SOLUTION BRIEF

Complete Email Security with INKY Outbound Mail Protection

Mobile-friendly outbound email protection and policy enforcement.

INKY Phish Fence revolutionized the mail protection user experience with dynamic warning banners giving users specific guidance about each real email they receive. This vastly lowers click-through rates and zero-click malicious actions like paying invoices. Even better, INKY banners require no special client support, so they offer the same user experience on every client and endpoint type.

INKY Outbound Mail Protection carries this revolutionary concept over to outbound email. By communication with users via banners and embedded actions links right in the inbox, INKY Outbound Mail Protection both provides a vastly better mobile user experience and gives you more choices about how a given policy violation should be handled. All in an endpoint- and client-agnostic way.

This solution brief will explain the innovative design ideas behind INKY Outbound Mail Protection and demonstrate ways it will help improve both security and productivity for your email users.

Outbound email workflow, reimagined.

Traditional DLP systems scan outbound emails looking for content that violates established policies. At INKY we identified two key limitations of these legacy solutions we wanted to address in INKY Outbound Mail Protection.

The first limitation is how these systems interact with senders when they spot a policy violation. Most commonly the DLP system simply bounces the mail back as undeliverable, leaving the user to decipher a cryptic non-delivery report (NDR) and try to resend.

Some DLP systems quarantine outbound mail and require use of a clumsy portal to release the offending mail; these portals assume desktop screen sizes and therefore work poorly on mobile – which is where users typically open over 80% of their emails.

Finally, some DLP solutions incorporate Outlook plugins that block outgoing messages client-side, usually displaying an informational pop-up. This improves the UX but comes with the serious disadvantage that it only works with Outlook. We all know that nowadays most users rely on the iOS or Android native mail client for at least some portion of their email workflow, rendering the Outlook plug-in useless. (Neither iOS nor Android allow plug-ins to their mail apps.)

Plug-ins also require IT to strictly version-match endpoint client apps, as any disparity between the plug-in version and the Outlook version breaks the plug-in. And, of course, plugins themselves pose security risks.

INKY Outbound Mail Protection reinvents the interaction between end users and the policy enforcement system with a mobile-first UX design that requires no specific client support. The magic comes from those same dynamic banners and action links that make (inbound) INKY Phish Fence so simple and effective.

SOLUTION BRIEF

Outbound Protection that detects more.

The second limitation of legacy DLP systems we address with INKY Outbound Mail Protection is detection. Traditional DLP relies almost entirely on regular expression (“regex”) matching and context words. To match a credit card, for example, the system predefines a regex matching the relevant number of digits, then couples that a list of terms that must appear near the match, like “credit card”. Specific detectors may include custom validation functions; credit card matches, for example, can be further verified using the so-called Luhn checksum algorithm.

While this regex-in-context approach works well for some kinds of sensitive content, it fails miserably on others. The ICD-10 classification of diseases contains over 16,000 codes with over 25,000 related terms. Regexes deal poorly with large datasets like these, especially when, as with ICD-10, the linkage between a particular code (“J00”) and its companion terms (“common cold”) is established by an enormous table.

And regexes do not work at all for policy violations like sending a phishing link, malicious file, or for catching potential user mistakes like CC’ing the wrong John Smith thanks to an autocomplete failure.

INKY Outbound Mail Protection combines the traditional regex-in-context approach with modern machine learning techniques to both improve accuracy and detect new classes of policy violations.

By combining more sophisticated detection methods with a more flexible user experience, INKY Outbound Mail Protection makes users safer and more productive. It gives admins more control over how a given policy violation is remediated, including first-class support for user education and self-remediation.