Silverfort

Protecting against Business Email Compromise (BEC) with Silverfort

Strengthen your resilience by closing identity security gaps beyond BEC risks

Business Email Compromise (BEC) is one of the costliest cyber threats for organizations worldwide. With an average loss of $50,000 per incident, and an estimated $6.3 billion in annual global damages, BEC now ranks alongside ransomware as one of the most destructive cyber risks.

While traditional security controls—including secure email gateways, Domain-based Message Authentication, Reporting, and Conformance (DMARC), and employee awareness training—help reduce exposure, they cannot prevent what happens once credentials are compromised. With compromised credentials, attackers can move laterally across systems, escalate privileges, and gain access to critical resources while appearing as legitimate users.

This makes the identity security layer the last line of protection for containing BEC and reducing the financial and operational impact on organizations and insurers.

How Silverfort mitigates BEC risks

Silverfort is the first identity security platform that extends modern identity security controls across the entire IAM infrastructure. By discovering every identity, analyzing exposures, and enforcing protection in real time, Silverfort closes the gaps that allow compromised accounts from BEC incidents to escalate into costly breaches.

1. Unified identity visibility & continuous monitoring

Gain end-to-end visibility into every identity, including human and non-human identities, and their authentication activities across on-prem and cloud environments. Silverfort continuously monitors identity activity, detecting anomalies such as unusual devices, privilege escalation, or lateral movement that may follow a BEC compromise.

2. Adaptive, risk-based access controls

Silverfort enforces real-time access policies that automatically trigger MFA prompt to verify or block risky authentications. This ensures that even if an account is compromised, it cannot be used to move laterally, escalate privileges, and spread ransomware across systems.

3. Extending MFA to previously unprotected resources

Silverfort extends MFA protection to resources traditional solutions can't reach without any infrastructure changes, including RDP, command-line tools, file shares, and legacy apps. This unified approach removes critical blind spots that BEC actors often exploit to expand access.

4. Rapid containment and incident response

Silverfort's Authentication Firewall blocks compromised accounts or risky authentications in real time. By correlating activity across hybrid environments, it reduces investigation and recovery time from weeks to hours, minimizing financial and operational impact.

Key benefits for insured organizations

Reduced exposure to BEC losses

Prevents abnormal activity and financial loss by blocking compromised accounts from being misused, even if email defenses are bypassed.

Proactive risk reduction

Continuously uncovers identity exposures, including misconfigurations, excessive privileges, or insecure authentication protocols, before they can be exploited into BEC incident.

Complements existing security tech stack

Works alongside secure email gateways, DMARC, and awareness training to provide the missing identity layer that closes the gap beyond BEC attacks.

Insurance and compliance readiness

Meets insurer and regulatory requirements for MFA and privileged accounts protection, helping organizations qualify for coverage and avoid higher premiums.

Faster incident response, lower claim costs

Enables rapid containment of compromised identities, reducing investigation and recovery timelines from weeks to hours – minimizing operational disruption and insurance payouts.

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.