

Email Security

Email remains one of the most common and effective channels for phishing, malware delivery, impersonation, business email compromise, and account takeover. Brite helps customers strengthen email security through layered filtering, threat detection, user awareness training, phishing simulations, account monitoring, and data protection controls.

By combining advanced email security platforms with user education and managed security oversight, Brite helps reduce the likelihood and impact of email-driven attacks.

Why Email Security?

Block Email-Based Threats

Detect and stop malicious links, attachments, impersonation attempts, spam, and phishing campaigns before they reach users.

Reduce Human Risk

Educate employees through security awareness training and phishing simulations to improve recognition and reporting.

Protect Accounts & Data

Monitor for account takeover activity and help prevent unauthorized transmission of sensitive information.



Advanced Email Filtering

Deploy and manage platforms such as Proofpoint, Abnormal, or similar solutions to detect phishing, malware, and impersonation.



Phishing Defense

Analyze sender behavior, message content, links, and attachments to identify and quarantine deceptive emails.



Security Awareness Training

Use platforms such as KnowBe4 to educate users and reinforce secure behavior through simulated phishing campaigns.



Account Takeover Monitoring

Identify suspicious mailbox activity, anomalous sending patterns, and signs of compromised user accounts.



Email DLP Support

Help enforce policies that reduce accidental or malicious exposure of sensitive information through email.

