KnowBe4

Stop Outbound Data Breaches Before They Happen with Prevent

Organizations lose data every day through human error, negligence and malicious behavior. KnowBe4 Prevent uses advanced AI and a contextual understanding of user behavior to proactively stop email data loss incidents before they happen.

Part of the KnowBe4 Cloud Email Security portfolio, Prevent leverages an intelligent, AI-native architecture, automatically improving its Data Loss Prevention (DLP) algorithm based on real-time and continuous risk assessments.

> ***" From a governance point of view, KnowBe4 Prevent helps maintain the integrity of client data and demonstrates that we've taken the necessary steps to reduce human error when emailing."***
>
> - Andrew Black
> Director of IT at Muckle LLP

Protect Against Accidental and Intentional Data Loss

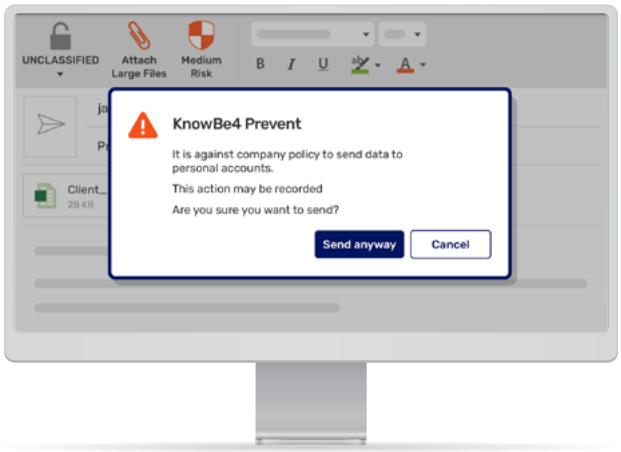
Static DLP is unable to prevent breaches caused by unpredictable human behavior. Prevent uses a combination of intelligent technologies, including machine learning, relationship mapping and contextual content analysis to detect anomalies that are indicative of human error or malicious intent.

Contextual prompts only engage employees right when they're about to send a risky email, enabling them to work efficiently and securely, and reinforcing training with real-time teachable moments.

Prevent™

Key Benefits

- Detects and prevents data loss incidents in outbound email
- Uses an AI-native architecture to continuously learn and improve detection based on risk
- Lowers administrative overhead with intelligent, self-learning outbound detection
- Engages users with an unobtrusive, real-time risk assessment as they compose an email
- Easy to deploy and maintain cloud service
- Provides visibility and quantifies risk based on user behavior



Quantify Risk While Lowering Admin Overhead

The Cloud Email Security Center provides on-demand visibility of each individual user's risk level, including insight into employees who receive frequent prompts, advice types, responses and monitoring of intentional exfiltration. When a user more frequently engages in risky behavior, Prevent will dynamically adapt its detection algorithm to enforce more frequent prompts, require sending approval, and other increased security measures to stop incidents before they happen.

Prevent is cloud-based, supported on all mobile devices and easy to deploy. It integrates seamlessly into Microsoft 365, augmenting both their native security and security offered by secure email gateways (SEGs). In addition, its self-learning detection technologies require minimal configuration and ongoing maintenance from admins. With Prevent, you're not just securing emails - you're empowering your team to communicate safely and confidently.

Key Features

- **AI-driven Technology:** Intelligent, self-learning technology that understands communication patterns to detect anomalies indicating human error or malicious intent, while minimizing user friction across your organization.
- **Misdirected Email Prevention:** Intelligently nudges users when emails may be sent to unintended recipients by detecting autocomplete errors, typos in email addresses, first-time external recipients, and greeting-recipient mismatches.
- **Data Exfiltration Protection:** Scrutinizes recipients and scans for attachments and unusual salutations to flag, block or report on exfiltration attempts.
- **Comprehensive Domain Protection:** Safeguards users from suspicious domains by alerting them to newly registered domains (less than 50 days old), blocking communication with domains on threat intelligence blocklists, and flagging potential sender impersonation attempts.
- **Real-Time Teachable Moments:** Prevent displays real-time email risk assessments, nudging users only when necessary, eliminating alert fatigue by intervening solely for genuine risks.
- **Microsoft Outlook Integration:** Hooks into Microsoft Office 365 via an Outlook Web Add-in and API and provides for full mobile and OWA coverage for end users, stopping data breaches when your teams are in the office, on the move, and at home.
- **Detailed Analytics & Reporting:** Access detailed analytics on user interactions with security prompts, identify high-risk individuals exhibiting non-compliant behavior, and leverage scenario-specific reporting to spot threats and demonstrate compliance—all from a single dashboard.

Prevent Enterprise

- **Supervised Machine Learning:** Combines relationship mapping, machine learning and DLP policies to identify misaddressed recipients and sensitive content, including attachments.
- **Custom Misdirected Content Analysis:** Analyzes the subject line, message body and attachments to learn what content users typically share with recipients and prevent them emailing the wrong, potentially sensitive, content.
- **Custom DLP Rule Enforcement:** Warns users when sending content matching company-specific sensitive keywords or patterns to unauthorized recipients.
- **Ethical Walls:** Preserve information barriers in your organization in order to avoid disclosure of information and conflicts of interest.
- **Microsoft AIP (Purview):** Tight integration with Azure Information Protection allows Prevent to prompt users whenever their emails are about to breach any existing Microsoft AIP sensitivity labels.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4 com