Silverfort

CASE STUDY

# Beyond cyber insurance policy renewal: Womble Bond Dickinson (UK) LLP strengthens their identity security posture with Silverfort

**BASED**
Greater London Area, UK

**INDUSTRY**
Law practice

**USERS**
1,500

**ENVIRONMENT**
On-prem Active Directory, Entra ID
250 business applications, SQL servers
247 service accounts

WOMBLE BOND DICKINSON

Womble Bond Dickinson (UK) LLP is a transatlantic law firm. With their regional heritage and local knowledge combined with a transatlantic outlook, they provide the breadth of legal experience and services to meet their client's needs across the UK. Womble Bond Dickinson (UK) LLP employs best-of-breed technologies to protect their data, services, and solutions.

**THE CHALLENGE:**

## Comply with cyber insurance requirements

- Comply with MFA requirements to renew their cyber insurance policy
- Improve visibility and insights into all identity data
- Gain visibility and detection of service accounts

**THE SOLUTION:**

## Real-time MFA protection across all users and renewed cyber insurance policy

- Implemented MFA protection for all users and resources
- Strengthened AD hygiene by having complete visibility into user types and their activity
- Gained full visibility and protection of all service accounts

## **The challenge:** MFA protection is essential for meeting new cyber insurance requirements

By enforcing stricter MFA prerequisites for policy renewals, cyber insurance firms are emphasizing the importance of proactive risk mitigation. This prompted Womble Bond Dickinson (UK) LLP to comply with the new MFA requirements and bolster their identity security measures accordingly.

"During the policy renewal phase, our insurer required certain MFA controls, including MFA for privilege account access, to protect all our internal resources," said James Holder, Infrastructure and Cyber Security Analyst of Womble Bond Dickinson (UK) LLP.

These new compliance requirements highlighted some larger gaps in their environment.

"After performing due diligence on our environments and security controls, our insurer required a greater level of security over our on-prem resources and Active Directory. To renew our policy and improve our overall security posture, we focused our efforts on resolving this security gap," added Janusz Wreba-Jaworski, Cyber Security Manager of Womble Bond Dickinson (UK) LLP.

> **"To renew our insurance policy, we needed a solution that would apply MFA protection across our environment while providing visibility and insight into our identity security posture."**
>
> — James Holder, Infrastructure and Cyber Security Analyst of Womble Bond Dickinson (UK) LLP

## Limited visibility into user and service accounts activity

In addition to complying with the MFA requirements for their cyber insurance policy, WBD wanted an improved understanding of all user account access requests and authentications.

> "We had limited visibility into our Active Directory user accounts and service accounts, minimal understanding of their overall activity, and no way to control any elevation requests or prevent lateral movement within our organization."
>
> — James Holder,
> Infrastructure and Cyber Security Analyst of
> Womble Bond Dickinson (UK) LLP

"We had AD data, but we lacked anything that could provide the visibility we needed alongside proactive insights into our AD activities," said Holder.

Additionally, WBD wanted greater visibility and protection of its on-prem resources. "We have 250 business applications, and each application must run on-prem. We needed to improve our visibility and protection of these resources, which did not have security controls at the time due to only using Azure MFA and SSO for cloud resources. We needed a way to extend MFA protection to our on-prem environment as well," added Holder.

Having searched for an identity security solution, WBD was recommended Silverfort. They soon realized Silverfort offered much more than their original requirements.

"We were initially seeking a point solution that wasn't too expensive and that would help us tick the box for our cyber insurance needs. We weren't looking to invest in a full identity management suite, so we thought we needed something specific that would hit the spot," said Wreba-Jaworski.

> "After our reseller recommended Silverfort, we did a demo and POC – and our jaws dropped. We were left wondering where this has been all our lives. We knew we absolutely needed this to fit our identity security needs, so we partnered with Silverfort."
>
> — Janusz Wreba-Jaworski, Cyber Security Manager of Womble Bond Dickinson (UK) LLP

## **The solution:** Fast deployment and policy enforcement helped WBD quickly renew its cyber insurance policy

After signing on with Silverfort, WBD quickly deployed the solution and saw results right away while renewing its cyber insurance policy.

"By quickly deploying Silverfort into our environment and applying access policies to our entire user base, we complied with our insurer's requirements. We were able to configure and apply different access policies including MFA Prompt, Deny, and Notify Only, which allowed us to quickly implement the security controls needed across our environment," said Holder.

As a result of applying different types of policies, WBD has gained a more complete visibility and understanding of their environments and users.

> "Our Silverfort policies have allowed us to ensure that our users and resources are protected and secure, and to gain complete visibility into all access and authentication activities."
>
> — James Holder,
> Infrastructure and Cyber Security Analyst of
> Womble Bond Dickinson (UK) LLP

“Some of our deny policies are risk-based for Kerberos and suspected Kerberos which has helped us limit our chances of falling victim to a lateral movement attack. Also, we have another deny policy set up for people who forget to connect to servers with their admin credentials. They sometimes use their user credentials which can cause some security risks,” says Holder.

WBD has been satisfied with the information provided by their policies when learning more about the activities of their users. “As a result of our different policies, we have gained better insights and proactive takeaways from Silverfort logs,” Wreba-Jaworski added.

> "Through the log screen, Silverfort highlighted several security risks in our environment, such as NTLMv1 usage, which we would not have known about without Silverfort."
>
> — Janusz Wreba-Jaworski, Cyber Security Manager of Womble Bond Dickinson (UK) LLP

## Complete service account protection

Once they understood how Silverfort could address additional use cases, WBD implemented Silverfort’s service account detection and protection capabilities.

“We didn’t realize when we initially looked into Silverfort that they could help us with our service accounts, but it has been of great value as their service account protection capability is exactly what we needed. We have around 250 service accounts that need to be protected. Being able to lock down those service accounts from source to destination helps us to pinpoint the accounts that have far too much access. Also, in the case of irregular activity, we can reach out to the application owners and alert them of the activity. This has been critical for visibility as we never had that before,” Holder added.

Additionally, WBD has strengthened its overall security posture by ensuring its service accounts are used properly.

“It has helped us understand our bad practices internally. We’ve had some people using service accounts as user accounts, and some people using user accounts as service accounts. Now we can identify the behavior and make sure the service accounts are used properly,” said Wreba-Jaworski.

> "Overall, we highly recommend Silverfort, as the identity insights you get and the flexibility for policy enforcement and the granularity have been critical for our success in protecting our environments."
>
> — Janusz Wreba-Jaworski, Cyber Security Manager of Womble Bond Dickinson (UK) LLP

## 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