	Global	$60B+	500,000+
• CISO • Network systems analyst	Healthcare	North America	$20B+	100,000+
Manager, identity management and engineering	Healthcare	North America	$5B+	25,000+
Senior manager, server architecture	Energy	Global	$10B+	5,000+
SVP	Financial services	North America	$5B+	10,000+

KEY CHALLENGES

Before investing in Semperis, the interviewees' organizations used disparate tools for identity threat detection, response, and prevention, but did not have a comprehensive hybrid AD protection platform inclusive of recovery from AD-related ransomware attacks. This setup created an array of inefficient manual processes and cascading business challenges related to significant end-user downtime and other business impacts, including damage to brand credibility. Interviewees noted that their organizations' prior environments also consisted of a rudimentary bare-metal recovery backup approach that did not guarantee a fully ransomware-free data backup following an AD attack, leaving their organizations vulnerable to the risk of malware reinfection.

Interviewees explained that the disparate nature of their organizations' before states yielded many blind spots and subsequent failures to identify and mitigate potential threats because they lacked a comprehensive view of their hybrid AD and Entra ID environments.

The interviewees noted how their organizations struggled with common challenges, including:

- **Lack of visibility into hybrid AD environments.** Interviewees reported a fragmented view of their organizations' AD and Entra ID landscape in the absence of a centralized solution with robust monitoring capabilities, leaving their organizations susceptible to undetected security threats and unauthorized access. Without full visibility, interviewees' organizations were unaware of critical changes and therefore had delayed incident response. This lack of visibility was particularly problematic in hybrid AD environments, where attacks could start in Entra ID and move to on-premises AD or vice versa, expanding the attack surface. Consequently, the interviewees noted their organizations suffered from a weakened security posture and poor AD and Entra ID change management practices.

  The technical architect of AD in professional services said: "We were unaware of what was going on in our AD environment before Semperis. It was difficult to track all of the changes that were being made across the organization on a daily basis and make sure that nothing suspicious was happening."

- **Arduous and time-consuming AD attack recovery effort, resulting in business disruptions and prolonged downtime.** Interviewees described the recovery process in the aftermath of an AD-related ransomware attack as long and labor-intensive. After an attack, IT teams were tasked with investigating the surface area of the attack, identifying affected accounts, and restoring configurations to a secure state. The prolonged recovery timelines resulted in extended periods of end-user downtime, disrupting business continuity. The cost of this cumbersome recovery process encompassed both revenue and productivity losses for the interviewees' organizations.

  The CISO in healthcare explained: "We did not have a tool in place to determine the threats in our Active Directory environment. We simply relied on the base controls, which were not sufficient because if a threat actor gets inside, that means they've penetrated through our system despite the protections. It was hard for us to determine the root cause and quickly recover."

The CISO continued, “Without Semperis, we had to spend weeks around the clock trying to recover from such a catastrophic disaster because we couldn’t leave one stone unturned trying to determine the source of the attack.”

> “[Before Semperis], we had non-AD-specific recovery tools that could not recover AD in the event of [an attack]. We needed to invest in ADFR because AD attacks are an existential threat to our entire organization. AD supports everything at our company.”
>
> SVP, FINANCIAL SERVICES

- **Frequent disruptions due to human error.** Interviewees’ organizations struggled with reoccurring accidental and unauthorized changes to objects and groups in the AD environment. These unintentional mistakes sometimes affected authentication and access for several hundred employees at a time. However, remediating these incidents was a highly manual process, and a lack of real-time visibility into object and group modifications made it difficult for the interviewees’ organizations to quickly identify and remediate incidents to restore users’ system access, resulting in extended end-user downtime.

  The technical architect of AD in professional services explained: “Whenever we had general administrative complications [around] accidental deletions or replication errors, it completely shook up our environment. It was a major inconvenience to our daily operations.”

- **Cumbersome and inexhaustive domain controller backup management and maintenance.** Interviewees described their previous manual domain controller backup process as time-consuming and incomplete. Without automation capabilities, their organizations experienced difficulties managing and

maintaining comprehensive and up-to-date domain controller backups. Furthermore, without the guarantee that their backups were completely reliable and free of ransomware, interviewees' organizations faced a heightened risk of data loss during AD attacks.

The technical architect of AD in professional services said: "[Before Semperis], we relied on basic backup solutions, but they were not specific to AD. In many cases, the data from those backups was infected with malware."

The technical architect of AD continued: "In the prior environment, if our backups were infected, then we would not be able to restore it. All of the backups rolling back to a month would be infected and we wouldn't be able to spin back up the environment to a good state."

The CISO in healthcare said: "We had a significant concern about an adversary getting into our AD environment and taking it offline. We didn't know how to rebuild a corrupted AD and were at risk of the attacker destroying our backups that would be very difficult to fully restore."

- **Damage to the organization's reputation.** AD-related ransomware undermined the credibility of the interviewees' organizations due to a perceived inability to mitigate cybersecurity threats and safeguard sensitive customer data. The resulting diminished customer trust and loyalty hindered sales, customer acquisition, and overall business growth opportunities.

  The technical architect of AD explained: "We were seeing the attacks happening to other enterprises or other businesses and we did not want to put [our] reputation at risk. That's one of the reasons why we chose this path."

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Shift their reactive approach to hybrid AD-related ransomware attacks into a proactive one, guided by identity security experts with direct experience successfully conducting AD- and Entra ID-related incident response for global organizations.
- Improve business continuity by reducing the AD attack recovery time.

- Ensure a fully malware-proof recovery to avoid further disruption and data loss.
- Use post-breach forensics capabilities to close back doors and eliminate persistence following an attack.
- Reduce end-user downtime during hybrid AD-related ransomware attacks and object- and group-level incidents.
- Improve visibility into the hybrid AD environment to mitigate potential risks and reduce IT team effort.
- Elevate the IT team's reputation across the organization by enabling proven recoverability of the business-critical identity system.

> "We were seeing organizations across the globe getting hit with AD attacks, which caused us to look inward and [ask ourselves] if we want to remain reactive or become proactive. We invested in Semperis because we want to make sure we're always prepared to handle incoming threats."
>
> TECHNICAL ARCHITECT, AD, PROFESSIONAL SERVICES

> “We were recommended Semperis and after doing our research, it became clear that it’s an amazing tool. When we looked at their competitors, feature to feature, no one came close. Once we met with the Semperis team and ran through the demo, I was very impressed — it was not a hard sell.”
>
> SENIOR MANAGER, SERVER ARCHITECTURE, ENERGY

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 six interviewees, 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 global organization headquartered in North America with 50,000 employees. It generates $10 billion in annual revenue. The organization operates in a highly regulated industry and has sensitive data. All segments of the composite’s businesses rely on Active Directory to function. The composite conducts identity access and authentication through an Active Directory environment that is globally distributed across three forests and 30 domain controllers and operates a hybrid identity environment.

Deployment characteristics. The composite organization adopts Semperis’ full suite of products, which includes Active Directory Forest Recovery (ADFR), Directory Services Protector (DSP), and the community tool, Purple Knight, across all 30 domain controllers in Year 1. The composite has six IT resources that spend a portion of their time monitoring the hybrid AD environment using Semperis.

Key Assumptions

$10 billion revenue

50,000 employees

Six IT resources spend 25% of their time monitoring the AD environment

30 domain controllers

Three forests

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	Improved business continuity due to faster hybrid AD attack recovery	$1,574,640	$1,574,640	$1,574,640	$4,723,920	$3,915,897
Btr	Improved business continuity due to a reduction in the likelihood of a successful hybrid AD attack	$495,720	$495,720	$495,720	$1,487,160	$1,232,782
Ctr	Object- and group-level remediation savings	$1,721,250	$1,721,250	$1,721,250	$5,163,750	$4,280,494
Dtr	Hybrid AD environment monitoring efficiencies	$43,805	$43,805	$43,805	$131,414	$108,936
	Total benefits (risk-adjusted)	$3,835,415	$3,835,415	$3,835,415	$11,506,244	$9,538,109

IMPROVED BUSINESS CONTINUITY DUE TO FASTER HYBRID AD ATTACK RECOVERY

Evidence and data. Interviewees said that investing in Semperis' ADFR solution enabled swift AD recovery, minimizing the financial impact of the attack by mitigating prolonged disruptions to business operations. Throughout the duration of the attack, a compromised AD meant that employees were locked out and therefore could not access their accounts and resources to continue their work. This cost of downtime was compounded by a reduction in revenue attributable to the inability to serve customers due to inaccessible systems and missed sales opportunities. With Semperis, all interviewees noted that the full AD-recovery timeline was reduced from several days to just a few hours. The automation capabilities of ADFR simplified the previously complicated, error-prone, multi-step process to a few clicks. In turn, the Semperis investment allowed interviewees' organizations to bounce back quickly after a hybrid AD attack and reestablish operational stability, ultimately cutting revenue losses, reputational damage, potential litigation and fines, and labor losses.

ACTIVE DIRECTORY RECOVERY	
Before Semperis	***After Semperis***
Long Active Directory recovery ranging from weeks to months	90% reduction in recovery time, cutting downtime from weeks to hours
Manual, error-prone recovery process involving tedious metadata cleanup, hardware provisioning, and other steps	Full automation of the entire recovery process (including cleanup) to accelerate recovery
Risk of follow-on attacks from the same or different attackers	Post-breach forensics to close backdoors and eliminate persistence after recovery to prevent repeat attacks
Large legacy bare-metal recovery backups that can contain malware that would be restored during recovery	Cyber-first backup approach that decouples the OS to prevent malware reinfection and reduces backup size
Environment configuration constraints that hinder hardware provisioning and recovery setup	Fast, flexible AD recovery that doesn't depend on preconfigured hardware, including the ability to restore to any virtual or physical hardware and on-the-fly IP mapping
Typically, no, or limited AD recovery expertise on staff, requiring time-intensive and pricey third-party help, prolonging recovery	Direct, 24/7 access to a dedicated AD incident response team

- The manager of identity management and engineering in healthcare explained that prior to Semperis, recovering from an AD attack and ensuring a ransomware-free backup of data took two weeks. The manager also noted that in the prior environment, their organization had to enlist third-party services in addition to internal resources to restore their data. After implementing Semperis, it took less than two business days to conduct recovery and post-recovery activities without the help of any external resources and return to normal.

The manager explained: “It was ADFR that prompted our investment in Semperis because of the risk to the organization around restoring our forests after an AD-related ransomware attack. Being able to manage the AD recovery process more effectively and efficiently is what got us to move away from a bare metal image backup to get back up and running with a fully functioning Active Directory more quickly.”

Interviewees noted that ADFR also automated time-consuming administrative cleanup tasks following an AD recovery, such as rebuilding the Global Catalog and restoring metadata, which resulted in further time savings.

The manager of identity management and engineering continued: “Once AD is brought back online, it’s ready for business. [Other tools] typically require a lot of cleanup that has to occur before you can release it back to the business.”

- The senior manager of server architecture in energy said that recovering from an AD-related ransomware attack without Semperis would take at least one week of effort from their entire AD team, IT access admin team, ID management team, and project managers. With Semperis in place, this timeline was reduced to 6 hours to resume business operations.
- The CISO in healthcare reported that the time it took their organization to recover from an AD attack with Semperis and ensure that all backup data was ransomware-free dropped from three weeks to 4 hours. The CISO emphasized that this reduction was critical to the business because 1 hour of downtime costs several million dollars for the healthcare organization.

  The CISO in healthcare described the time savings their organization reaped during the post-recovery process with ADFR’s automated malware-proof backup capability: “Being able to do a few clicks and get the restoration from a backup is huge — it’s like night and day. [Before Semperis], recovery was a nightmare because it was so complex and required a lot of resources. Having the ability to restore from a backup of AD at your fingertips is huge. … It’s mind-boggling how simple it is.”

> “In the event of a ransomware attack, [Semperis] ensures we can easily recover our AD in hours versus weeks or months. … To know that we have a viable alternative when the worst of the worst happens allows us to sleep better at night.”
>
> CISO, HEALTHCARE

- The SVP in financial services said that an AD attack without ADFR would render their entire bank inoperable for weeks and would impact at least 25,000 people until full recovery was achieved. They also explained that a single hour of downtime costs the business several million dollars because every segment of the business relies on AD to function.

  The SVP described the impact of an AD-related ransomware attack on their customers, “Active Directory supports authentication and authorization, so an AD-related attack not only breaks down the internal workforce production but also impacts our customers’ ability to interact with the bank because they rely on AD for authorization.”

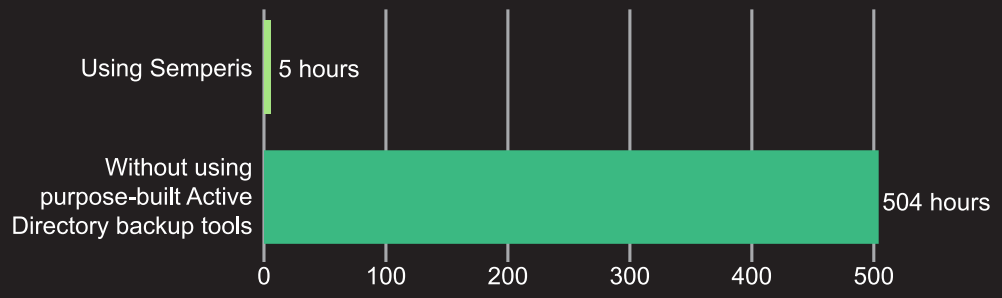
> “If you don’t learn from what happens to someone in your industry, then you’re sticking your head in the sand. So, we got up and said, ‘What can we do differently?’ and Semperis was part of a total package we put together to help solve that problem. It doesn’t mean that bad things aren’t going to happen, but instead of being down for weeks, we’re down for hours.”
>
> CISO, HEALTHCARE

TOTAL HOURS TO RECOVER ACTIVE DIRECTORY

Semperis ADFR enables faster Active Directory recovery and allows the composite organization to resume critical business operations signfiicantly earlier following a ransomware attack.

The benefit of recovering Active Directory with Semperis will vary depending on the duration of Active Directory recovery before an organization invests in Semperis.

While this analysis conservatively assumes that the composite organization has an AD attack recovery time before Semperis of 48 hours, readers are encouraged to consider their own situation. The following data is based on customer interviews to help readers better understand their own situations.



Base: Six representatives with experience using Semperis for Active Directory recovery at their organizations.
Source: A commissioned study conducted by Forrester Consulting on behalf of Semperis, April 2024.

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

- Forrester quantifies the cost of 1 hour of downtime based on the lost labor due to end-user downtime and lost revenue from stalled operations. For every hour that Active Directory is down, the composite organization experiences combined labor and revenue losses of $2.7 million.
- In the legacy environment, it takes the composite organization 48 hours to recover from an AD-related ransomware attack using the legacy backup tool or manual approach. Note, in environments without an AD-specific backup and recovery solution, 48 hours for recovery is an extremely conservative estimate made for the purpose of financial modeling. Most companies Forrester interviewed estimated that a full AD recovery would range from many days to several weeks or even months of downtime.

- Semperis' ADFR tool reduced the time it takes for the composite organization to recover from a hybrid AD attack by 90%.
- The probability of experiencing a ransomware attack that infects Active Directory varies greatly across organizations of diverse firmographics. As such, for this financial analysis, Forrester makes an extremely conservative assumption that the composite organization has a 2.0% chance of experiencing an AD-related ransomware attack. Based on Benefit B, the composite organization experiences a 25% reduction in the average likelihood of AD-related ransomware attack, making the likelihood of an attack 1.5% for the composite organization.

90%

Reduction in AD attack recovery time

VARIATION IN RISK OF RANSOMWARE

As ransomware becomes more prevalent, some industries, geographies, and types of organizations are more at risk than others.The benefit of recovering Active Directory with Semperis will vary depending on the likelihood that a ransomware attack will infect an organization's Active Directory.

While this analysis conservatively assumes an average of a 1.5% likelihood of a ransomware attack infecting Active Directory each year after investing in Semperis, readers are encouraged to consider their own situation. The following scenarios have been calculated for the composite organization to help readers better understand their own situations.

Likelihood of a ransomware attack infecting Active Directory	Expected value of faster recovery through Semperis
0.5%	$1.3 million
2.0%	$5.2 million
3.5%	$9.1 million
5.0%	$13.1 million
7.5%	$19.6 million

Base: Six representatives with experience using Semperis for Active Directory recovery at their organizations.
Source: A commissioned study conducted by Forrester Consulting on behalf of Semperis, April 2024.

Risks. Improved business continuity due to faster AD attack recovery may vary depending on the following:

- The elements taken into consideration when calculating the cost of 1 hour of downtime.
- The average likelihood of an AD-related ransomware attack, which may vary depending on organizational size and industry, security posture, user awareness and training, backup and recovery practices, and external threat landscape.
- The hybrid AD attack recovery time in the prior environment.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $3.9 million.

Improved Business Continuity Due To Faster Hybrid AD Attack Recovery					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Employees	Composite	50,000	50,000	50,000
A2	Cost of one hour of downtime to the business	Composite	$2,700,000	$2,700,000	$2,700,000
A3	Hybrid AD attack recovery time before Semperis (hours)	Interviews	48	48	48
A4	Business losses during AD recovery process	A2*A3	$129,600,000	$129,600,000	$129,600,000
A5	Reduction in AD recovery time with Semperis	Interviews	90%	90%	90%
A6	**Subtotal: Business value protected during hybrid AD attack with Semperis**	**A4*A5**	**$116,640,000**	**$116,640,000**	**$116,640,000**
A7	Average likelihood of an AD-related ransomware attack after Semperis	B7	1.5%	1.5%	1.5%
At	Improved business continuity due to faster hybrid AD attack recovery	A6*A7	$1,749,600	$1,749,600	$1,749,600
	Risk adjustment	↓10%			
Atr	Improved business continuity due to faster hybrid AD attack recovery (risk-adjusted)		$1,574,640	$1,574,640	$1,574,640
	Three-year total: $4,723,920			**Three-year present value: $3,915,897**	

IMPROVED BUSINESS CONTINUITY DUE TO A REDUCTION IN THE LIKELIHOOD OF A SUCCESSFUL HYBRID AD ATTACK

Evidence and data. Interviewees noted that in conjunction with ADFR, their organizations reduced the likelihood of a successful AD attack by using Semperis' DSP tool to continuously monitor hybrid AD activities, including user authentication, access requests, and changes to AD and Entra ID configurations for unusual or suspicious activities. The ability to analyze log data, authentication attempts, and changes to AD and Entra ID configurations in real time with DSP helped the interviewees' organizations identify potential threats before they escalated to full-blown attacks. DSP's advanced features also enabled automated remediation to recognize threats and automatically roll back unauthorized changes, reducing the chances of a ransomware attack that compromises AD. Through this reduction, the interviewees' organizations protected additional business value on top of what they retained with ADFR in Benefit A, further improving business continuity.

- The network systems analyst in healthcare explained how DSP enabled better oversight of their organization's hybrid AD environment to prevent issues before they occur: "DSP helps us mitigate issues before they become issues. With Semperis, we're able to identify user accounts that have possibly been tampered with and notify those users before a larger problem arises. Also, it helps us identify weaknesses in our [AD environment] so we can actually address them. It's just a wonderful tool."
- The CISO in healthcare said: "Having the knowledge that there was no dormant threat lying within our Active Directory somewhere waiting to pounce was a huge sigh of relief. In the past, we've experienced AD attacks where our backup was only partially clean, and we did not know if we had remnants of ransomware. Semperis gives us the peace of mind that nothing is lying dormant. Having that knowledge is a huge relief."
  They continued: "Before DSP, we had zero visibility into our [hybrid AD environment]. Today, we have a tool that generates alerts that we're able to actively validate whether or not we have a threat in the system rather than finding out after an attack happens. It's an intrusion prevention system for us. That's worth its weight in gold."

> “DSP gives us immediate knowledge if [a threat] is lying dormant. It gives us protection, so that if something happens in our AD environment, we can just roll back the change. For example, if a threat actor gets into our Active Directory and makes 18 changes, Semperis can just roll all 18 right back for us and we don’t have to do any recovery. It’s a holy-grail product.
>
> **CISO, HEALTHCARE**

- The technical architect of AD in professional services described how Semperis reduced the risk of reinfection and provided post-breach forensics to prevent repeat attacks. The interviewee explained: “Semperis helps us conduct post-recovery cleanup activities to ensure that an AD attack does not resurface. It guarantees that we have a ransomware-free environment. We would not be able to get a clean restore without Semperis.”
- The SVP in financial services said: “Semperis provides more targeted recovery in the case of a ransomware attack. It gives us greater control to support business resiliency and allows us to continue to harden our AD environment to reduce the attack surface. Without [DSP], it can be very difficult to narrow down threats.”

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

- Forrester quantifies the cost of 1 hour of downtime based on the lost labor due to end-user downtime and lost revenue from stalled operations. For every hour that Active Directory is down, the composite organization experiences combined labor and revenue losses of $2.7 million.

- In the legacy environment, it takes the composite organization 48 hours to recover from an AD-related ransomware attack using the legacy backup tool or manual approach. Note, in environments without an AD-specific backup and recovery solution, 48 hours for recovery is an extremely conservative estimate done for the purpose of financial modeling. Most companies Forrester interviewed estimated that a full AD recovery would range from many days to several weeks or even months of downtime.
- Semperis' ADFR tool reduces the time it takes for the composite organization to recover from an AD attack by 90%.
- The probability of experiencing a ransomware attack that infects Active Directory varies greatly across organizations of diverse firmographics. As such, for this financial analysis, Forrester makes an extremely conservative assumption that the composite organization has a 2.0% chance of experiencing an AD-related ransomware attack.
- Through continuous monitoring of the AD and Entra ID environments with DSP, the composite organization reduces the likelihood of a successful hybrid AD attack from 2.0% to 1.5% — a 25% reduction.

Risks. Improved business continuity due to a reduction in the likelihood of a successful hybrid AD attack may vary depending on the following:

- The elements taken into consideration when calculating the cost of 1 hour of downtime.
- The average likelihood of an AD-related ransomware attack before investing in Semperis, which may vary depending on organizational size and industry, security posture, user awareness and training, backup and recovery practices, and external threat landscape.
- The reduction in the average likelihood of a successful AD-related ransomware attack with Semperis.
- The AD attack recovery time in the prior environment.

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 $1.2 million.

25%

Reduction in the average likelihood of a successful AD attack

Improved Business Continuity Due To A Reduction In The Likelihood Of A Successful Hybrid AD Attack					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Cost of one hour of downtime to the business	A2	$2,700,000	$2,700,000	$2,700,000
B2	Hybrid AD attack recovery time before Semperis (hours)	Interviews	48	48	48
B3	Business losses during AD recovery process	B1*B2	$129,600,000	$129,600,000	$129,600,000
B4	Reduction in AD recovery time with Semperis	Interviews	90%	90%	90%
B5	**Subtotal: Business value protected during hybrid AD attack with Semperis**	**B3*B4**	**$116,640,000**	**$116,640,000**	**$116,640,000**
B6	Average likelihood of an AD-related ransomware attack	Forrester research	2.0%	2.0%	2.0%
B7	Average likelihood of an AD-related ransomware attack after Semperis	Interviews	1.5%	1.5%	1.5%
B8	Reduction in the average likelihood of an AD-related ransomware attack with Semperis	1-(B7/B6)*100%	25.0%	25.0%	25.0%
B9	**Subtotal: Avoided likelihood of an AD-related ransomware attack with Semperis**	**B6-B7**	**0.5%**	**0.5%**	**0.5%**
Bt	Improved business continuity due to a reduction in the likelihood of a successful hybrid AD attack	B5*B9	$583,200	$583,200	$583,200
	Risk adjustment	↓15%			
Btr	Improved business continuity due to a reduction in the likelihood of a successful hybrid AD attack (risk-adjusted)		$495,720	$495,720	$495,720
	Three-year total: $1,487,160			**Three-year present value: $1,232,782**	

OBJECT- AND GROUP-LEVEL REMEDIATION SAVINGS

Evidence and data. Interviewees described the significant remediation effort and subsequent end-user downtime resulting from object- and group-level incidents before investing in DSP. Object- and group-level incidents at the interviewees' organizations included several annual instances of the following events at the individual or collective level, respectively:

- Unintended modifications to organizational units affecting the organizational structure.
- Unauthorized changes to user account attributes (e.g., passwords, group memberships).
- Deletion or modification of security groups affecting access permissions.
- Compromise of privileged user accounts or service accounts.
- Changes to group policies that impact security settings across the network.

Interviewees stated that DSP detected and automatically reversed unwanted changes to objects and groups in the AD and Entra ID environments quickly and with minimal human intervention from IT teams. While these incidents were not malicious and often were a result of accidental modifications made by employees, they hindered end-user productivity because the affected employees were unable to log in to their computers or access network resources tied to AD or Entra ID credentials, including files, folders, and applications needed to continue working. The resulting productivity losses spanned the duration of IT teams' remediation efforts, which involved identifying, mitigating, and recovering from the incident to restore normal configurations.

- The network systems analyst in healthcare explained that human operational errors occurred on a weekly basis at their organization, affecting between 300 and several thousand employees depending on the severity of the incident. Before Semperis, remediating these errors took several hours; after the investment, it took 30 minutes.

> “We were having frequent group- and object-level incidents where we would have to spend hours trying to restore objects before Semperis. Now, we know how to fix the issue within minutes. It’s night and day.”
>
> NETWORK SYSTEMS ANALYST, HEALTHCARE

- The manager in identity management and engineering in healthcare said that before Semperis, fixing role-based access control issues used to take six subject-matter experts (SMEs) several days; now with DSP in place, it takes two SMEs about 2 hours to resolve.

  The manager in identity management and engineering outlined the effort previously required to remediate object- and group-level incidents: “[Before Semperis,] when a user would make an object-level change, we would rely on our cyberthreat team to investigate the changes to ensure that they were done with the appropriate request management. To initiate the investigation with our prior tool, our team would get generated alerts and incident management from the SIEM [security information and event management]. They would then have to use multiple interfaces to determine which changes needed to be undone to generate a report of every individual user and change. This process was time-consuming and highly error-prone, requiring deep expertise. With DSP, unintentional changes made by end users are automatically rolled back to the source and notifications are sent out in lieu of our previous process. We no longer have to do all of the investigation prior to determining the best course of action. Semperis has allowed us to become proactive rather than reactive.”

  The manager continued: “We needed subject-matter experts due to the complexity of the [remediation] process. When an incident occurred, we had to make sure we had resource availability from the right people that could

effectively restore the object. This put a strain on our resources because it was hard to get other team members trained on such a specific task."

The manager concluded: "Semperis allows us to optimize our operations in regard to addressing [object- and group-level] incidents as they come up. It gives us an ongoing ability to reeducate our teams and train them on new and better ways of fixing issues to get end users back up and running."

> "We chose Semperis because it simplifies the remediation process. With DSP, we no longer need subject-matter experts to be the gatekeeper of fixing issues when they arise."
>
> MANAGER, IDENTITY MANAGEMENT AND ENGINEERING, HEALTHCARE

- The senior manager of server architecture in energy reported that it used to take their team up to 8 hours to remediate an AD-related human error before Semperis. After the investment, it took 30 minutes to fully resolve the issue and get end users back into the system to continue their work.

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

- On average, 1% of the composite organization's employee count is affected by a major object- or group-level incident.
- In the legacy environment, the composite experiences 5 hours of downtime for remediation per incident.
- With DSP in place, the composite organization realizes a 90% reduction in downtime for remediation.
- The average hourly salary per affected employee is $36.
- The composite organization has 25 major object- and group-level incidents each year.

90%

Faster object- and group-level remediation

Risks. Object- and group-level remediation savings may vary depending on the following:

- The number of employees affected per major object- or group-level incidents. Forrester assumes that 1% of the composite organization's employees are affected in each incident based on interviews; however, this may differ across organizations based on factors such as IT infrastructure complexity and scale, security posture, and access control policies.
- The downtime an organization experiences for major group- and object-level incidents prior to the Semperis investment.
- The average hourly salary per affected employee.
- The number of major object- or group-level incidents per year.

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 $4.3 million.

Object- And Group-Level Remediation Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Employees affected per major object- or group-level incident	A1*1%	500	500	500
C2	Downtime for objects to be restored before Semperis (hours)	Interviews	5	5	5
C3	Reduction in downtime due to remediation of objects after Semperis	Interviews	90%	90%	90%
C4	Downtime due to remediation of objects after Semperis (hours)	C2(1-C3)	0.5	0.5	0.5
C5	Average hourly salary per affected employee (rounded)	TEI standard	$36	$36	$36
C6	Cost of downtime per incident before Semperis	C1*C2*C5	$90,000	$90,000	$90,000
C7	Number of major object- or group-level incidents per year	Interviews	25	25	25
C8	Annual cost of downtime due to object- or group-level remediation before Semperis	C6*C7	$2,250,000	$2,250,000	$2,250,000
Ct	Object- and group-level remediation savings	C3*C8	$2,025,000	$2,025,000	$2,025,000
	Risk adjustment	↓15%			
Ctr	Object- and group-level remediation savings (risk-adjusted)		$1,721,250	$1,721,250	$1,721,250
	Three-year total: $5,163,750		**Three-year present value: $4,280,494**		

Hybrid AD Environment Monitoring Efficiencies

Evidence and data. Interviewees reported significant IT team time savings on monitoring AD and Entra ID environments with Semperis' DSP tool. With real-time alerting, IT teams were immediately notified of any suspicious or unauthorized changes in hybrid AD environments to promptly address the potential incident rather than conducting manual investigation to locate possible threats. The interviewees noted their organizations realized additional efficiencies from DSP's automation capabilities, such as automated rollback of malicious changes, which detected potential issues and took predefined corrective actions without intervention from IT team members. DSP's continuous monitoring helped the interviewees' organizations identify and address identity security indicators to close gaps and prevent AD- and Entra ID-related attacks.

- The senior manager of server architecture in energy said that their IT access team spent 40% to 50% less time monitoring their hybrid AD environment after investing in DSP. The senior manager said: "Our IT teams' workload has reduced with Semperis. Typically, we would have to dig through logs to search for things

in the environment. Now, we get automatic alerts for issues, which reduces the time spent on monitoring. We also get automated emails that our data is properly backed up and that our AD environment is solid. Semperis has given us peace of mind."

They concluded: "Changes to objects and groups in our Active Directory took a toll on our IT access team before DSP. They would have to spend a lot of time figuring out the root cause of the problem. Now, they can easily look at the changes to know what was done, who did it, and quickly remediate the issue."

- The manager in identity management and engineering explained how automation with DSP has enabled efficiencies across their IT teams: "Our IT teams have seen a lot of efficiencies since we've invested in DSP. We're able to block and even roll back unauthorized changes immediately. Unless changes are a request chain that has been approved, they cannot occur unless channeled appropriately."
- The CISO in healthcare said: "[DSP] is a solution that is actively watching our Active Directory environment on our behalf. In many ways, it allows us to set it and forget it. It protects our IT teams from having to wear multiple hats and allows them to focus on other things."
- The network systems analyst in healthcare said: "I get email notifications from DSP every morning with a summary of what's happening in the AD environment. If there is a red 'x,' we have to go in and make adjustments. Otherwise, if everything appears green, I know that the environment doesn't need any issues addressed. The ease of monitoring is huge. It makes it a lot easier to be able to review highlights first thing in the morning and just continue with my day."

> "[DSP] is a solution that is actively watching our Active Directory environment on our behalf. In many ways, it allows us to set it and forget it. It protects our IT teams from having to wear multiple hats and allows them to focus on other things."
>
> CISO, HEALTHCARE

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

- The composite organization has six IT FTEs that spend 25% of their time monitoring the hybrid AD environment.
- After investing in Semperis, the composite's IT FTEs realize a 40% reduction in time spent monitoring the hybrid AD environment, entirely freeing up one to two FTEs to work on other critical tasks.
- The average fully burdened annual salary of an IT FTE is $108,160.
- Since not all time saved is used for additional work, Forrester applies a 75% productivity recapture to the time saved with Semperis to remain conservative.

40%

Reduction in time spent monitoring the hybrid AD environment

Risks. Hybrid AD environment monitoring efficiencies may vary depending on the following:

- The number of IT FTEs involved in continuous monitoring of the hybrid AD environment.
- The percentage of time IT FTEs spend monitoring the hybrid AD environment.
- The average fully burdened annual salary of an IT FTE.
- The percentage of productivity recaptured for value-added activities.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $109,000.

Hybrid AD Environment Monitoring Efficiencies					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	IT FTEs involved in continuous monitoring of hybrid AD environment	Interviews	6	6	6
D2	Percentage of time spent monitoring hybrid AD environment before Semperis	Interviews	25%	25%	25%
D3	Percent reduction in time spent on monitoring the hybrid AD environment with Semperis	Interviews	40%	40%	40%
D4	Average fully burdened annual salary of an IT FTE	TEI standard	$108,160	$108,160	$108,160
D5	Productivity recapture	TEI standard	75%	75%	75%
Dt	Hybrid AD environment monitoring efficiencies	D1*D2*D3*D4*D5	$48,672	$48,672	$48,672
	Risk adjustment	↓10%			
Dtr	Hybrid AD environment monitoring efficiencies (risk-adjusted)		$43,805	$43,805	$43,805
	Three-year total: $131,414			**Three-year present value: $108,936**	

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Improved brand credibility.** After investing in Semperis, interviewees noted their organizations achieved a more resilient hybrid AD environment that offered a higher degree of data integrity guided by identity security experts with hands-on

experience in incident response through Semperis' breach preparedness and response services. With real-time monitoring, the interviewees' organizations realized heightened visibility and were thus able to promptly detect and respond to potential threats before they evolved into a large-scale attack. This overall improvement in security posture reinforced a positive brand image, bolstering interviewees' organizations' reputations among customers and unlocking new opportunities for business growth.

The CISO in healthcare outlined the importance of maintaining credibility in an industry that handles highly sensitive data: "The reality of healthcare is that we know our patients can choose to go elsewhere. We want them to have every confidence that we're doing everything we can to protect them and care for them and their information."

The CISO continued: "Because we deal with so much personal identifying information in our industry, we're a prime target for a breach attack and theft of patient information. This creates a lot of fear for consumers as a healthcare organization. Part of our culture is making sure they feel safe."

The technical architect of AD said: "The danger of having an AD attack is not just about a loss in revenue. We are chiefly concerned with how it impacts our reputation as an organization."

- **Improved visibility of hybrid AD environment.** Through improved visibility into their hybrid AD environment, interviewees' organizations gained instant access to valuable insights into user behaviors, facilitating proactive identification of potential risks. With a clearer view of AD and Entra ID changes and configurations, the interviewees' organizations streamlined remediation processes to minimize downtime and maintain business continuity. Interviewees reported that their organizations ultimately established greater environmental resiliency, minimizing the overall identity attack surface.

  The SVP in financial services said: "With Semperis, we went from zero visibility to full visibility. It's a huge leap. We now understand what we previously were unaware of within our environment. That's massive for us."

  Interviewees' organizations with hybrid identity environments specifically noted that, as their attack surfaces continued to expand, attacks that may start on-premises could move to the cloud. With Semperis, interviewees noted their

organizations were able to see across multiple identity environments to make critical connections to threats that may otherwise have been missed due to siloed data and tools. They also said that continuous monitoring of the hybrid AD environment helped their organizations identify and address hybrid environment security vulnerabilities with security indicators for on-premises AD and Entra ID. Semperis empowered their organizations with a complete picture of exposures across their hybrid AD environment.

> "The ability to provide our patients with confidence in the services that we provide is critical. We need them to know that we're doing the right things to protect their data. It's all about trying to make sure we're doing the right thing for the customer always."
>
> CISO, HEALTHCARE

FLEXIBILITY

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

- **Maintaining a strong security posture as business grows.** Interviewees said that the Semperis investment has provided a secure foundation for sustained business growth. By being able to adapt to evolving cybersecurity challenges, their organizations were able to scale their hybrid AD environments securely without compromising their overall security posture or violating industry compliance standards. Achieving a more resilient infrastructure with products purpose-built by identity security experts for comprehensive cyber resilience

allowed the interviewees' organizations to mitigate vulnerabilities that inevitably arose as the potential surface area of an attack increased.

The CISO in healthcare described how Semperis enabled a unified AD environment across existing and new business segments: "We just completed our initial rollout as part of a recent expansion within our footprint. [Semperis allowed] these new segments of our business to level-set their AD environment within the larger organization."

They continued: "Employees in the new segments told us that their previous solution was strictly a backup and wasn't even making sure the backup was fully clean and free of malware. Semperis is doing what their previous tool was doing, plus 1,000%. They immediately got rid of their incumbent vendor and could not get the paperwork done quick enough — that's how much they wanted Semperis."

The senior manager of server architecture in energy discussed their plans to leverage Semperis to maintain resiliency as their organization continued to grow its AD environment: "We are looking at expanding our footprint with Semperis in the coming year to include four additional domain controllers. There's a lot of segmentation we have to do inside our environment to keep operations and our pipeline systems separated, which will require more domains for our base environment. We plan to use Semperis as a standard tool across all of these environments."

The senior manager continued: "We are using Semperis as part of our strategy to make sure [an AD attack] never happens. We want to create an air-tight environment, and Semperis is the tool that we're currently using to take our backups and move them into a unified, protected environment."

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

> “In the healthcare space, it’s a constant daily battle. Having a strong security posture is top of mind. We have to stay ahead and get it right 100% of the time, whereas those bad actors only have to be right once.”
>
> CISO, HEALTHCARE.

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 vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

Total Economic Impact Approach

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

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

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."

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 period

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

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.

APPENDIX C: ENDNOTES

[1] Source: "2022 Trends in Security Digital Identities," Identity Defined Security Alliance (IDSA), 2022; Forrester's Security Survey, 2023.

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

FORRESTER®