DATASHEET

mimecast

Incydr Adaptive Controls

Implement a wide variety of adaptive controls to protect data without disrupting productivity or burdening security teams

Your adaptive controls strategy is one of the most critical components to successfully protecting data from insiders. Apply the right level of protection to the right users with a flexible suite of adaptive controls that safeguards data without sacrificing productivity.

Leverage everything from instant blocking to targeted education to stop data exfiltration.

Incydr adaptive controls allow you to:

- Deploy granular blocking to ensure adherence to acceptable use policies.
- Target controls to at-risk users using custom watchlists or deploy organization-wide.
- Deliver ROI from your program by balancing employee productivity with security needs.

The right response control for every insider activity – from mistake to threat.

Communicate	Educate	Block	Contain
Set expectations with users on how they should use data and corporate assets.	Deliver tailored, micro-training videos to correct low-risk actions.	Prevent your highest-risk users from sending data to untrusted destinations.	Ensure insider threats aren't able to damage the business.
Ideal for: • Reducing the frequency and severity of risky file activity. • Ensuring employees know and acknowledge expectations.	**Ideal for:** • Automating response to low-risk events. • Delivering empathetic correction and ensuring accountability. • Changing user behavior to reduce risk over time.	**Ideal for:** • Departing employees, repeat offenders, contractors, & at-risk users. • Protecting sensitive and high-value data. • Ensuring adherence to Acceptable Use Policies. • Supporting security and compliance frameworks.	**Ideal for:** • Active insider threats. • Use during hands-on security investigation.

Feature	Control	Specifications
Communicate	Administrative controls to communicate user expectations.	Mimecast provides communication and policy templates, role-based training and more to help you set expectations with users.
Educate	Automated delivery of short, scenario-based training videos.	90+ proactive, situational, and responsive videos integrated into Incydr. Sent automatically via alert rules or triggered by an analyst. Delivered via email, Microsoft Teams, or Slack.
Block	Block web uploads from high-value sources going to untrusted locations.	Blocks web uploads originating from high-value sources, like SaaS software, network shares, or source code repositories from being exfiltrated to untrusted sources. Includes the option to enable a temporary user-override specific to the user and a given domain.
	Block untrusted web uploads for users on a watchlist.	Blocks web uploads. Includes the option to enable a temporary user-override specific to the user and a given domain.
	Block removable media from mounting for users on a watchlist.	On Windows and Mac. Removable media includes USB, Thunderbolt, SD card, eSATA, and more.
	Block external cloud file sharing for users on a watchlist.	Available for corporate Microsoft OneDrive & SharePoint, Google Drive, and Box. Disables public link creation and sharing to untrusted domains.
	Block paste events to untrusted locations or specific destinations.	Blocks pasting of texts or images into untrusted browsers or specified destination sites. Includes the option to enable a temporary user-override specific to the user and the given domain.
	Tenant-wide blocking.	Blocks USB, applications, personal cloud, upload, and other restrictions to users on a watchlist or tenant-wide —helping reduce policy gaps.
	Temporary allow override option.	Configurable in most blocking scenarios, the “Temporary allow” option allows all or selected users via a watchlist to self-report why they need to move data, with details tracked on the back-end for reporting or audits.
Contain	Revoke cloud file sharing permissions.	Available for corporate Microsoft OneDrive, GoogleDrive, and Box. Allows security analysts to unshare files directly within Incydr.
	Quarantine endpoint.	Using EDR/XDR solutions. Trigger via Incydr integrations with SOAR or through an Incydr Flow.
	Reduce or remove system access.	Using IAM/PAM solutions. Trigger via Incydr integrations with SOAR or through an Incydr Flow.

Customers find Mimecast helps them drive risk reduction in their business in a way that is both more effective and easier to manage than other approaches. Available Content Inspection and integration with Microsoft Information Protection (MIP) tags lets teams automatically bolster protection for PII, PHI, and other sensitive organizational data.

Only with Incydr, you can:

- Get unmatched visibility from day 1 – no policy setup required.
- Send tailored nudges to correct employee mistakes as they happen – driving down events and data risk.
- Speed investigations using agentic AI, with integrated case management and access to file contents.