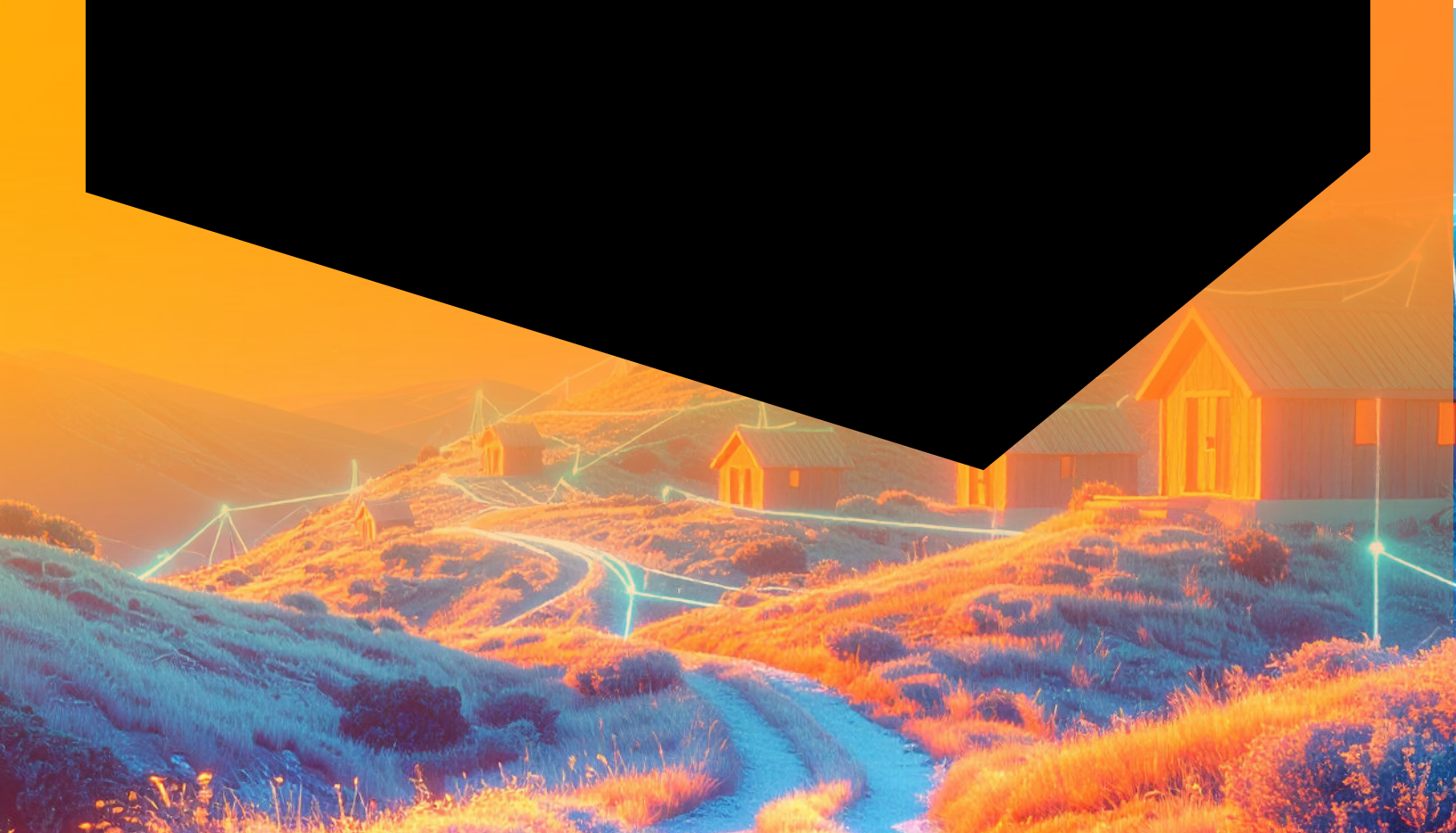
Silverfort

Leading manufacturer prevents lateral movement in a supply chain attack with Silverfort's Identity Security Platform

Case Study



Executive summary

Lateral movement attacks continue to plague global enterprises. In the current threat landscape, compromised credentials are part of the threat actor's arsenal, similar to malware scripts and other attack tools. While the implications of using compromised credentials to gain access to sensitive resources during lateral movement attacks are well known, there are also other methods of attacking enterprises that are becoming more significant, such as exploiting known vulnerabilities, malicious unauthorized access, and malware.

This case study discusses a supply chain cyber incident where a leading manufacturer was attacked by nation-state actors who were attempting to move laterally from a compromised factory network to the manufacturer's domain environment via laptops that were maliciously accessed while several of the company's employees were visiting the factory.

Fortunately, the manufacturer's security team was able to thwart the attack by using Silverfort's capabilities to prevent, detect, and respond to identity threats that use compromised credentials to access targeted resources.

The supply chain attack story will explore the incident from initial access to the lateral movement attempt. In parallel, we'll also show the key role Silverfort took in protecting against the attack — first, by alerting the security team during the credential compromise attempts, and secondly by blocking the lateral movement attempts with an access policy. In analyzing this scenario, we will demonstrate how Silverfort provides organizations in any industry with actionable authentication data and real-time prevention of identity-based attacks. This attempted attack, which is hardly unique, illustrates the critical part that compromised credentials play in today's threat landscape and the importance of having a real-time identity protection solution in place.

Customer overview

About

A multinational discreet manufacturing company, with products designed for both businesses and consumers. In order to manufacture and produce their end-product securely, the company has invested heavily in cybersecurity solutions to ensure all the attack surfaces in their manufacturing plants, products, sensitive resources, and users are secured against cyberattacks.

Challenge

Extend MFA and modern identity security to systems that didn't support it so far, in order to detect and prevent identity threats such as account takeover and lateral movement.

Solution

Deploy Silverfort to gain real-time protection against malicious use of compromised credentials, as well as visibility and risk context of authentications and access attempts to enable alerting and investigations of identity threats.

Why now and key results

Identity protection: a top priority

As one of the world's leading manufacturers in its field, the company has always made security a top priority – especially related to identity-based attacks – by working to protect its employees and critical resources from escalating cyberattacks.

Partnering with Silverfort

In 2017, the company sought a solution that would add a security layer to increase its resilience to various identity threats. They chose Silverfort due to its ability to detect malicious access attempts with its advanced risk engine as well as apply access policies that enforce either MFA or access denial to block them.

Access policies for proactive threat prevention

Today, the company has its entire workforce protected with the Silverfort platform's access policies, ensuring that even in a compromised credentials scenario attackers won't be able to leverage these for malicious resource access.

Alert policies for service accounts

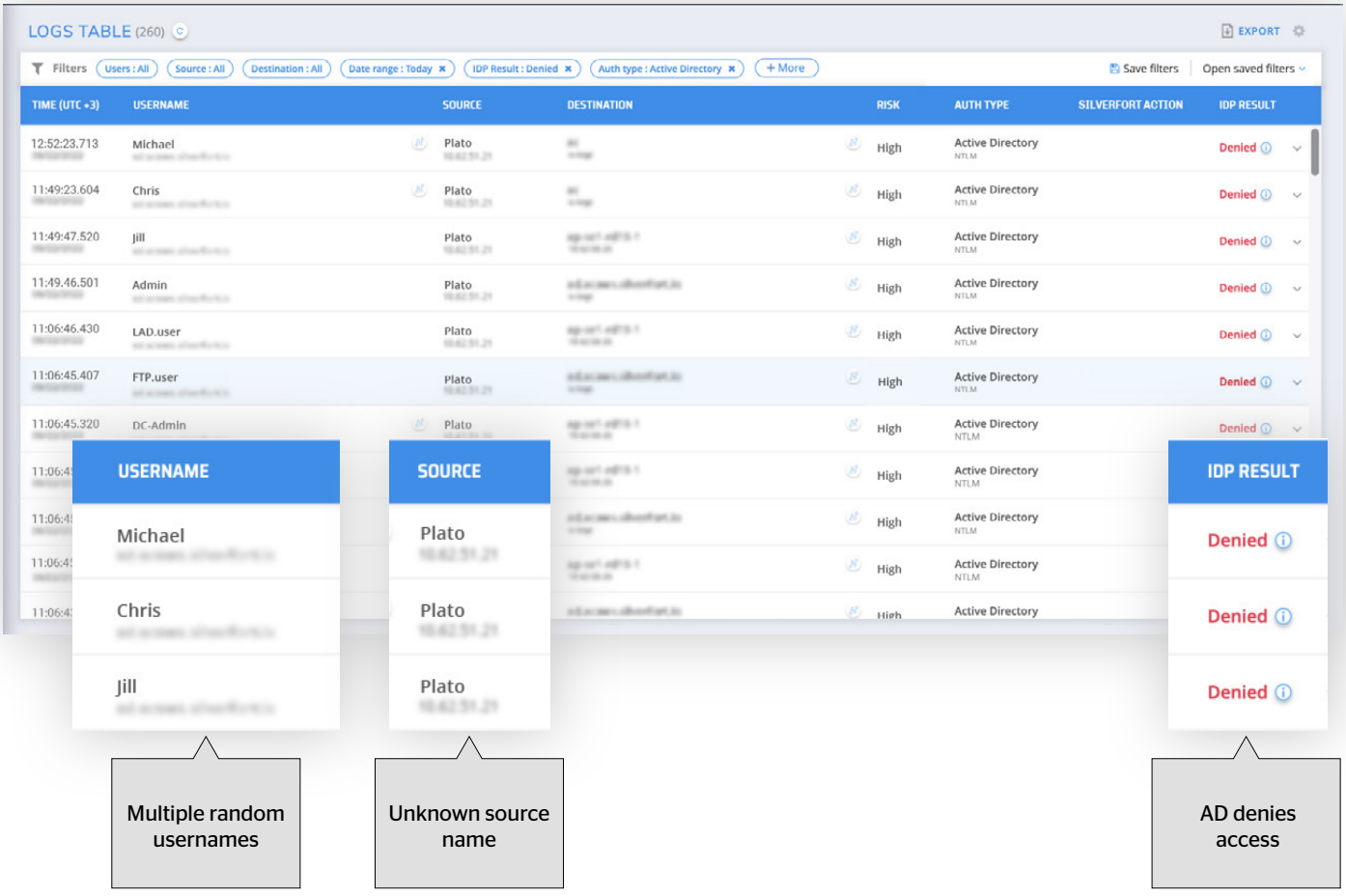
The Security team continuously monitors authentication requests and user activity by forwarding Silverfort logs to their SIEM solution. Silverfort's solution also provides data that otherwise would have to be collected and correlated manually, as well as built-in detections of malicious activities such as brute force, pass the ticket, Kerberoasting, and other identity threat techniques. Denied MFA requests also act as the ultimate Indicator of Compromise (IoC), providing real-time insights into which machines are compromised and enabling the security team to act rapidly in case of a breach.

The attack flow

Alerting on brute force attempts with Authentication Logs

In April 2022, the company's security team detected in Silverfort's log screen an irregular user and unusual machine activity on three company laptops. At the time, these laptops were in use by three employees who were visiting another company's factory. This first gave rise to the suspicion that this activity represented a supply chain attack.

The screenshot below shows Silverfort's authentication logs' screen. Note the rapid change in attempted usernames originated from the same source and the denial of all of them in the right 'IDP Result' column, indicating that the IDP (Active Directory in that case), has blocked them by itself due to the non-existent usernames. The Risk level of all these authentications is set to 'High' by Silverfort since it's clearly a Brute Force attack.



Screenshot 1: Multiple access attempts denied by the IDP (Active Directory)

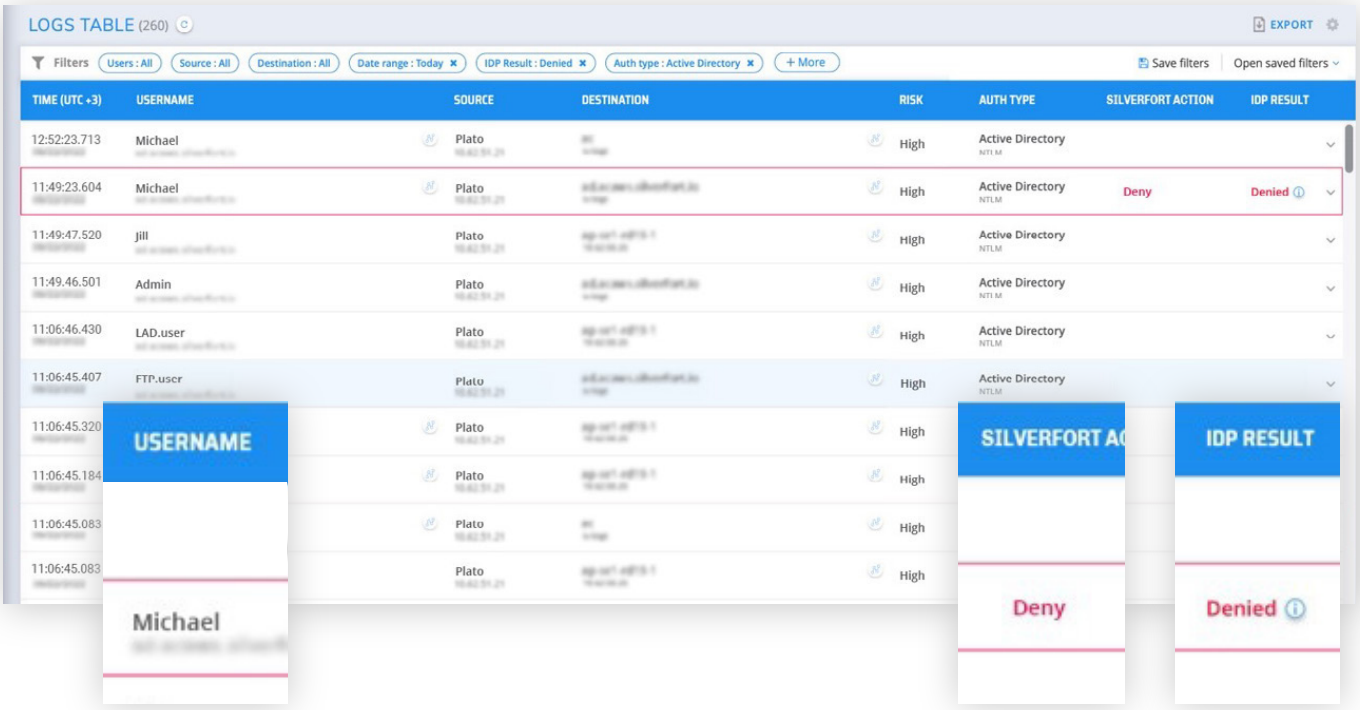
Within 30 minutes, the security team concluded that suspicious activity was taking place and immediately instructed the targeted users not to use their laptops until further investigation.

Stopping lateral movement with access policy

Analyzing the authentication logs that Silverfort provided, the security team came up with the following findings:

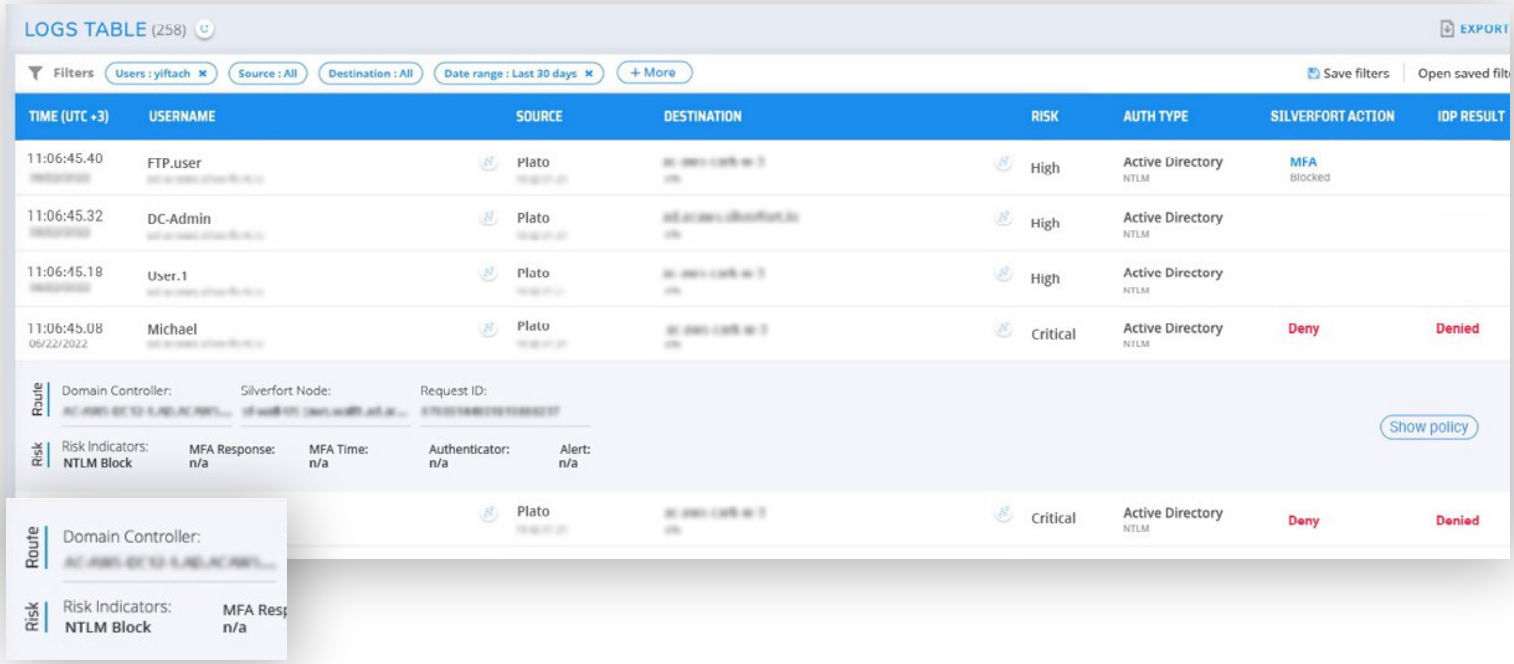
1. Suspected threat actors, via initial brute force attacks, had attempted to guess domain users of the customer's environment but failed.
2. These attempts were blocked by Active Directory due to the non-existent usernames used.
3. However, at a certain point, the attackers did manage to correctly guess an administrator's username and password.
4. Silverfort policy that was previously configured and enabled blocked this access attempt, one that otherwise would have become a steppingstone into the customer's domain and sensitive resources.

Below is the authentication logs screen displaying Silverfort's detection of malicious activity from the user 'Michael'. Silverfort and their IDP denied the access request. The screenshot of the authentication logs below shows the authentication of 'Michael'. As you can see, while all other authentication attempts were warded off by Active Directory, this one has also 'deny' on the 'Silverfort Action' column indicating that the username and password have satisfied AD requirements, but were detected as 'Critical' by Silverfort (see 4th column from the right), that instructed AD to deny access.



Screenshot 2: Single access attempt denied by Silverfort

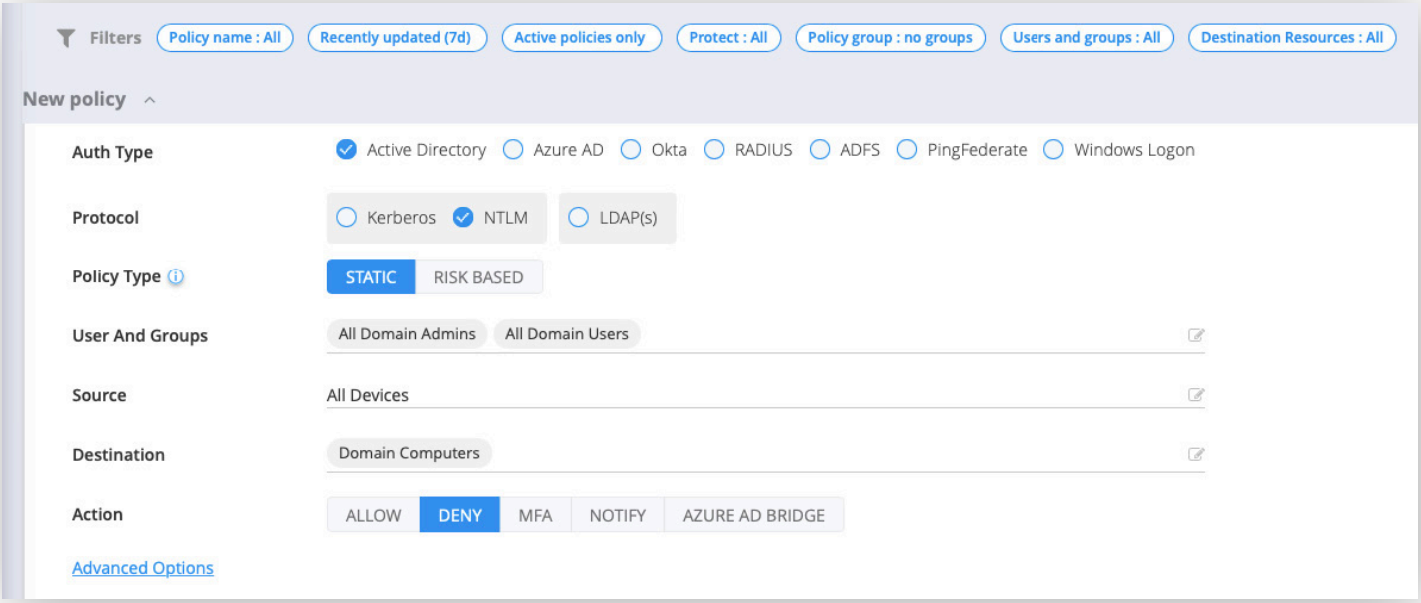
Expanding the log of this authentication reveals that Silverfort detected 'NTLM authentication' risk indicator in this access attempt. The 'show policy' on the right shows that there was an active policy in place that prevented this authentication from succeeding.



Screenshot 3: Authentication log expansion

Silverfort policy zoom-in

Preceding the attack, the company had put a policy in place via the Silverfort platform not to allow any NTLM logins between workstations and servers. As explained, this policy prevented the malicious access attempt in real-time – despite the compromised credentials – and enabled them to successfully thwart the attack. Below is the policy created by the company in the Silverfort platform. It is a rule-based policy that denies any access attempt that is carried out through NTLM.



Screenshot 4: Silverfort's policy

Identifying the initial compromise vector

Following a forensic investigation of the laptops, the company's security team deduced the following:

1. All three laptops were accessed from an unknown external IP.
2. Searching this IP in various threat intelligence engines revealed that this address had sourced multiple network attacks in the previous month and was associated with nation- state threat actors.
3. The threat actors had compromised the factory's Wi-Fi network, intercepting the communication of every machine that connected to the Wi-Fi router, including the three visitors' laptops.
4. Following the initial access to the laptops, the threat actors attempted to log in as customer domain users, leading to the attack stages described earlier.

Further investigation revealed that the blocked lateral movement was the only part of the attack in which valid employee credentials were compromised and put to attempted use. After reviewing Silverfort logs and removing malware traces from the infected laptops, the security team determined that the incident has been resolved.

Conclusion: Lateral movement from main to secondary targets in supply chain attacks

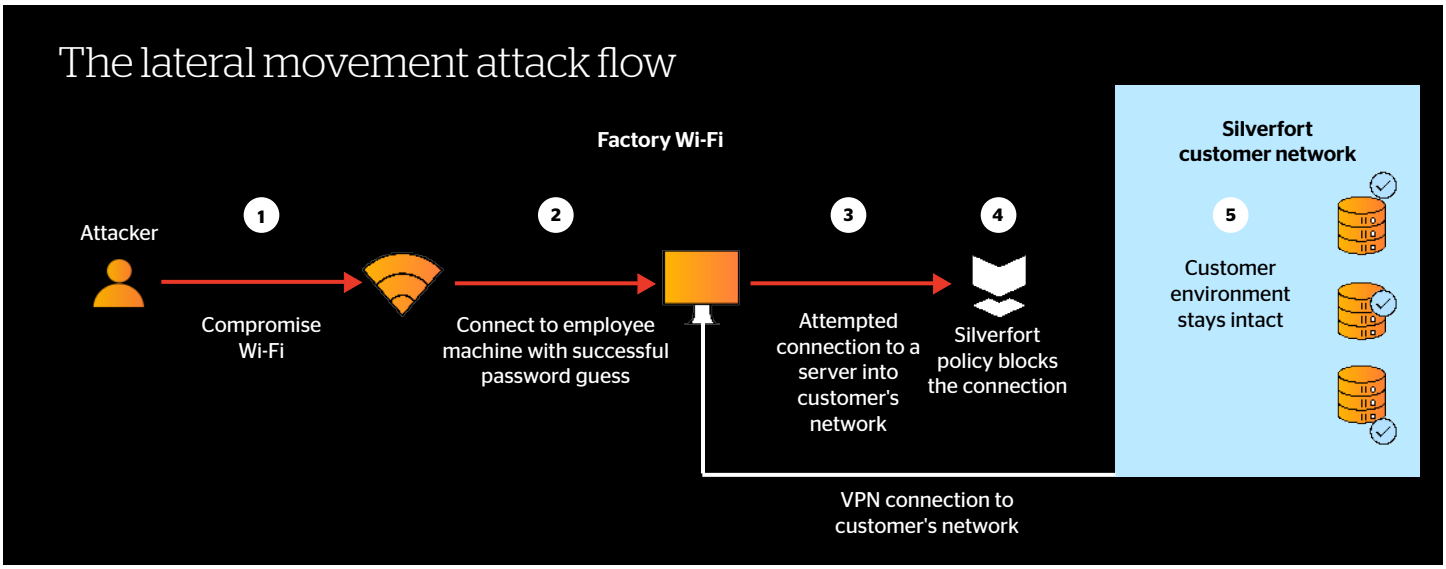
At this point, the team realized they were not the intended target but rather collateral damage in an attack aimed at the third-party factory via its Wi-Fi routers, so it immediately alerted the factory of this security event.

It is interesting to note, however, that despite not being the attack's initial target, once the threat actors realized that they had compromised an unexpected victim, they shifted gears and employed manual resources to capitalize on this unintended new compromise. This is not usual in supply chain attacks, where collateral victims are targeted per their contribution to the compromise of the main target.

This incident may, in fact, reflect a different type of supply chain attack that is not actually focused on the main victim. Rather, it gains a foothold in selected environments to use them as a "watering hole" to compromise their visitors' ecosystem. These visitors present an attractive attack surface, since they can be part of the compromised local network as well as their own domain network simultaneously.

This might call for reviewing the definition of lateral movement and widening it to include moving between different organizations' networks. Traditionally, lateral movement is defined as spreading from an initial access foothold to additional targets within the same network to reach a desired target. However, in a supply chain attack such as the one described here, the attempted lateral movement actually took place within a single machine. And its purpose was to move from guest presence to logging in as a domain user.

This is illustrated in the following diagram:



Silverfort real-time identity protection spotlight

Following the initial access to the Wi-Fi routers and the execution on the employees' laptops, the attack moved to its identity-based stage. From that point onwards, Silverfort enabled the security team to fully address the identity aspect of this attack:

Rapid and efficient response

The authentication logs provided by Silverfort enabled the security team to spot the brute force attack almost immediately after taking place. Based on the detection alerts from Silverfort, the security team had concrete knowledge of the attempted attack and its scope, enabling it to take immediate action and instruct its employees to shut down their laptops. Thus, the attack was fully monitored and contained.

Real-time blocking

Silverfort's NTLM access policy prevented the attackers from utilizing the credentials they had compromised to move laterally within the manufacturer's environment. It's important to note that this blocking took place in a fully automated manner due to the initial configuration and activation of the access policy, without any further manual intervention from the security team.

Silverfort real-time identity protection spotlight

While the manufacturer blocked the use of NTLM connections completely, many organizations can't ban NTLM due to various operational reasons. In that case, a similar Silverfort policy that replaces the action parameter from 'DENY' to 'MFA, would enable to maintain the use of NTLM while preventing its abuse for malicious access.

The following table summarizes the attack, mapping its stage to the MITRE attack framework, illustrating how in such type of supply chain attack identity protection is the first line of defense for the secondary targets. Although Silverfort's customer couldn't control a wireless network in a third-party company, it was definitely capable of monitoring and protecting its domain users.

Tactic	Technique	Target	Silverfort protection
Initial Access	**Wireless Compromise ID: T0860**	**Third-party factory**	
Execution	**User Execution: Command and Scripting Interpreter ID: T1059**	**Manufacturing customers employees' laptops**	
Credential access	**Brute Force: Password Guessing ID: T1110.001**	**Manufacturer customer's users**	 **Alerting the security teams on repeated brute force attempts**
Lateral movement	**Valid Accounts ID: T1078**	**Manufacturer's domain network**	 **Blocking the lateral movement with an access policy**

Conclusion

Detecting and preventing identity threats is critical

The story of this attack clearly demonstrates how security teams can gain the upper hand against advanced cyberattacks by implementing real-time identity protection to their security stack. This is because the identity-related aspects of these attacks – both the credential compromise and the lateral movement attempts – are key weapons in today's threat actors' arsenal. Silverfort Unified Identity Protection is the only tool that provides security teams with a truly comprehensive way to combat identity threats and maintain a secure environment.

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