UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

CONGRUENT MEDIA RESOURCING LLC, Plaintiff, v. **SILVERFORT, INC.,** Defendant.	C.A. No. 2:26-cv-00643 **JURY TRIAL DEMANDED** **PATENT CASE**

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Congruent Media Resourcing LLC files this Original Complaint for Patent Infringement against Silverfort, Inc. and would respectfully show the Court as follows:

I. THE PARTIES

1. Plaintiff Congruent Media Resourcing LLC ("Plaintiff") is a Texas limited liability company with a principal place of business located at 5900 Balcones Drive, Suite 100, Austin, Texas 78731.

2. On information and belief, Defendant Silverfort, Inc. ("Defendant"), is a corporation organized and existing under the laws of Delaware with its U.S. headquarters at 5525 Granite Parkway, Plano, Texas, 75024. Defendant has a registered agent Corporation Service Company at 211 E. 7th Street, Suite 620, Austin, Texas 78701.

II. JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction of such action under 28 U.S.C. §§ 1331 and 1338(a).

4. On information and belief, Defendant is subject to this Court's specific and general personal jurisdiction, pursuant to due process and the Texas Long-Arm Statute, due at least to its business in this forum, including at least a portion of the infringements alleged herein. Furthermore, Defendant is subject to this Court's specific and general personal jurisdiction because Defendant maintains a place of business at 5525 Granite Parkway, Plano, Texas, 75024.

5. Without limitation, on information and belief, within this state and this District, Defendant has used the patented inventions thereby committing, and continuing to commit, acts of patent infringement alleged herein. In addition, on information and belief, Defendant has derived revenues from its infringing acts occurring within Texas and this District. Further, on information and belief, Defendant is subject to the Court's general jurisdiction, including from regularly doing or soliciting business, engaging in other persistent courses of conduct, and deriving substantial revenue from services provided to persons or entities in Texas and this District. Further, on information and belief, Defendant is subject to the Court's personal jurisdiction at least due to its providing services within Texas and this District. Defendant has committed such purposeful acts and/or transactions in Texas and this District such that it reasonably should know and expect that it could be haled into this Court as a consequence of such activity.

6. Venue is proper in this district under 28 U.S.C. § 1400(b). On information and belief, Defendant maintains a place of business at 5525 Granite Parkway, Plano, Texas, 75024. On information and belief, from and within this District Defendant has committed at least a portion of the infringements at issue in this case.

7. For these reasons, personal jurisdiction exists and venue is proper in this Court under 28 U.S.C. § 1400(b).

III. UNITED STATES PATENT NO. 9,135,418

8. Plaintiff incorporates the above paragraphs herein by reference.

9. On September 15, 2015, United States Patent No. 9,135,418 ("the '418 Patent") was duly and legally issued by the United States Patent and Trademark Office. The '418 Patent is titled "System and Method for Creating Secure Applications." A true and correct copy of the '418 Patent is attached hereto as Exhibit 1 and incorporated herein by reference.

10. Congruent Media Resourcing LLC is the assignee of all right, title, and interest in the '418 patent, including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the '418 Patent. Accordingly, Congruent Media Resourcing LLC possesses the exclusive right and standing to prosecute the present action for infringement of the '418 Patent by Defendant.

11. The invention in the '418 Patent relates to systems and methods for creating secure workspaces and applications, including the management and enhancement of same. (Ex. 1 at 1:16-19). The goal of the '418 Patent is to reduce security breaches by creating secure workspaces and applications. (*Id.* at 1:16-38). To do this, the '418 Patent discloses imposing functions, such as intercepts, that convert an unsecured target application to a secure application. (*Id.* at 1:54-57). These functions may be considered as an actual replacement of existing instruction or a new instruction that may interrupt program flow and conditionally return control to the program flow. (*Id.* at 1:66-2:3). By adding these functions, the behavior of the secure application can be different from the original behavior of the target application. (*Id.* at 1:57-61). The '418 Patent explains that when these functions are added to the targeted application, the now secure application can be repackaged with the additional functions integrated with the original file. (*Id.* at 2:4-6).

12. The '418 patent provides details regarding how application securitization occurs. Specifically, it discloses that one way application wrapping may occur is via an automated process in which no source code is modified, thereby reducing programmer oversight and errors. (*Id.* at

12:19-26). Additionally, the '418 patent provides examples of this, including 1) replacing references to system services with references to a library that applies the necessary mechanisms and policies and 2) inserting secure references into the code of an application to replace non secure references. (*Id.* at 12:24-35). Specifically, this securitization process may include interposing system API calls to allow a secure framework to intercept and control application functions. (*Id.* at 21:43-49). This process may further include encryption for additional protection of applications. (*Id.* at 21:49-58). One major benefit may be that management layers may be injected onto the compiled applications, removing the need for source code or developer implemented application changes. (*Id.* at 12:36-47).

13. The '418 patent also discloses technical examples of the use of securing applications via an intercept. One example method is called byte code injection, which replacing byte code API calls with intercepts. (*Id.* at 22:45-51). This is particularly useful for applications formatted for the Android operating system. (*Id.*; *also* Figure 11; 23:45-60). Another disclosed technical method is to link replacement calls for native object code. (*Id.* at 22:51-57). This method is useful for applications that use native code and do not run under a virtual machine. (*Id.*). An example of this type of injection is link injection, which replaces preexisting system calls or the inclusion of new instructions in an immutable entity. (*Id.* at 24:64-25:24). The '418 Patent further discloses that linking order may be statically or dynamically linked, and that priority can be established during runtime. (*Id.* at 25:6-17). Finally, a system of obfuscation may prevent further modification or reversal of the securitization process. (*Id.* at 25:15-17).

14. The '418 patent further discusses the technical benefits of repackaging the target application during a reconstruction phase. (*Id.* at 24:3-21). This is performed by a repackager. (*Id.* at 3-7). The repackager may be made of software or hardware elements and may be further

modified by secure object references injected before. (*Id.* at 24:7-9). In addition, this reconstructed and modified application may need a new certificate to be trusted. (*Id.* at 24:11-16).

Asserted Claim

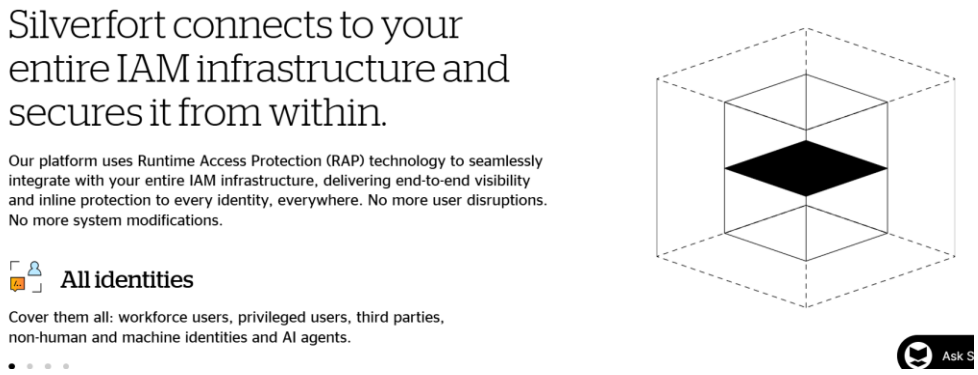
15. Claim 1 of the '418 Patent claims:

> A method of operating a secure application, comprising:
>
> receiving a request to activate the secure application through an input device, wherein the secure application was created from a target application having a first set of functions associated with a first application behavior and the secure application has a second set of functions that are imposed on the first set of functions and that are associated with a second application behavior:
>
> in response to the receipt of the request, forcing the secure application to override the first application behavior with the second application behavior, wherein the second application behavior takes priority over the first application behavior; and
>
> via a processing unit, performing the second application behavior.

IV. COUNT I
(PATENT INFRINGEMENT OF UNITED STATES PATENT NO. 9,135,418)

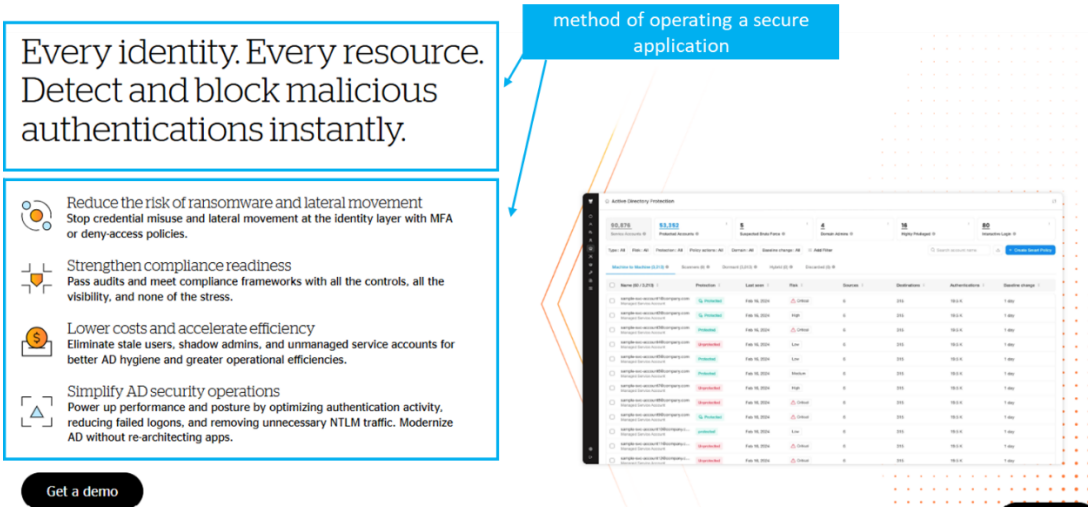
16. Upon information and belief, Defendant has directly infringed claim 1 of the '418 Patent in Texas, in this District, and elsewhere in the United States, by using and performing the claimed method by using the Silverfort Identity Security Platform ("Accused Instrumentality").

17. **Direct Infringement**. As explained below, Silverfort's Identity Security Platform comprises a method of operating a secure application. Silverfort's Identity Security Platform integrates with a user's identity management architecture to provide inline protection to each identity. Identities may include users, third parties, non-human identities, and AI agents. Silverfort's Identity Security Platform is built to provide identity security with a focus on runtime protection. Silverfort's Identity Security Platform provides an identity security solution by reducing ransomware and lateral movement, strengthening compliance readiness, and optimizing authentication activity.



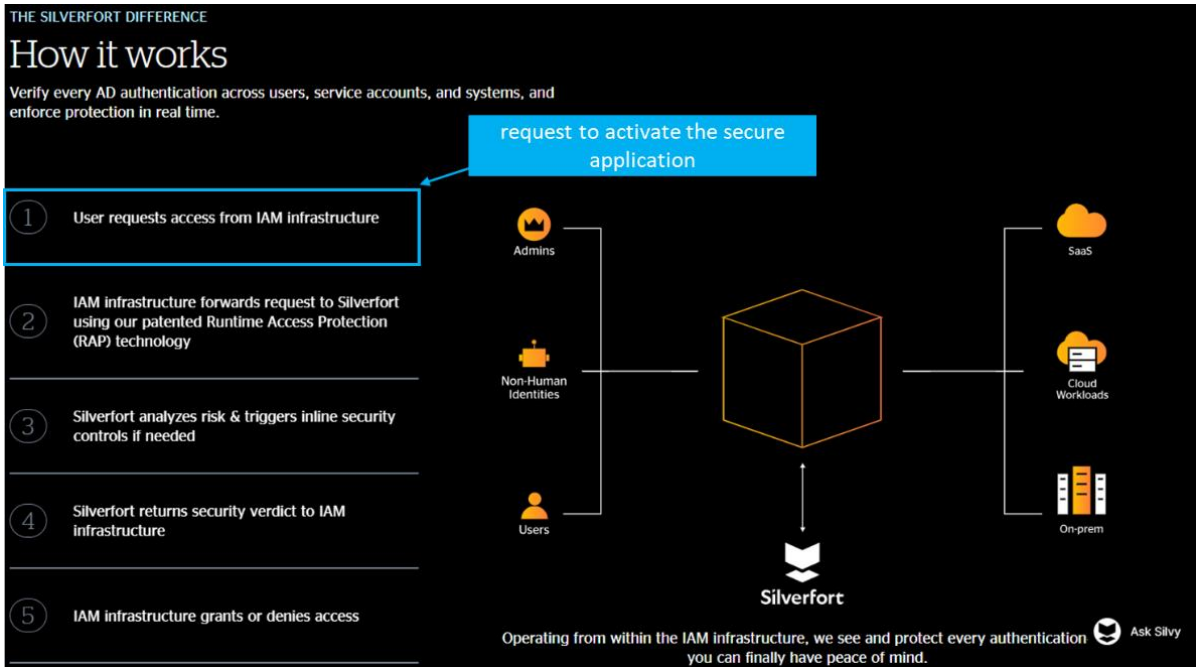
(*E.g.*, https://www.silverfort.com/platform/).

(*E.g.*, https://www.silverfort.com/use-cases/active-directory-protection/).

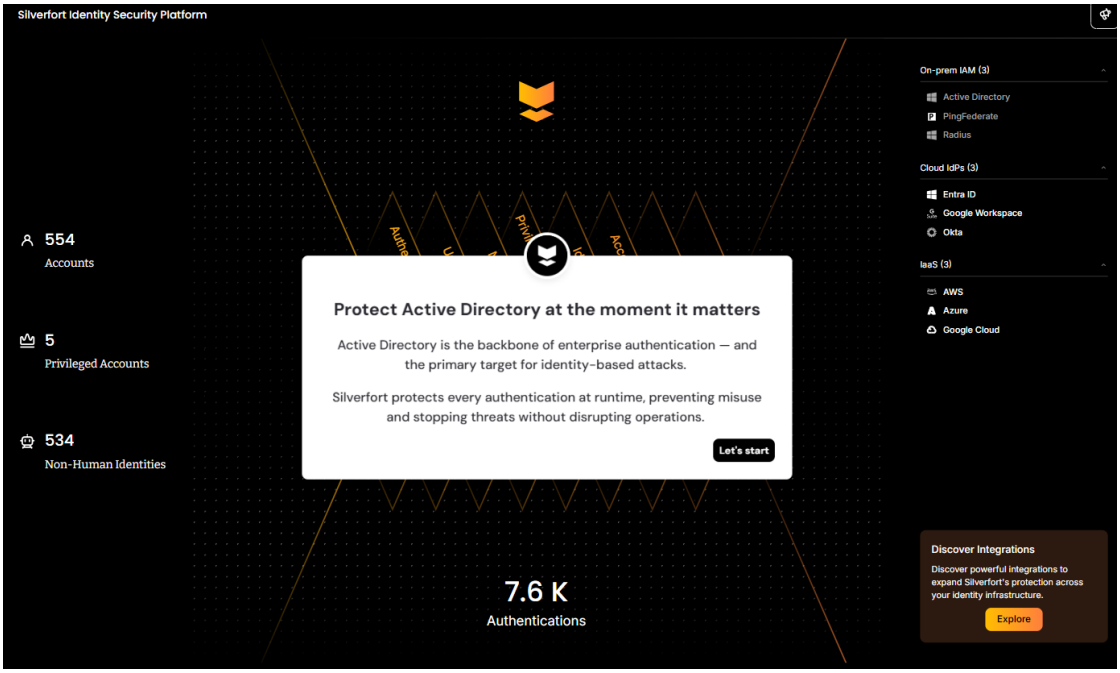


(*E.g.*, https://www.silverfort.com/use-cases/active-directory-protection/).

18. Silverfort's Identity Security Platform practices the step of receiving a request to activate the secure application through an input device, wherein the secure application was created from a target application having a first set of functions associated with a first application behavior and the secure application has a second set of functions that are imposed on the first set of functions and that are associated with a second application behavior. Silverfort's Identity Security Platform prevents misuse and stops threats at runtime without disrupting operations.



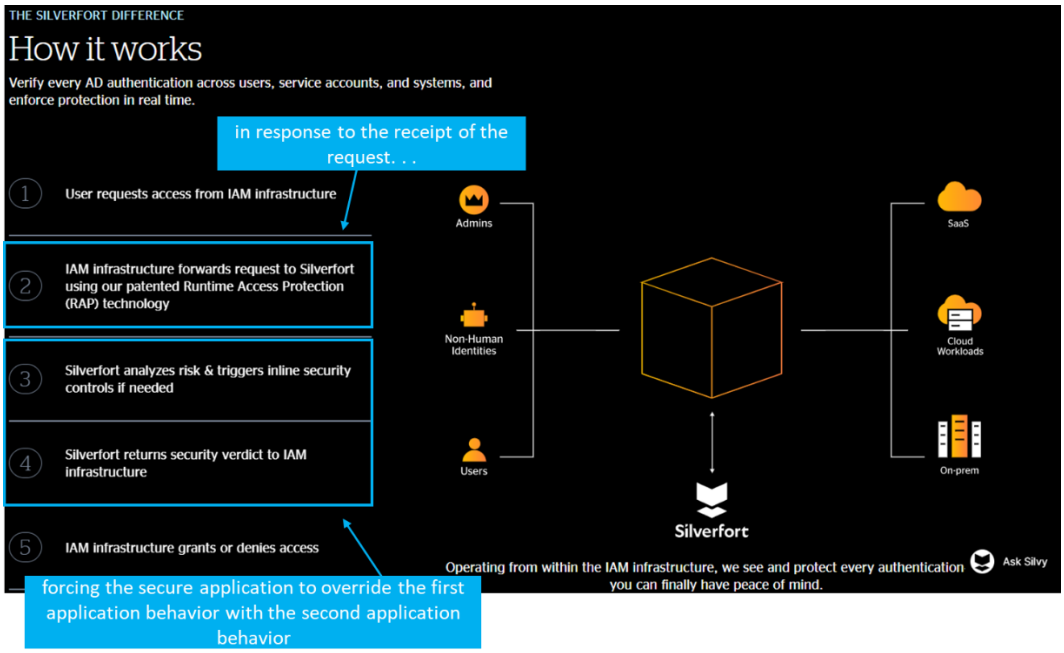
(*E.g.*, https://www.silverfort.com/use-cases/active-directory-protection/).



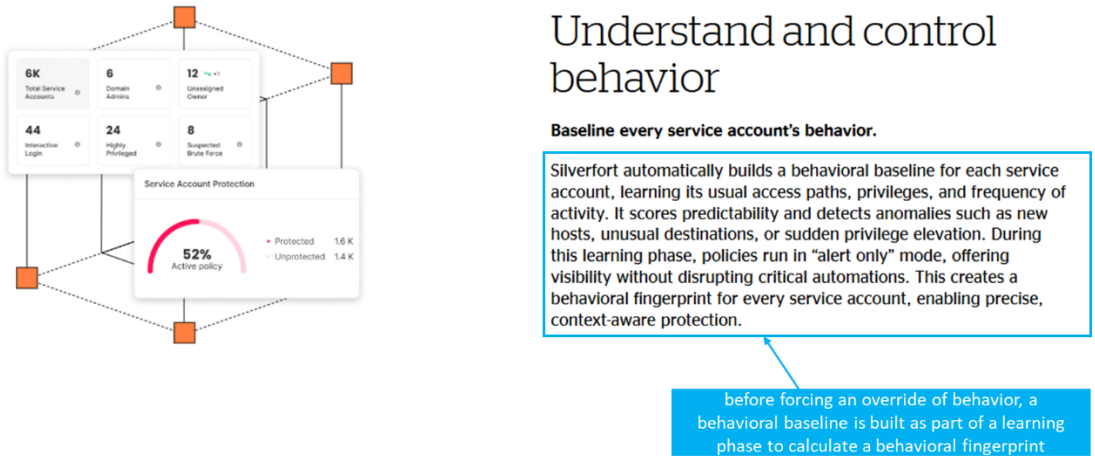
(*E.g.*, https://demo-w1.silverfort.com/player?demoId=65f03d39-c138-45ce-9209-d235d123d4b5&screenId=ec636009-c913-4a28-9bb0-bbb606d3bf38&showGuide=true&showGuidesToolbar=true&showHotspots=true&openGuidesToolbar=false&_gl=1*p9xcig*_gcl_au*MTY1MjE0NjE1Ny4xNzc2ODE1NTgy*_ga*MTE0Nzg5ODU0My4xNzc2ODE1NTgy*_ga_4052YMBRRZ*czE3NzkxMjM5MTEkbzgkZzEkdDE3NzkxMjUxNDMkajEzJGwwJGgw&utm_campaign=41698086-Walnut+Active+Directory+Protection).

19. Silverfort's Identity Security Platform practices the step of, in response to the receipt of the request, forcing the secure application to override the first application behavior with the second application behavior, wherein the second application behavior takes priority over the first application behavior. Silverfort's Identity Security Platform provides an automated response which detects, redacts, blocks, or redirects malicious activity. This is an override of the first application behavior (for instance, by an unsecured agent). In order to determine whether to override first application behavior, Silverfort's Identity Security Platform builds a behavioral baseline, learning usual access patents, privileges, and frequency of activity. Once the Silverfort

Identity Security Platform establishes a baseline, it enforces adaptive policies that permit only expected behavior (allowed behavior) for a service account. The policy will override unexpected behavior with second application behavior (for instance, blocking lateral movement attempts or detected misuse). Silverfort describes the mechanism for overriding a first application behavior (non-secure behavior) with a secure behavior as triggering inline security controls.



(*E.g.*, https://www.silverfort.com/use-cases/active-directory-protection/).



(*E.g.*, https://www.silverfort.com/platform/non-human-identity-security/).

Enforce inline, real-time policies—without breaking automation

Apply virtual fences and adaptive policies to block compromise.

Once baselines mature, Silverfort enforces adaptive policies that lock down activity and permit only expected behavior for each service account. These real-time controls act like virtual fences, automatically blocking abnormal activity—such as unexpected source or destination, or lateral movement attempts—without disrupting legitimate processes. Least Privilege can become dynamic and self-adjusting, keeping automation safe while preventing misuse, ransomware spread, and privilege abuse.

forcing the secure application to override the first application behavior with the second application behavior

(*E.g.*, https://www.silverfort.com/platform/non-human-identity-security/).

A deeper look at Silverfort's innovation: Runtime Access Protection

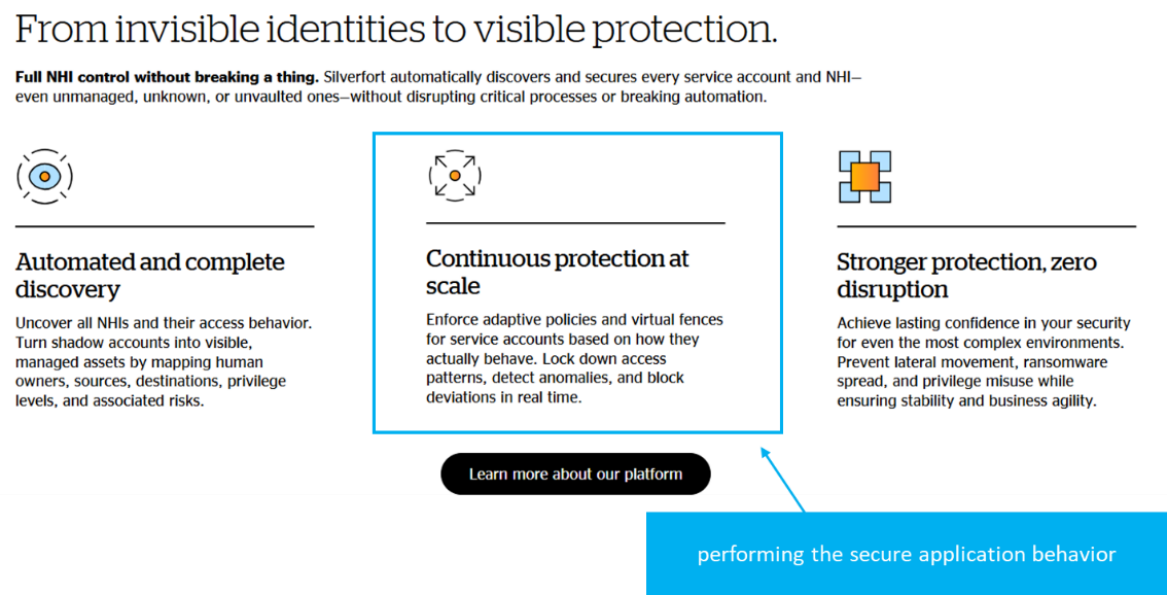
With identity security as Silverfort's sole focus and mission, the company pioneered a way to deliver end-to-end identity security—securing every dimension of identity via its patented technology, Runtime Access Protection (RAP). RAP natively integrates into an enterprise's identity infrastructure to secure it from within. It removes the complexity of securing every identity and extends protection to previously "unprotectable" assets like non-human identities (NHIs), legacy systems, command line tools, IT/OT infrastructure and more. Once integrated into an organization's Identity Access Management (IAM) infrastructure, RAP forwards a user's access request to Silverfort for analysis and triggers inline security controls if needed. Silverfort sends its verdict to the IAM infrastructure to grant or deny access. The result is identity security with end-to-end visibility and active protection—with minimal disruption to users or administrators.

forcing secure application to override first application behavior with second application behavior

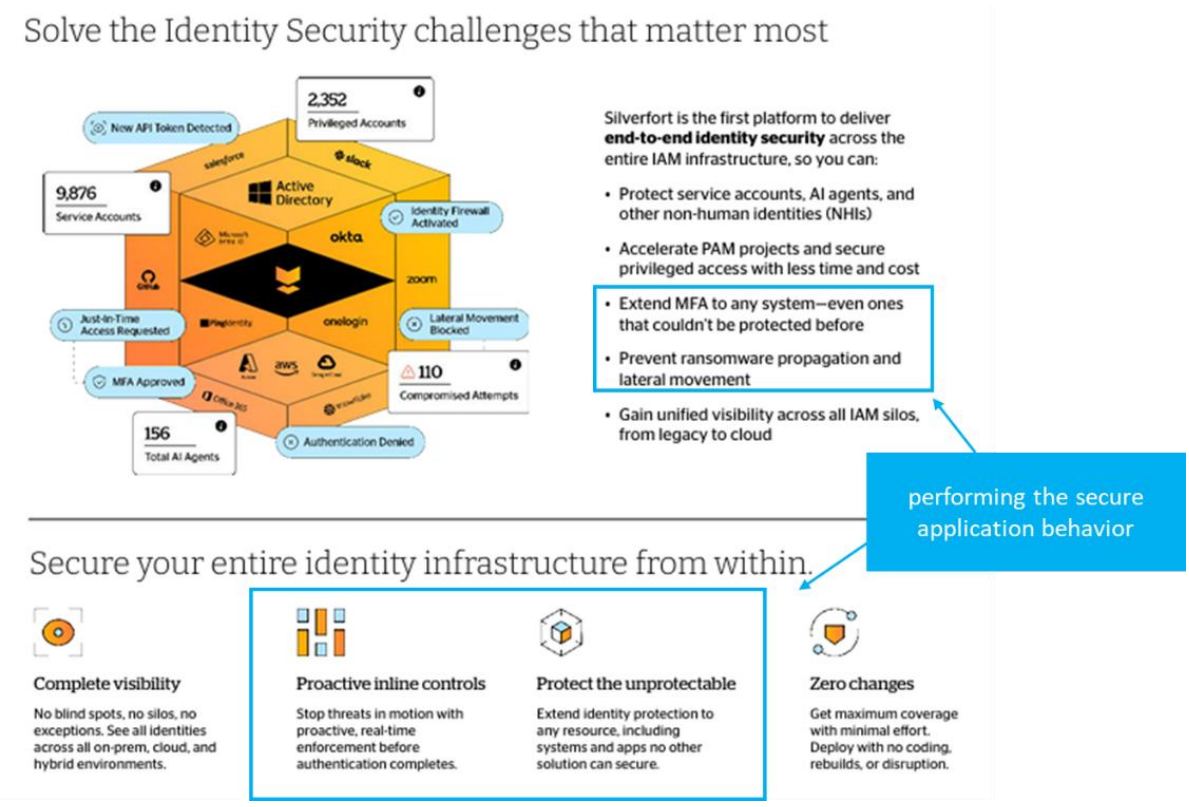
(*E.g.*, https://www.silverfort.com/press-news/silverfort-stakes-its-claim-in-the-identity-security-market-with-patented-architecture-and-rebrand/).

20. Silverfort's Identity Security Platform performs the step of, via a processing unit, performing the second application behavior. Silverfort's Identity Security Platform enforces adaptive policies and virtual fences by locking down access patterns and blocking deviations in real time. This inline solution is used to execute secure application behavior by preventing behavior that exceeds an expected baseline. Silverfort enforces deny and segmentation policies at authentication in order to block unauthorized or risky access before lateral movement occurs.

Silverfort's Identity Security Platform includes a Logs screen which indicates the IDP result in the right hand side. The IPD result indicates when an override occurred as a result of the inline system taking action.



(*E.g.*, https://www.silverfort.com/platform/non-human-identity-security/).



(*E.g.*, https://www.silverfort.com/wp-content/uploads/2025/12/Silverfort-Company-Overview-2025.pdf).

How it works

Silverfort enforces deny and segmentation policies directly at the authentication layer by integrating with Active Directory to analyze and control every access attempt in real time.

Step 1: Connect to Active Directory to gain full visibility
Silverfort integrates natively with AD to monitor all authentication traffic across cloud, on-prem, and hybrid environments. This provides complete visibility into every access request without changing network architecture.

Step 2: Enforce deny and segmentation policies at authentication
Silverfort evaluates every authentication attempt in real time against user identity, behavior, and access context, blocking unauthorized or risky access automatically to stop attackers before they move laterally.

Step 3: Contain active threats immediately
When a breach is detected, Silverfort isolates compromised identities and blocks malicious authentications to prevent further spread and minimize impact.

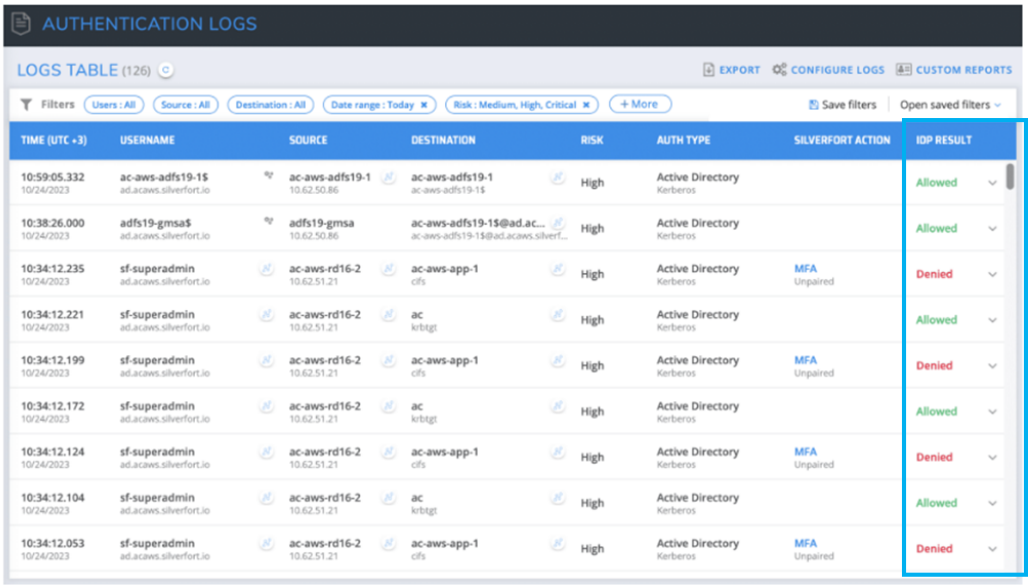
The result: organizations gain real-time control over access and containment, stop identity-based attacks before they spread, and enforce least-privilege access across hybrid environments.

(*E.g.*, https://www.silverfort.com/wp-content/uploads/2025/11/Silverfort-Authentication-Firewall.pdf).

Visibility of User Activity & Authentication

Full User Context

The Silverfort Logs screen provides full visibility into all user logs, authentication activity, and risk indicators. The moment Silverfort is integrated with your IDP, all user accounts are detected, allowing you to monitor their activity and associated risks. As each user is detected, their details are displayed, including username, risk level assigned by Silverfort, authentication type, Silverfort's action, and the IdP result.



Screenshot #1: Silverfort's authentication logs screen

(*E.g.*, https://www.silverfort.com/blog/how-silverfort-empowers-you-to-detect-and-resolve-identity-risks-with-zero-effort/).

21. **Indirect Infringement**. Upon information and belief, Defendant has been and now is indirectly infringing by way of inducing infringement and contributing to the infringement of claim 1 of the '418 Patent in the State of Texas, in this District, and elsewhere in the United States, by providing the Accused Instrumentality for use as described above by Defendant's customers. Defendant advertised, offered for sale, and/or sold the Accused Instrumentality to its customers for use in a manner that Defendant knew infringed claim 1 of the '418 Patent. For example, Defendant provided marketing material and videos advertising that the Accused Instrumentality performs the claimed method of generating a secure application from a target application designed to interact with an operating system as claimed in claim 1 of the '418 Patent. (*Supra* ¶¶17-20 (identifying marketing materials)).

22. On information and belief, since Defendant became aware of the '418 patent and the infringement at least as of the date of the service of the Original Complaint, Defendant is and has been committing the act of inducing infringement by specifically intending to induce infringement by providing the Accused Instrumentality to its customers and by aiding and abetting its use as demonstrated by the marketing materials in a manner known to infringe by Defendant. Since becoming aware of the infringing use of the Accused Instrumentality, Defendant knew that the use of the Accused Instrumentality by its customers as instructed constituted direct patent infringement. Despite this knowledge, Defendant continued to encourage and induce its customers to use the Accused Instrumentality to infringe as described above and provided instructions for using the Accused Instrumentality to infringe, including through instructional materials, support, and user's guides. Exemplary materials are cited above. (*Supra* ¶¶17-20 (identifying marketing

materials)). Defendant therefore knowingly induced infringement and specifically intended to encourage and induce the infringement of the '418 Patent by its customers.

23. On information and belief, since Defendant became aware of the infringement at least as of the date of the service of the Original Complaint, Defendant is and has been committing the act of contributory infringement by intending to provide the identified Accused Instrumentality to its customers knowing that it is a material part of the invention, knowing that its use was made and adapted for infringement of the '418 Patent, and further knowing that the accused use of the Accused Instrumentality is not a staple article or commodity of commerce suitable for substantially non-infringing use. As described above, Defendant was aware that all material claim limitations are satisfied by the use and implementation of the Accused Instrumentality by Defendant's customers in the manner described above yet continued to provide the Accused Instrumentality to its customers knowing that it is a material part of the invention. (*Supra* ¶¶17-20 (identifying marketing materials)). As described above, since learning of the infringement, Defendant knew that the use and implementation of the Accused Instrumentality by its customers was made and adapted for infringement of the '418 Patent. (*Id.*). A new act of direct infringement occurred each time a customer implemented and/or used the Accused Instrumentality in the manner described above. After Defendant became aware that the use of the Accused Instrumentality infringes at least claim 1 of the '418 Patent, Defendant knew that each such new use was made and adapted for infringement of claim 1 of the '418 Patent and Defendant continued to advertise and provide the Accused Instrumentality for such infringing activities. (*Supra* ¶¶17-20 (identifying marketing materials and videos)). Furthermore, as described more fully above, the Accused Instrumentality has functionality designed to perform the steps in the manner described above and is therefore not a staple article or commodity of commerce suitable for substantially non-infringing use. (*Id.*).

24. Plaintiff has been damaged as a result of Defendant's infringing conduct. Defendant is thus liable to Plaintiff for damages in an amount that adequately compensates Plaintiff for such Defendant's infringement of the '418 Patent, *i.e.*, in an amount that by law cannot be less than would constitute a reasonable royalty for the use of the patented technology, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

25. Unless a preliminary and permanent injunction is issued enjoining Defendant and all others acting in active concert therewith from infringing the '418 Patent, Plaintiff will be greatly and irreparably harmed.

26. Plaintiff is only asserting a method claim and as such the marking requirements of 35 U.S.C. 287(a) do not apply. *Crown Packaging Technology, Inc. v. Rexam, Beverage Can Co.*, 559 F.3d 1308, 1316-1317 (Fed. Cir. 2009) ("Because Rexam asserted only the method claims of the '839 patent, the marking requirement of 35 U.S.C. 287(a) does not apply."); *Hanson v. Alpine Valley Ski Area, Inc.*, 718 F.2d 1075, 1083 (Fed.Cir. 1983) ("It is 'settled in the case law that the notice requirement of this statute does not apply where the patent is directed to a process or method." (*Quoting Bandag, Inc. v. Gerrard Tire Co.*, 704 F.2d 1578, 1581 (Fed. Cir. 1983)). Plaintiff has therefore complied with the marking requirements 35 U.S.C. 287(a).

V. JURY DEMAND

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court find in its favor and against Defendant, and that the Court grant Plaintiff the following relief:

a. Judgment that claim 1 of United States Patent No. 9,135,418 has been infringed and is being infringed, either literally and/or under the doctrine of equivalents, directly and/or indirectly, by Defendant;

b. Judgment that Defendant account for and pay to Plaintiff all damages to and costs incurred by Plaintiff because of Defendant's infringing activities and other conduct complained of herein, and an accounting of all infringements and damages not presented at trial;

c. That Defendants be preliminarily and permanently enjoined from any further activity or conduct that infringes;

d. That Plaintiff be granted pre-judgment and post-judgment interest on the damages caused by Defendant's infringing activities and other conduct complained of herein; and

e. That Plaintiff be granted such other and further relief as the Court may deem just and proper under the circumstances.

July 30, 2026

DIRECTION IP LAW

/s/Steven G. Kalberg
David R. Bennett (IL Bar No.: 6244214)
Steven G. Kalberg (IL Bar No.: 6336131)
P.O. Box 14184
Chicago, Illinois 60614-0184
Telephone: (312) 291-1667
dbennett@directionip.com

Attorneys for Plaintiff
Congruent Media Resourcing LLC