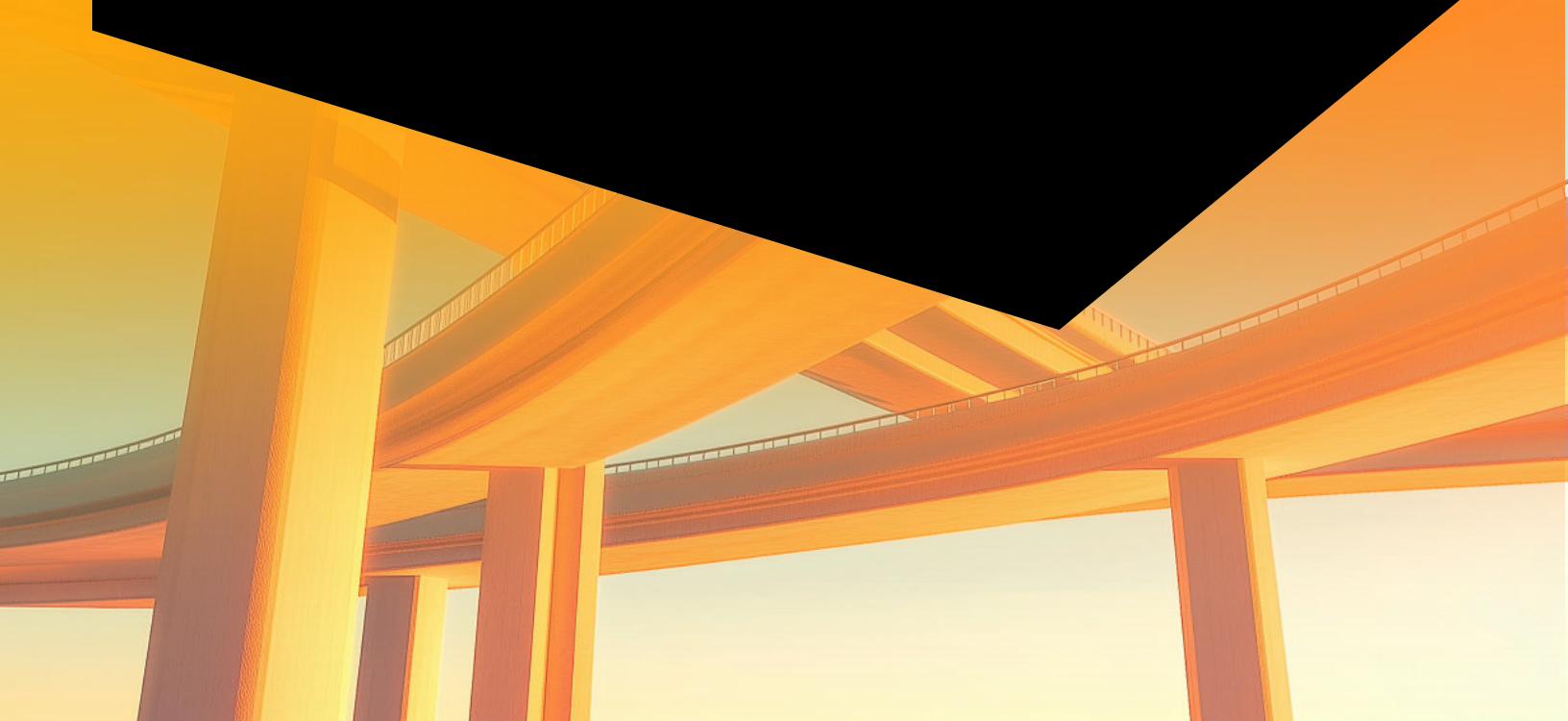
Silverfort

Lateral movement prevention with MFA and service account protection

Case Study



Executive summary

Ransomware attacks fueled by lateral movement have become an operational risk for practically every organization today. Threat actors' standard practice today is to leverage the compromise of the 'patient zero' machine to move within the targeted environment until reaching a point in which they can execute the ransomware payload on mass number of machines simultaneously. As such, lateral movement is now incorporated in more than 80% of ransomware attacks today.

While all verticals are targeted by ransomware attacks, the potential impact on manufacturing companies is significantly more severe, as it a successful attack not only endangers data but actual manufacturing processes. A sound backup plan can ensure that on critical data is lost, but nothing can bring back production time that was lost because of ransomware related shutdown.

This case study describes how a global manufacturing company has partnered with Silverfort to gain real-time protection against such attacks by implementing MFA and Service Account protection policies in its Active Directory environment. Moreover, it also includes a detailed analysis on an occasion in which these policies' strength was put to the ultimate real-life test. This occurred when threat actors have attempted to use compromised credentials of privileged users – both human admins and service accounts – to launch a large-scale lateral movement operation with the purpose of gaining domain dominance.

Silverfort's Identity Security Platform enabled the customer to successfully thwart the large portion of this attack as well as to conduct a rapid and efficient incident response to eradicate all malicious activity and presence from its environment. This illustrates once more the critical role real time protection against identity threats has within organizations' security stack today.

Customer overview

About

The customer is a public global company with manufacturing facilities in eight countries. It provides critical parts that are vital to manufacturing processes in various industries, from building to automotive. Availability and standing up to supply timelines are imperative.

Challenge

The customer's security team has identified a critical weakness in its ability to mitigate attack scenarios that involve threat actors that have already gained initial access to the customer's environment and are using compromised credentials of privileged users to access additional workstations and servers.

Solution

Leverage Silverfort's unique ability to enforce MFA and Block Access on RDP and command-line access (PsExec, PowerShell, etc.) to protect all admin users and high-privileged service accounts. Once these policies were set in place, they would disable attackers' from using the compromised credentials of these users for malicious access.

Why now and key results

Protection against lateral movement: top priority

Based on its analysis of the current threat landscape the customer has come to realize that the ability to detect and block post-compromise lateral movement in its AD environment is imperative to increase its resiliency to ransomware attacks.

Partnering with Silverfort

In 2020 the customer has teamed up with Silverfort to address this issue. Silverfort was chosen due to its ability to extend MFA to all access interfaces admins users employ for administrative access as well as to its ability to discover, monitor and protect service accounts.

MFA policies for admin users

The customer has implemented a multi-layered MFA protection for its admin users all admin users with both rule-based and risk-based policies that cover and proactively prevent the vast majority of lateral movement scenarios.

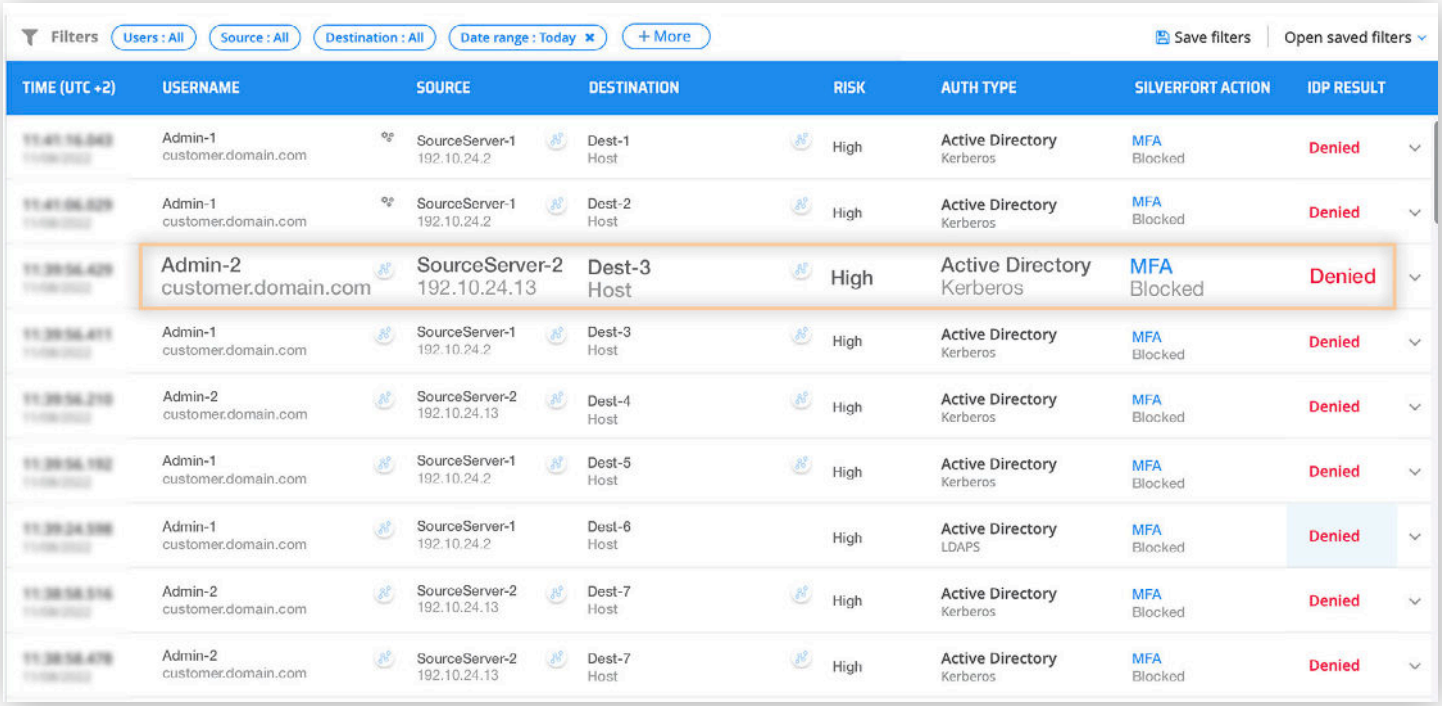
Alert policies for service accounts

The customer leveraged Silverort's platform to discover all its privileged service accounts and enable Silverfort's auto-created policies to trigger a protective action when any of them deviates from its determined behavior. However, the customer chose not to block the service accounts' access when a deviation occurs but rather to alert only.

The attack flow

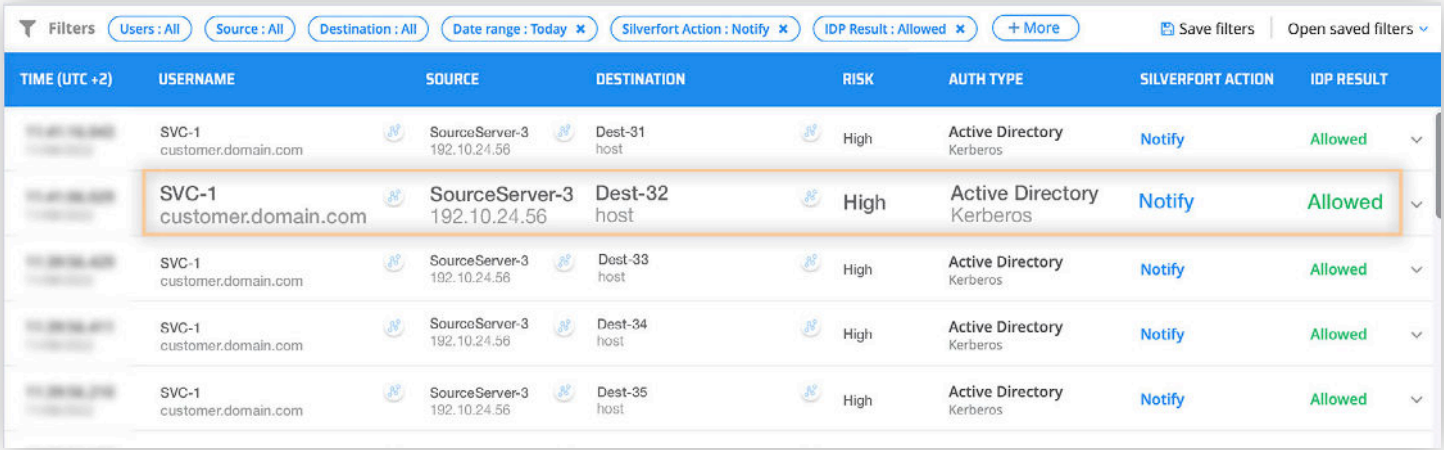
In May 2022 the customer's security teams encountered two security events that called for immediate response:

1. An extremely unusual spike of denied MFA requests from two of its admin users, each originating from a different server, which subsequently have contacted the security team to check why it is happening. We'll call the users Admin-1 and Admin-2m and the source servers SourceServer-1 and SourceServer-2 respectively. Overall access to 13 resources has been attempted using Admin-1 credentials and 9 using Admin-2's.



Screenshot 1: Silverfort's log screen showing attempted lateral movement by Admin-1 and Admin-2 that was blocked by Silverfort's MFA

2. An alert on a high-privileged service account, that was triggered due to multiple interactive logins attempts originating from a source machine this account has never used before. We'll refer to this account as SVC-1.

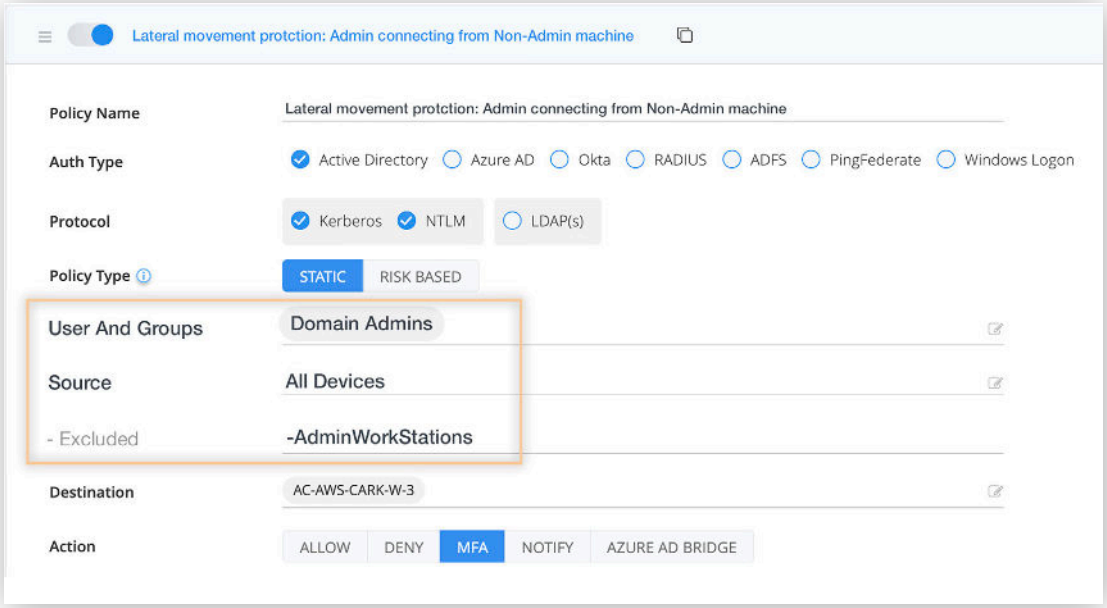


Screenshot 2: Silverfort's log screen showing successful connections by SVC-1 that triggered Silverfort's alert on anomalous service accounts activity.

Let's dive into the following activities the security team has conducted following up on each event.

Denied MFA investigation and response

Quick look at Silverfort's screen revealed that the MFA requests were triggered by the following policy:



Screenshot 3: Silverfort's policy screen showing the MFA policy that prevented the attackers form using the compromised credentials of Admin-1 and Admin-2 for lateral movement.

This policy pre-anticipates a common lateral movement scenario in which threat actors have managed to compromise an admin's credentials. However, in most cases the machine they operate from will not be the admin's own workstation or server. **This makes an admin authentication from a non-admin machine a suspicious enough scenario to require MFA verification** before granting access – as happened in this attack.

Immediate investigation in Silverfort's logs screen showed two attack sources. The access attempts with Admin-1 user account originated from SourceServer-1, while those of Admin-2 were from SourceServer-2.

There was no interconnection between the two servers. However, there were two machines for which access was attempted from both sources. Additionally, one of the machines the attackers attempted to access using Admin-1's account would have enabled them direct access one of the customer's Domain Controller. However, **none of these access attempts was successful and they were all blocked due to the policy in place**.

Diagram 1 shows the attack's attempted path with the compromised credentials of Admin-1 and Admin-2. Notice also the broken gray line that shows the potential risk to the DC.

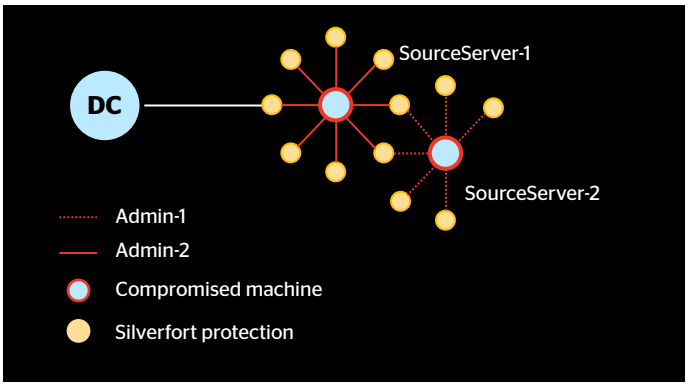


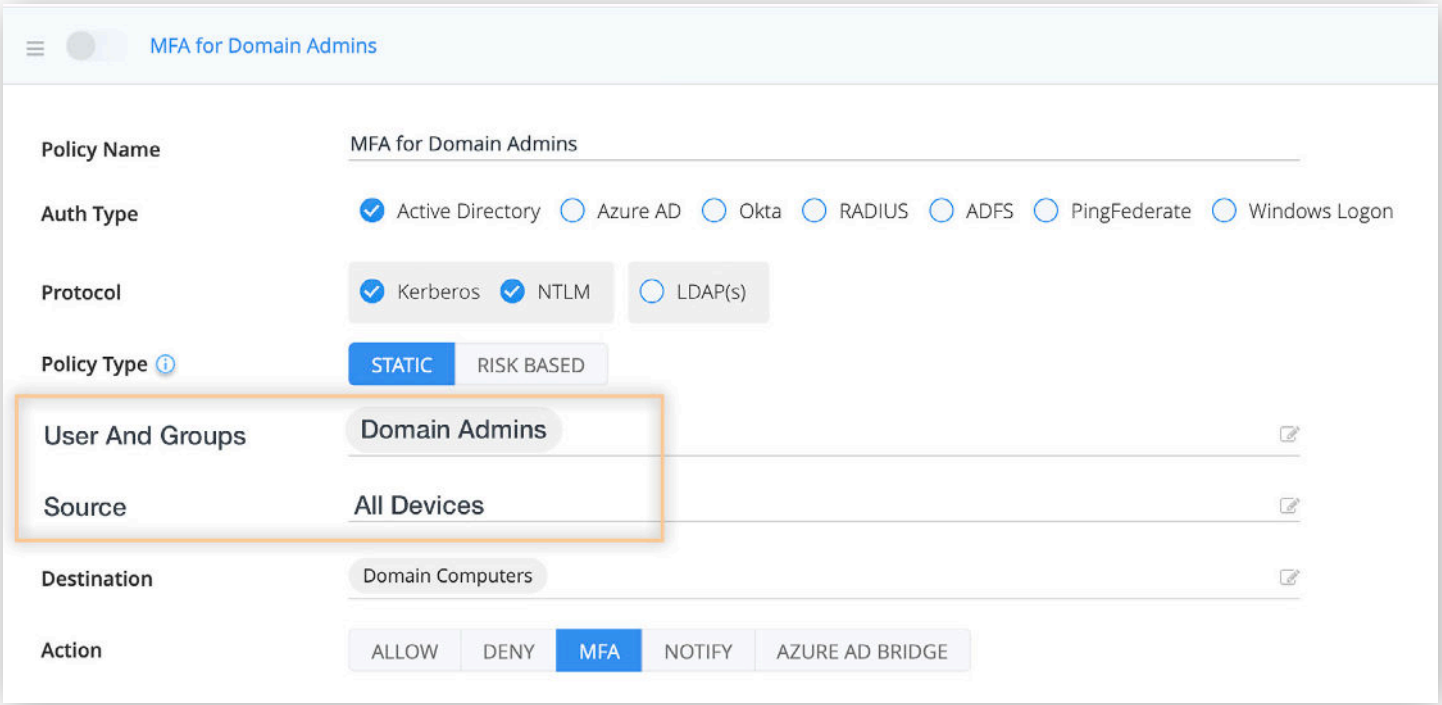
Diagram 1: Attempted lateral movement using Admin-1 and Admin-2 accounts that was blocked by Silverfort's MFA

The access logs haven't revealed any use of malicious modification of the authentication protocol, such as Pass-the-Hash, Pass-the-Ticket, or any others. This implied that the threat actors already had usernames and cleartext credentials before launching the attack.

The two admins' passwords were reset and as a precaution measure, until concluding the investigation and validating that all malicious presence was eradicated, the following steps were taken:

1. All admins were moved to the Protected Users group, mainly to reduce their attack surface by disabling NTLM authentication for these accounts.

2. A more restrictive Silverfort policy was activated to enforce MFA on **any** authentication performed by an admin user, regardless of the source machine and the discovered risk indicators.



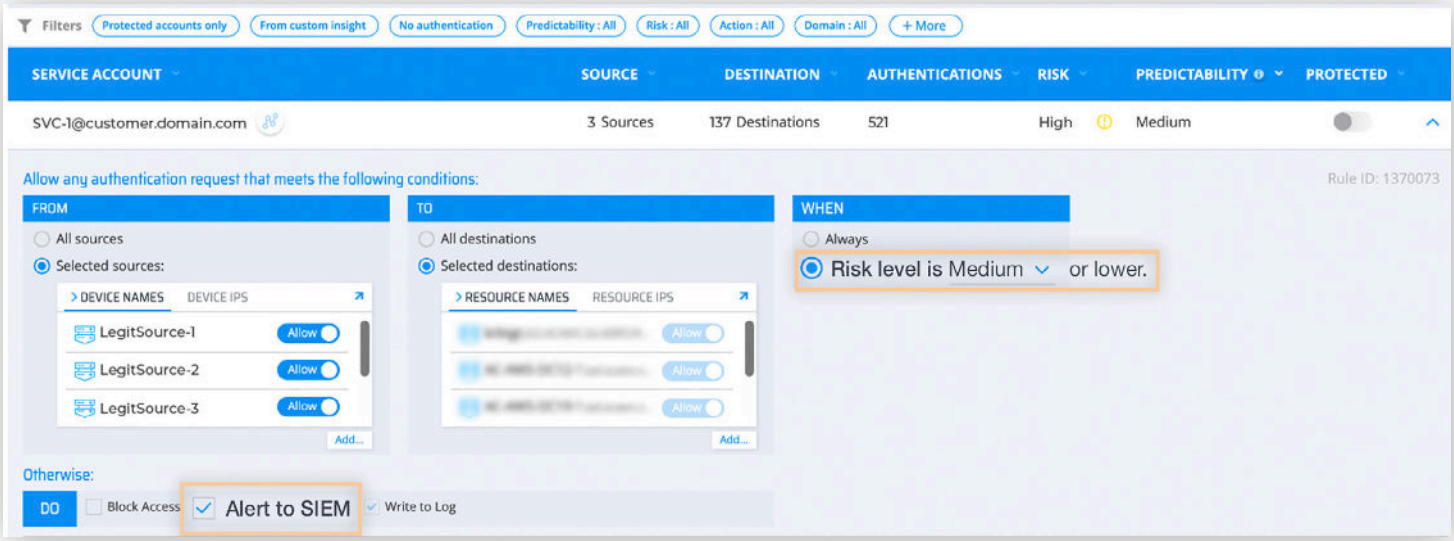
Screenshot 4: Silverfort's policy screen showing the updated policy that enforces MFA on any connection initiated by the customer's admins

Service account anomalous access investigation and response

SVC-1 standard behavior is logging from either one of three defined source machines to multiple workstations and servers in the environment. The policy in place is configured to trigger an alert whenever the two following conditions were met:

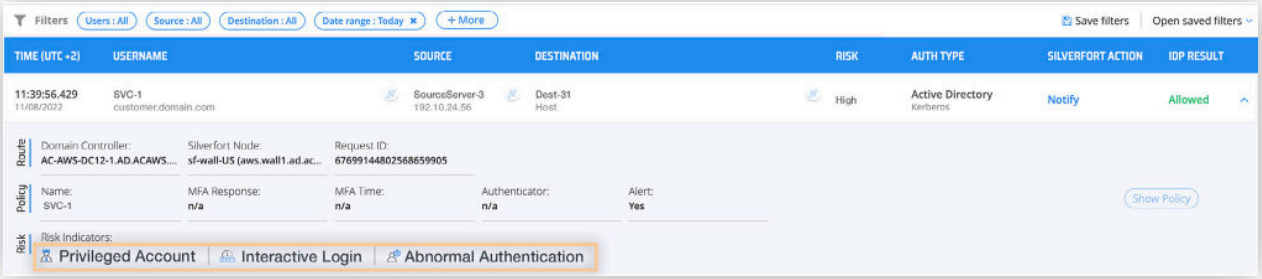
1. Deviation from source or destination machine (in practice it would only be the source machine since the destination encompassed most machines in the environment).

2. Elevation of the account risk level, resulting from its abuse by attackers. An example of such elevation would be when an interactive login would be detected. Since service accounts are used for machine-to-machine communication interactive logins can indicate that a threat actor has compromised the service account's credentials and is now using them for lateral movement.



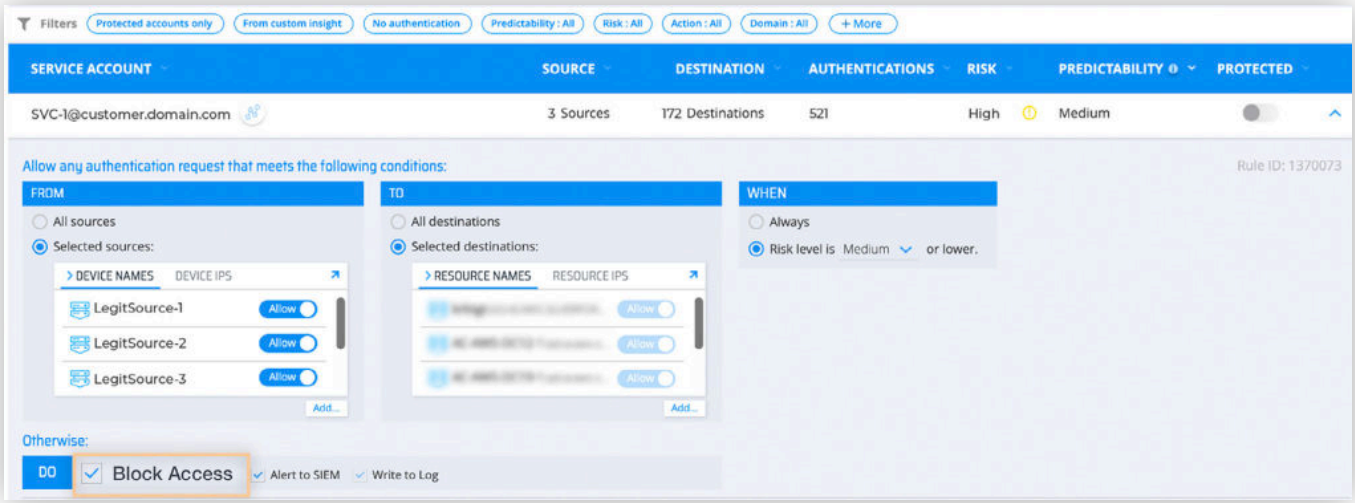
Screenshot 5: Silverfort's service account policy for SVC-1 configured to alert when a deviation from SVC-1's standard behavior occurs

The screenshot below shows a zoom-in on one of the malicious authentications that were accomplished with the compromised SVC-1. Note the three risk indicators on the bottom: Privileged Account, Interactive Login, and Abnormal Authentication.



Screenshot 6: Silverfort's log screen – showing a zoom-in on one of the malicious authentications that were performed with SVC-1

Once the security team noticed the anomalous access attempts SVC-1 performed they have switched the protection action in the policy from 'Alert to SIEM' to 'Block Access'.



Screenshot 7: Silverfort's service account policy screen for SVC-1 updated to block access when a deviation from SVC-1's standard behavior occurs

This policy change has resulted with immediate blocking of 17 consecutive access attempts.

Filters | Users : All | Source : All | Destination : All | Date range : Today | + More | Save filters | Open saved filters

TIME (UTC +2)	USERNAME	SOURCE	DESTINATION	RISK	AUTH TYPE	SILVERFORT ACTION	IDP RESULT
11:41:16.043 11/08/2022	SVC-1 customer.domain.com	SourceServer-3 192.10.24.56	Dest-45 Host	High	Active Directory Kerberos	Deny	Denied
11:41:06.029 11/08/2022	SVC-1 customer.domain.com	SourceServer-3 192.10.24.56	Dest-46 Host	High	Active Directory Kerberos	Deny	Denied
11:39:56.429 11/08/2022	SVC-1 customer.domain.com	SourceServer-3 192.10.24.56	Dest-47 Host	High	Active Directory Kerberos	Deny	Denied
11:39:56.411 11/08/2022	SVC-1 customer.domain.com	SourceServer-3 192.10.24.56	Dest-48 Host	High	Active Directory Kerberos	Deny	Denied
11:39:56.210 11/08/2022	SVC-1 customer.domain.com	SourceServer-3 192.10.24.56	Dest-49 Host	High	Active Directory Kerberos	Deny	Denied
11:39:56.192 11/08/2022	SVC-1 customer.domain.com	SourceServer-3 192.10.24.56	Dest-50 Host	High	Active Directory Kerberos	Deny	Denied
11:39:24.598 11/08/2022	SVC-1 customer.domain.com	SourceServer-3 192.10.24.56	Dest-51 Host	High	Active Directory Kerberos	Deny	Denied

Screenshot 8: Silverfort's log screen showing attempted connections by SVC-1 that were blocked due to the Silverfort's policy change

It should be noted that two of the 17 machines to which the attackers' attempted to access, would have provide them with direct access to one of the customer's Domain Controllers (the same one that could have potentially been accessed with the credentials of Admin-1). Blocking the authentication ensured that the attack was contained prior before the threat actors had any real chance of gaining domain dominance.

Diagram 2 shows the attack's path – the 7 machines for which anomalous access was performed and the 17 ones for which access was blocked following the policy switch. Like the parallel attack we've previously shown, there the route from 2 machine in the second group to the DC is represented in a broken gray line.

All the successful access attempts that took place before switching to 'block access' mode originated from SourceServer-3. Both SourceServer-3 and the machines that the attacker was able to access were quarantined and inspected.

In addition to switching SVC-1's access policy to 'Block Access' mode, its password was reset. Prior to doing that, the customer's identity management team has used Silverfort's dedicated SVC-1 screen to map all its dependencies and update the password in all the scripts that contained an SVC-1 authentication.

The password change has rendered unseccesful the attacker's repeating attempts to access the initial 7 machines. These machines were quarantined and after validating thay they do not feature any malicious presence were connected back to the network.

Moreover, following the attack, the policies for all other privileged service accounts in the environment were changed to 'Block Access' mode as well.

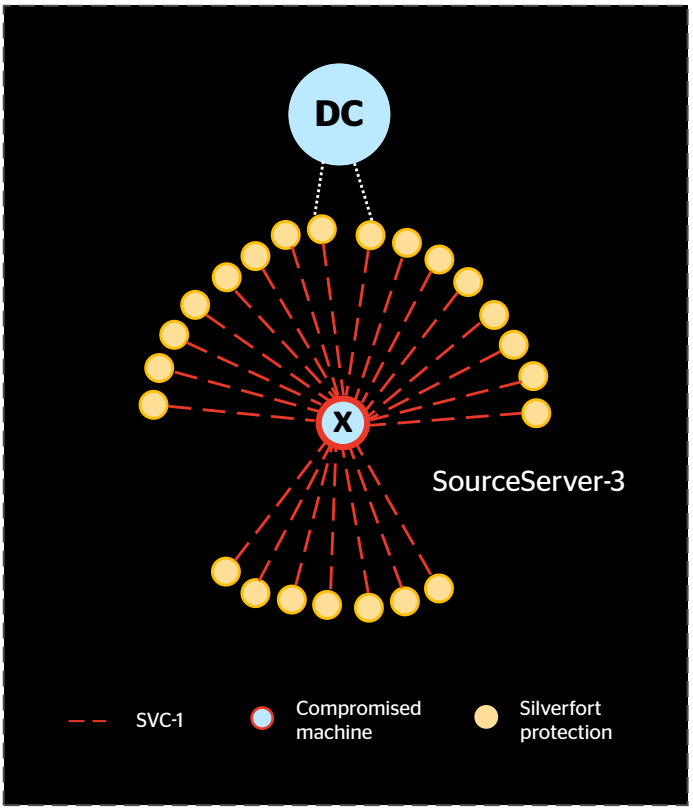


Diagram 2: Attempted lateral movement using SCV-1 account, that initially succeeded but ultimately was blocked by Silverfort's adaptive access policy

Three sources – Single targeted operation

- Examination of the three source servers revealed that all had an active outbound connection to the same attacker. This connection was established by a successful spear phishing attack that used a weaponized email that contained a Word doc with malicious Macros.
- Forensic investigation on the three source servers revealed that the attacker used PsExec to perform the remote connections.
- The lack of any protocol modifications such as Pass-the-Hash, Pass-the-Ticket, etc., indicated that the threat actors had the credentials for the two admins and service account in advance, and didn't rely on compromising credentials within the attack itself. Whether the credentials of these users were obtained by the same threat actor in a preliminary operation is still unclear.
- That way or the other it's clear that the attackers didn't want to waste precious time once inside the customer's network in opportunistic credential hunting but strived to operate as rapidly as possible. It should also be noted that such use of compromised credentials is the hardest to detect since unlike PTH, PTT and others, it fully resembles a legitimate AD authentication.

Three sources – Single targeted operation

The following diagrams shows in the clearest manner the impact of having Silverfort's policies implemented in the customer's environment secured again.

Diagram 3 shows all the malicious authentications Silverfort has blocked. Note that while the attacker has initially succeeded to access 7 machines with the compromised SVC-1 service account, Silverfort's alerting enabled the identity team to act immediately and ensure these machine are secure again.

Diagram 4 shows the potential impact of this attack if Silverfort hadn't been in place. Note that while we've only showed DC as a potential target due to its immediate connection with the attacked machines, the true damage potential was far greater and spans thousands of machines in the customer's environment.

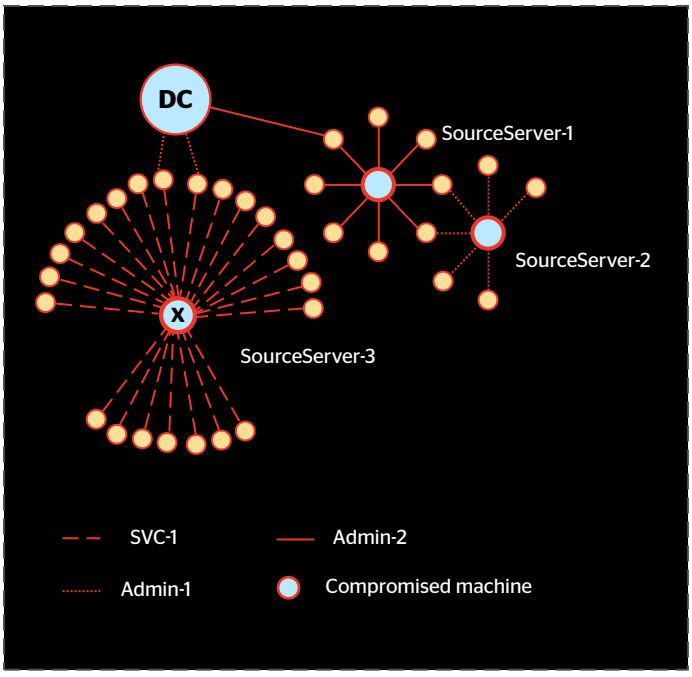


Diagram 4: The full attack layout without Silverfort protection in place

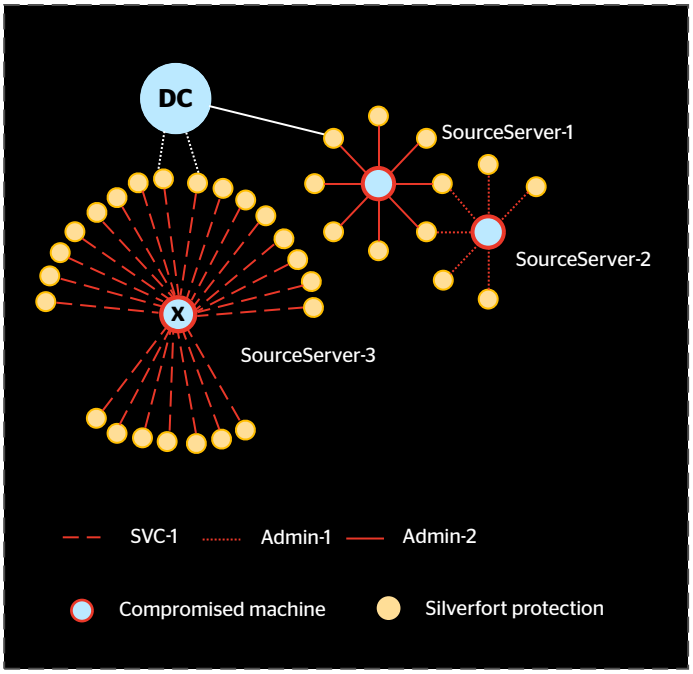


Diagram 3: The full attack layout with Silverfort protection in place

Key insights and conclusions

Real time protection against the use of compromised credentials

What enabled the customer to thwart this attack was the ability to block malicious authentication with compromised user credentials in real time. This is already the standard prerequisite for protecting against malware execution, malicious network traffic or any other adversary activity – the identity attack surface is not different.

Service accounts must have the same level of protection as any privileged user

Attackers go for privileged accounts, regardless of if they are associated with a human user or not. Moreover, they might even prefer utilizing a service account than an actual admin due to the high chances of this account nor being monitored and protected. This calls for security teams to evaluate the protections they have in place and ensure service accounts are not excluded.

Extending protection to command line access is critical

Forensic investigation of the three source servers revealed that the attackers have used PsExec when attempting to access additional machines. Using PsExec and other command line tools for lateral movement is common practice. This is no wonder, because there is no tool in today's security stack that can enforce MFA on them, exposing them to any attacker that obtains compromised user credentials.

MFA is the most cost-efficient protection method

MFA prevents malicious access with zero effort from the security team. In the case described here, the actual protection was a result of the policy in place, rather than of manual effort. This is a huge advantage over any other reactive protection method. In addition, MFA provides the security team with concrete and actionable forensic information on the attacks immediate scope and the entities - users and machines – that should be isolated for investigation.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.

Learn more