Silverfort | BlueFort Security

CASE STUDY

Southampton City Council strengthens its ransomware resilience and incident response with BlueFort Security and Silverfort

BASED
Southampton, UK

INDUSTRY
Local government

USERS
3,500+ employees and external partners

ENVIRONMENT
Active Directory
Entra ID, Microsoft Authenticator
VMware, Citrix and Cisco

SOUTHAMPTON CITY COUNCIL

Southampton City Council is a leading local authority in the South of England, serving one of the region's major urban centres. The council supports residents, businesses, and communities across the city, with a broad range of responsibilities, including housing, education, transport, social care, and environmental management.

THE CHALLENGE:

Strengthen protection against ransomware while securing access across systems

- Low ability to enforce MFA on internal Windows services and infrastructure components
- Lack of visibility into service accounts, including stale accounts and potential misuse
- Dependence on token-based authentication with restricted admin coverage
- Need to enhance the protection of public services from the risk of cyber attacks

THE SOLUTION:

Reduced ransomware risk and achieved stronger identity security

- Enforced MFA protection across all remote access, on-prem systems, and third-party connections
- Discovered and remediated a large number of dormant service accounts, progressing towards gMSA adoption
- Replaced physical tokens with modern authentication, lowering costs, improving user experience, and enhancing administrative efficiency

The challenge: Limited MFA options and hidden service account risks increased ransomware exposure

As a public sector authority, Southampton City Council is responsible for maintaining the continuity of critical services and operations that thousands of citizens rely on every day. With ransomware attacks escalating across UK government institutions, identity security quickly became a strategic priority for the Council's IT team.

"The biggest driver for us was ransomware. It's about trying to stop lateral movement. If you have MFA on, it just makes it difficult for them to get a foothold. The main problem was that we couldn't do MFA on our internal network for Windows services. Our existing token-based deployment had shrunk over time and was expensive to maintain, and Microsoft's on-prem MFA options didn't have the full capabilities we were looking for."

— Infrastructure and Security Lead,
Digital and Strategic IT for Southampton City Council

At the same time, service accounts created another layer of risk, with limited visibility into how they were being used or where they were active.

"We've had some of these service accounts for years: they'd been used on different servers than originally intended, and we had limited visibility of where they were now being used. We couldn't see when they were last active, what systems they touched, or even what protocols they relied on, " said the Infrastructure and Security Lead.

Finding the right identity security platform

Southampton City Council was aware of its identity security gaps and the IT team recognised the need for a solution that could extend MFA across on-prem systems. They also wanted to move away from physical tokens and gain much-needed visibility into service accounts.

As a long-standing security partner, BlueFort Security played a key role in introducing Silverfort. Following initial discussions, a guided POC quickly demonstrated how Silverfort could modernise and consolidate the Council's authentication approach, while extending protection across Active Directory and other critical systems. The ability to secure authentications without requiring infrastructure changes proved particularly compelling.

"MFA was already in place for our users, and we were actively looking to extend it. We'd done some work with Microsoft's solution, but felt it didn't fit all our requirements. Silverfort worked straight away, and it sold itself to us. We had proof of concept, workshops, and a fully guided install process. That was great because it meant we could turn it around quickly, but also meant we were learning as we were going."

— Infrastructure and Security Lead,
Digital and Strategic IT for Southampton City Council

The solution: Extended MFA protection to legacy systems and reduced service account risks

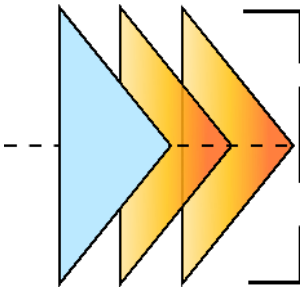
After completing the POC, Southampton City Council worked with BlueFort Security's services team to deploy Silverfort across its hybrid environment. With BlueFort's support, the rollout for major integrations, including Remote Desktop, Hyperviser systems, Infrastructure and historic remote access systems, was completed in just a matter of days. It allowed Southampton City Council to enforce MFA credentials on all required systems with minimal effort, immediately reducing the Council's exposure to ransomware and lateral movement.

"From an admin perspective, it was just turn it on and go. Once we got a grip on it, Silverfort was really straightforward. We deployed Silverfort on some of our systems in no time. We just updated the rule, removed the old 2FA, and integrated seamlessly. The same was true with what we thought would be complicated systems, where replacing Microsoft MFA with Silverfort took about half a day. Even Networking equipment integration moved across easily once we tied it into AD authentication," said the Infrastructure and Security Lead

Another key priority for the Southampton City Council was cleaning up service accounts. Silverfort discovered a substantial number of dormant accounts and provided end-to-end visibility into how and where they were being used, helping the team reduce the risk of misuse.

> "The great thing is Silverfort gave us visibility which we didn't have before. We saw lots of service accounts we didn't have full or up-to-date information about. Silverfort showed us the sources, destinations, and what protocols they were using. With these insights, we got rid of many dormant accounts. We could see when accounts were last active on the network, which made it much easier to clean them up with confidence and that nothing would break."
>
> — Infrastructure and Security Lead,
> Digital and Strategic IT for Southampton City Council

Looking ahead: Building long-term resilience with an identity-first security approach



Southampton City Council has made Silverfort a cornerstone of its identity security strategy. Beyond securing privileged access to critical resources, the team embedded Silverfort in ransomware playbooks, enabling incident response teams to block authentication attempts instantly in the event of a breach.

Southampton City Council also plans to continue refining service account management, progressing towards broader gMSA adoption and ensuring ownership and control remain in place. In the event of mergers with neighbouring councils, Southampton is confident it has a clean and resilient identity security foundation that can scale to meet future demands.

> "Silverfort gave us the visibility and control we were missing. It's now part of how we plan for ransomware protection and long-term resilience. At the same time, it's made life easier both for administrators and for colleagues using it day-to-day, which gives us real confidence moving forward."
>
> — Infrastructure and Security Lead,
> Digital and Strategic IT for Southampton City Council

About Silverfort

Silverfort secures every dimension of identity. We are the first to deliver an end-to-end identity security platform that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surfaces, and enforce security controls inline to stop lateral movement, ransomware, and other identity threats.

About BlueFort Security

BlueFort is the UK's leading Security Solutions Provider (SSP), trusted since 2007 to help organisations operate securely in an increasingly complex digital world. BlueFort protects hundreds of organisations and millions of users through solutions aligned with globally recognised security and compliance frameworks — from NIST, ISO 27001, and Cyber Essentials Plus to CIS Controls, NIS2, SOC 2, DORA and the UK's NCSC guidelines. Their expertise begins with robust identity & access management and advanced cloud security, then extends across the full landscape of cybersecurity, including operational technology (OT) security, data protection, threat detection and response, compliance, and the safe adoption of AI tools. BlueFort Security is a trusted cybersecurity partner and a Crown Commercial Services and G-Cloud 14 supplier.