SILVERFORT

CASE STUDY

Silverfort Helps Optix Renew Cyber Insurance and Prevent Lateral Movement Attack

Optix

Optix is the market leader in the optics IT software industry which helps optical retailers to manage patients, staff, suppliers, operations, and finances since 2001. Using a clean, modern, intuitive interface, Optix sends both patients and staff the clear message that their business is embracing cutting-edge technology. Optix's business management application enables customers to achieve improved patient care and increased and higher-quality sales.

BASED
York, England

INDUSTRY
Business Software

USERS AND SERVICE ACCOUNTS
Over 250

ENVIRONMENT
On-prem Active Directory workstations and servers, privileged accounts

The Challenge: Comply with Cyber Insurance Requirements

- Meet new cyber insurance requirements around MFA protection
- Secure all domain access requests
- Limited visibility and detection of service accounts

The Solution: Renewed Cyber Insurance Policy

- Cyber insurance policy renewed
- All domain access requests admin now authenticated with MFA
- Complete visibility into all service accounts

The Challenge

MFA Protection Needed to Comply with New Cyber Insurance Requirements

In response to the continuing increase in global ransomware attacks, Optix's cyber insurance provider tightened requirements for customers seeking to renew their policy. The insurance company specified several new conditions with which Optix needed to comply, including the ability to enforce Multi-Factor Authentication (MFA) on all domain admin access requests.

Optix examined different traditional MFA solutions but did not want to add agents to every machine. "We didn't like the fact that, in theory, any user with the appropriate permissions could disable the agent and remove it from their machine," explained Trevor Rowley, Managing Director of Optix.

> "Our insurer requested that we implement a solution that would allow us to authenticate every admin access request, and until we had that solution in place, we would not be able to renew our policy."

This challenge forced Optix to seek out an agentless solution for MFA protection. "In truth, we were just saying there must be another and better way of doing this than putting an agent on every single server and machine," Rowley explained.

Limited Visibility Into Service Accounts

On top of adding MFA protection for domain-level admin access, Optix was looking for a solution that would enable them to gain better visibility into their service accounts. "We needed a better picture of the details of each service account: how they were configured, what services they were running, what privileges they had, and if they had admin access permissions. Our state of managing service accounts definitely needed to be improved," said Rowley.

In addition to managing these accounts, Optix wanted a way to detect all user accounts that were configured to be service accounts. "We needed a way to detect accounts that should never have been assigned as service accounts. These should have been a dedicated service account with controlled privileges, not a domain admin account where someone just shoved in the administrator credentials onto the service account," Rowley explained.

After searching for agentless MFA, Optix discovered Silverfort and realized it was the right solution for their identity protection needs. "Once we decided to go with Silverfort, we started to see other extremely useful capabilities, such as detecting service accounts," said Rowley.

> "We choose Silverfort for agentless MFA protection and also because the solution helped us checkmark our cyber insurance policy requirement."

The Solution

Fast Onboarding Helped Optix Quickly Renew its Cyber Insurance Policy

Once Optix implemented Silverfort across its environments, they were able to renew its cyber insurance policy shortly after. And while cyber insurance was the key driver, Optix appreciated that they had gained a true identity protection partner.

> “Once we started to use Silverfort, we truly understood the depth of the product and the capabilities it offered.”

Optix was also pleased with Silverfort’s onboarding process. “From installing Silverfort in our environment to working closely with the Silverfort team we were quickly able to onboard and get the results with the solution right away. I’ve got to congratulate Silverfort on their customer onboarding,” said Rowley.

Additionally, Optix especially appreciates the hands-on support Silverfort’s customer success team provides. “They will look after you, so knowing that you’re not just going to be left on your own trying to work it out has been critical to our success in using the platform,” Rowley explained.

360° Visibility Into Service Account Protection

Although the detection of service accounts was not an initial driver, Optix quickly discovered the value Silverfort provides with service account management.

> “Silverfort’s service account detection capabilities have enabled us to gain visibility into every service account in our environment, including ones that we didn’t mark previously as a service account.”

Silverfort helped Optix quickly uncover these accounts, which otherwise would’ve remained undetected. “After detecting all 110 service accounts, we could see a lot of servers used domain admin accounts as service accounts, so we needed to fix this. We know when a particular server is using administrator optics as a service account and we can go in, look at the services, and find the one and fix it,” Rowley said.

One feature Optix particularly appreciates is how Silverfort helps them limit the usage and destinations of service accounts. “These capabilities have allowed us to enforce sensible limits so that service accounts can only access their intended machine in order to run their service,” said Rowley.

Preventing a Lateral Movement Attack

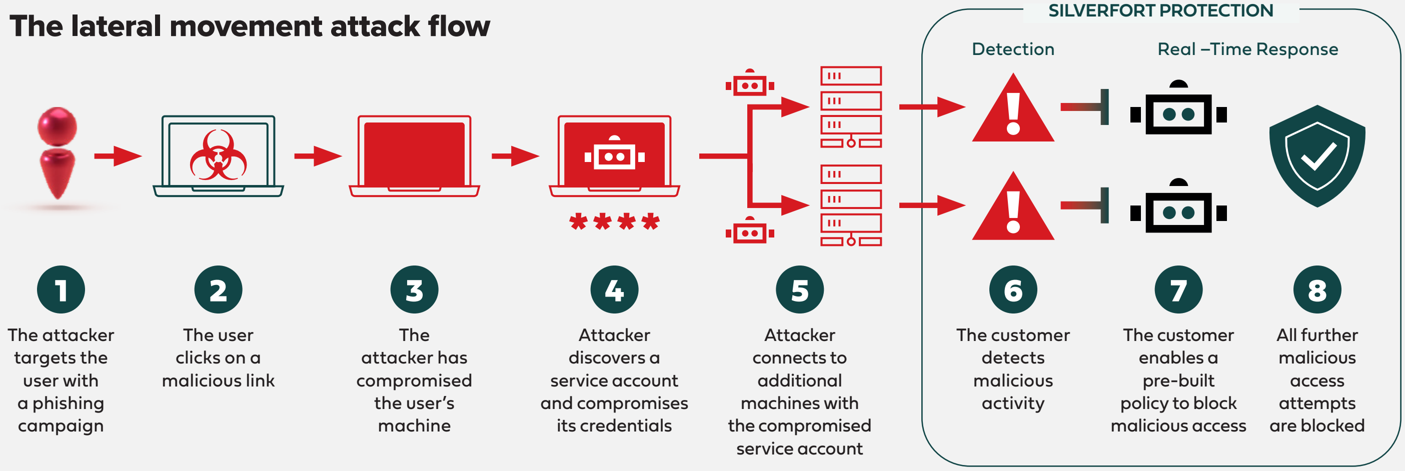
Two months after deploying Silverfort, Optix was targeted by a malicious actor who was trying to move laterally across their network using the compromised credentials of an Optix service account.

During a session with Silverfort, the customer success team highlighted abnormal behavior in the service accounts logs. “After further investigation, we clearly understood and saw that a machine in our environment had been compromised by a malicious actor,” said Rowley. Because an Optix user had clicked on a malicious link, the attacker was to gain access to the user’s machine and move laterally with a service account. “We could see that through service account access the machine using the credentials was trying to access every single machine on our network. The Silverfort team showed us how many times that machine had accessed other machines, so we drilled into the logs to see the details behind these malicious access requests,” Rowley explained.

> “Without Silverfort we would have never seen this abnormal behavior and the malicious actor would have successfully moved laterally across our network,”

By using Silverfort, Optix was able to identify the root cause and immediately blocked all access for the user whose credentials had been compromised.

The lateral movement attack flow



1. The attacker targets the user with a phishing campaign
2. The user clicks on a malicious link
3. The attacker has compromised the user’s machine
4. Attacker discovers a service account and compromises its credentials
5. Attacker connects to additional machines with the compromised service account
6. The customer detects malicious activity
7. The customer enables a pre-built policy to block malicious access
8. All further malicious access attempts are blocked

This example illustrates the importance of having a full identity protection solution in place, not just to comply with new cyber insurance requirements but to prevent attacks by threat actors using compromised credentials.

> “Due to deploying Silverfort for our cyber insurance requirements, we were able to stay secure when we needed it the most.”