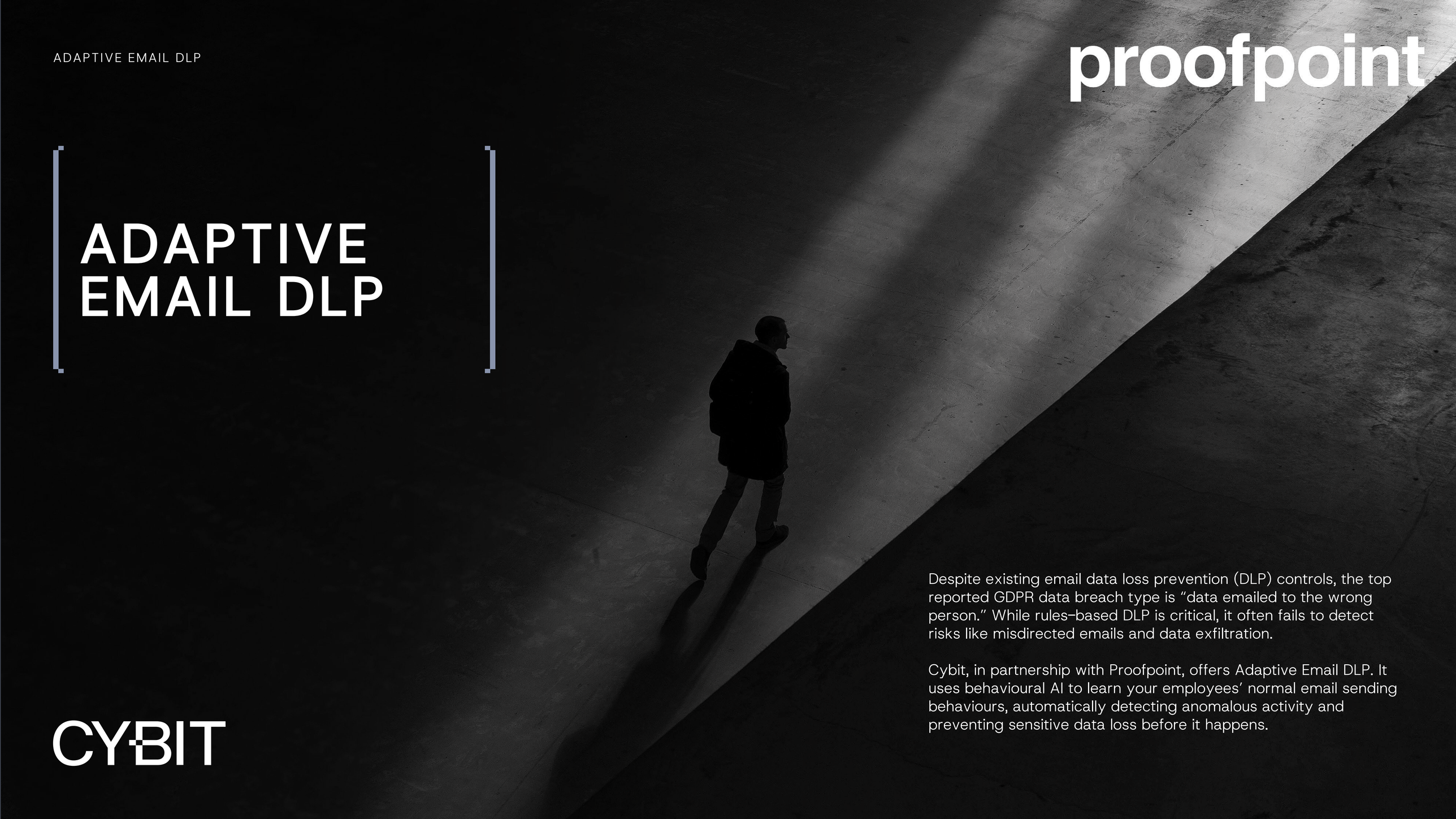
proofpoint

ADAPTIVE EMAIL DLP



Despite existing email data loss prevention (DLP) controls, the top reported GDPR data breach type is “data emailed to the wrong person.” While rules-based DLP is critical, it often fails to detect risks like misdirected emails and data exfiltration.

Cybit, in partnership with Proofpoint, offers Adaptive Email DLP. It uses behavioural AI to learn your employees’ normal email sending behaviours, automatically detecting anomalous activity and preventing sensitive data loss before it happens.

CYBIT

PRODUCT DESCRIPTION

Adaptive Email DLP uses behavioural AI to learn about your employees' normal email sending behaviours, their trusted relationships and how they communicate sensitive data. It then analyses each email to detect anomalous behaviour, notifying admins of potential data loss incidents and warning users in real time to prevent sensitive data loss through email.

KEY DELIVERABLES

- **Behavioural AI analysis:** Machine learning that understands employee email behaviour and identifies data loss incidents through relationship graphs.
- **Real-time user coaching:** Automatic warnings before sensitive information is sent, helping users avoid mistakes and policy violations.
- **Misdirected email prevention:** Detection and prevention of emails sent to wrong recipients using relationship analysis.
- **Misattached file protection:** Identification of unusual attachments with automatic warnings to prevent accidental data exposure.
- **Email exfiltration prevention:** Automatic data classification and personal email discovery to block unauthorised transfers.
- **Security awareness enhancement:** Real-time coaching that complements training by teaching users about email risks.

KEY FEATURES & BENEFITS

1. **Prevent accidental and intentional data loss:** Stop sensitive data loss through email using advanced behavioural AI that detects anomalous sending patterns.
2. **Mitigate reputation and customer risks:** Reduce risks of market reputation damage and customer attrition from data breaches.
3. **Reduce GDPR and CCPA fines:** Minimise regulatory penalties by preventing the top reported GDPR breach type – data emailed to wrong person.
4. **Stop misdirected emails:** Use relationship graphs and behavioural analysis to prevent emails being sent to wrong recipients.
5. **Prevent misattached files:** Detect when attachments look unusual for recipients and warn users before sensitive information is sent.
6. **Block email exfiltration:** Automatically classify sensitive data and discover personal email accounts to prevent unauthorised data transfers.

PRICING

- **Integrated solution:** Pricing available as part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.
- **Flexible deployment:** Available as cloud-based solution with scalable pricing based on user count and data volume requirements.
- **Optional add-ons:** Additional security awareness training and advanced threat protection modules available. Pricing on request.

WHY CYBIT?

Choosing the right partner for your Adaptive Email DLP deployment is crucial for maximising your investment.

Here's why CYBIT stands out:

- ✓ Proofpoint strategic partnership: As an established Proofpoint partner, we have direct access to premier support and advanced training to ensure rapid resolution of complex issues.
- ✓ Human-centric security expertise: We understand that effective DLP must focus on user behaviour and education, not just technical controls, ensuring solutions that drive real security outcomes.
- ✓ Always compliant, always protected: Cybit ensures your email DLP solution follows retention requirements and regulatory compliance, with proactive monitoring to prevent issues.
- ✓ 30+ years of IT expertise: Our extensive experience in cybersecurity and cloud services ensures you receive knowledgeable guidance that aligns with your business objectives.
- ✓ Behavioural AI specialists: Deep understanding of machine learning and behavioural analysis ensures optimal configuration and maximum protection from email-based data loss.
- ✓ Our commitment: Fast, comprehensive deployment with ongoing support to ensure your Adaptive Email DLP solution continues protecting your sensitive data as your business evolves.

[C]