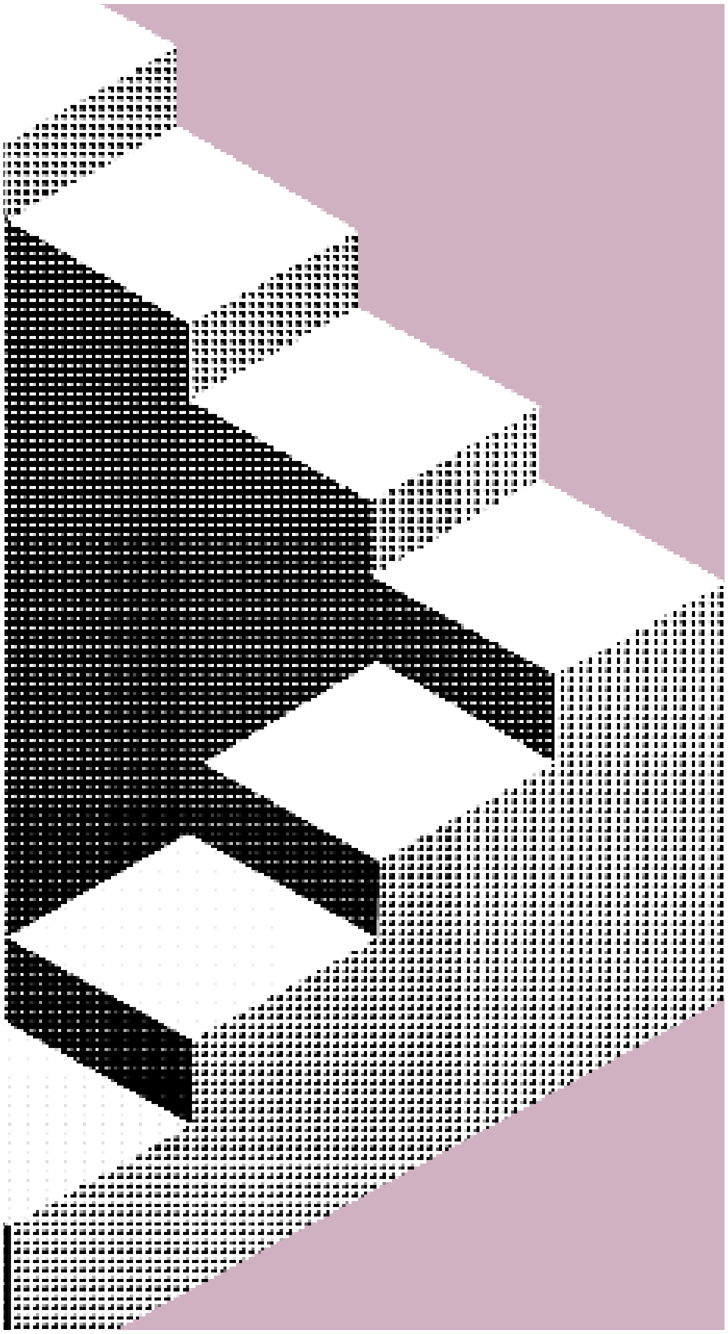
Datasheet
March 2022

okta | Material

Bring Zero Trust Security to email with Okta and Material

Protect the most sensitive messages with extra authentication



Email—it's no longer just a messaging app. It's a massive repository of sensitive content, the key to other accounts, and a critical enabler of your business. It's also a huge attack surface, and it's your job to keep it safe. Unfortunately, while how we use email has changed, how we protect it hasn't. Most email security solutions are still focused on blocking messages in a perimeter-centric security model. They don't account for the majority of attacks where email isn't just the way in, it's the actual prize.

Material and Okta have a better way: an integrated solution that brings Zero Trust security to mailboxes—protecting users and data even after a successful attack. The solution leverages your existing Okta deployment to add just-in-time authentication to the most sensitive email workflows. Gain visibility over your entire email footprint, and limit the scope of a potential breach all without retraining users or hurting their productivity.

Key Solution Benefits

- Protect sensitive content in email from attackers or malicious insiders using your existing Okta deployment.
- Extend Okta SSO protection to email-based password resets—even for apps that don't support SAML.
- Identify high-risk accounts with unsafe settings, personal account forwarding, frequent password resets, and more.
- Support internal investigations and legal requests with real-time message search and administration.

Protect sensitive content in mailboxes.

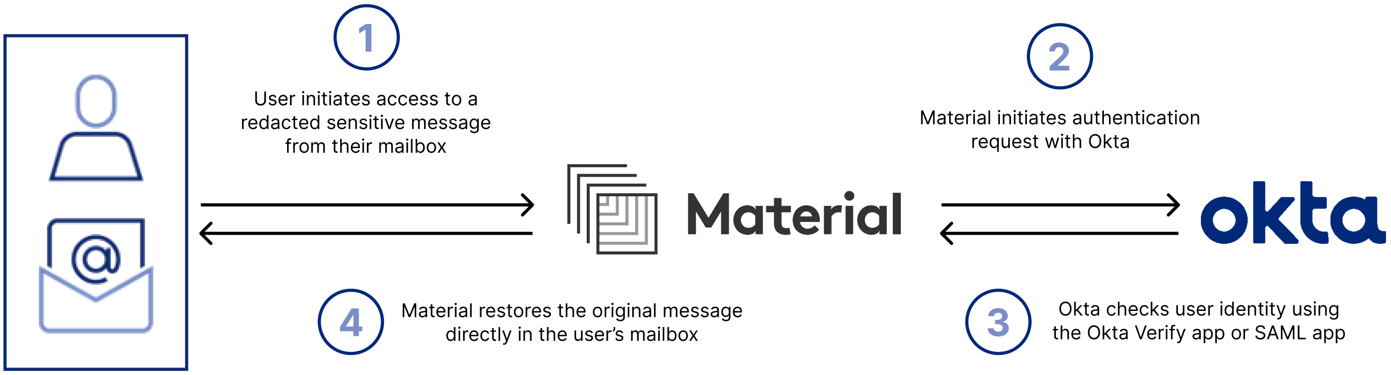
Modern mailboxes are vast repositories of sensitive content, including PII, financial reports, legal contracts, and more. While most of the content sits tucked away in archive folders, it is an extremely valuable target for attackers and malicious insiders. A Zero Trust approach calls for adding controls to individual messages, not just the email account in which they reside.

Material scans mailboxes for sensitive content and redacts messages so bad actors can't get them, even if they gain access to the email account. Users can still access redacted messages on-demand after a simple identity verification step, such as approving an Okta Verify request.

Close SSO gaps with password reset flow protection.

Okta Single Sign-On (SSO) allows IT and security teams to centralize the user login experience across hundreds of apps. But email is still the de facto identity provider for many apps that are unsanctioned or don't support SSO. In these cases, attackers can move laterally from email to another app via email-based password resets.

Material stops this common attack by adding an Okta identity verification step before delivering password resets and other types of account verification emails. That way, even if an attacker gains access to a user's email, they can't move laterally to other vulnerable apps. Close SSO gaps with Okta and Material without getting in the way of your users' productivity.


1
User initiates access to a redacted sensitive message from their mailbox
2
Material initiates authentication request with Okta
Material
okta
4
Material restores the original message directly in the user's mailbox
3
Okta checks user identity using the Okta Verify app or SAML app

With Okta and Material, enterprises can…

- Adopt a Zero Trust security approach to protecting sensitive email workflows—without hurting user productivity.
- Allow the workforce to seamlessly access sensitive messages while ensuring they are safe in a potential breach.
- Protect apps that don't support SSO with just-in-time Okta verification for signup confirmations and password resets.
- Gain unprecedented visibility and control over the entire email footprint, including foundational risk factors and powerful investigation tools.

How Okta and Material Work Together

Material extends your existing Okta investment to continuously secure sensitive email workflows—without adding friction for users.

First, Material syncs users and groups with Okta Universal Directory so you can roll out protections for just the users or teams that need them. Then, for protected email accounts, Material leverages Okta Multi-Factor Authentication (MFA) to verify users' identities whenever they try to access messages with privileged or extra-sensitive content. You can use existing MFA factors and contextual access policies in Okta for a seamless user experience and painless rollout. The result is a true Zero Trust approach to protecting email. Instead of a single all-or-nothing account-level control, you get a security model that incorporates message, device, and user context for added protection.

For more information on this integration,
go to **material.security/okta**

If you have more questions, please contact
our sales team at **okta.com/contact-sales**

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 6,500 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 9,400 organizations, including JetBlue, Nordstrom, Siemens, Slack, T-Mobile, Takeda, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, go to **okta.com**.

About Material Security

Material is taking a fresh approach to protecting every organization's most critical app: email. Material protects accounts even after they're compromised or harmful messages get through. It is entirely cloud-based, deploys in 30 minutes, and can be exclusively managed by the customer. The world's best security teams, including Mars, MassMutual, Lyft, Flexport, HackerOne, and Roblox, trust Material to keep their users and data safe. Material was founded in 2017 and is headquartered in Redwood City. To learn more, go to **material.security.**