Data Protector

INVOICES AND FINANCIAL ATTACHMENTS IN EMAIL

The bad guys are watching the customer's incoming email traffic specifically for invoices and statements that include banking and payment details. After determining the pattern, the incoming emails are intercepted before reaching the intended customer. The attachments within them are modified, and then the emails are sent onward to the intended customer.

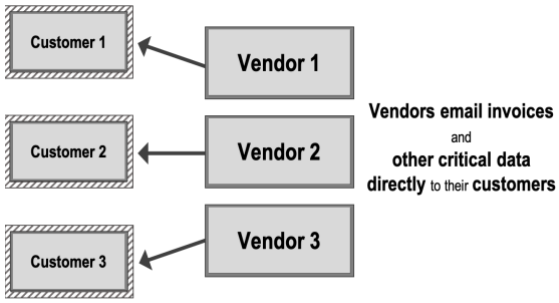

Figure 1. Use case for invoice and financial attachments in email

Using an intermediary service, the email pattern is altered using an email proxy, and the attachments are sorted according to the vendor and their respective customers The Sertainty Data Protector is implemented. The Data Protector provides an automated protection process for the attachments before they are sent to the intended customer.

Note: Each individual customer in this flow implements the Data Protector locally.

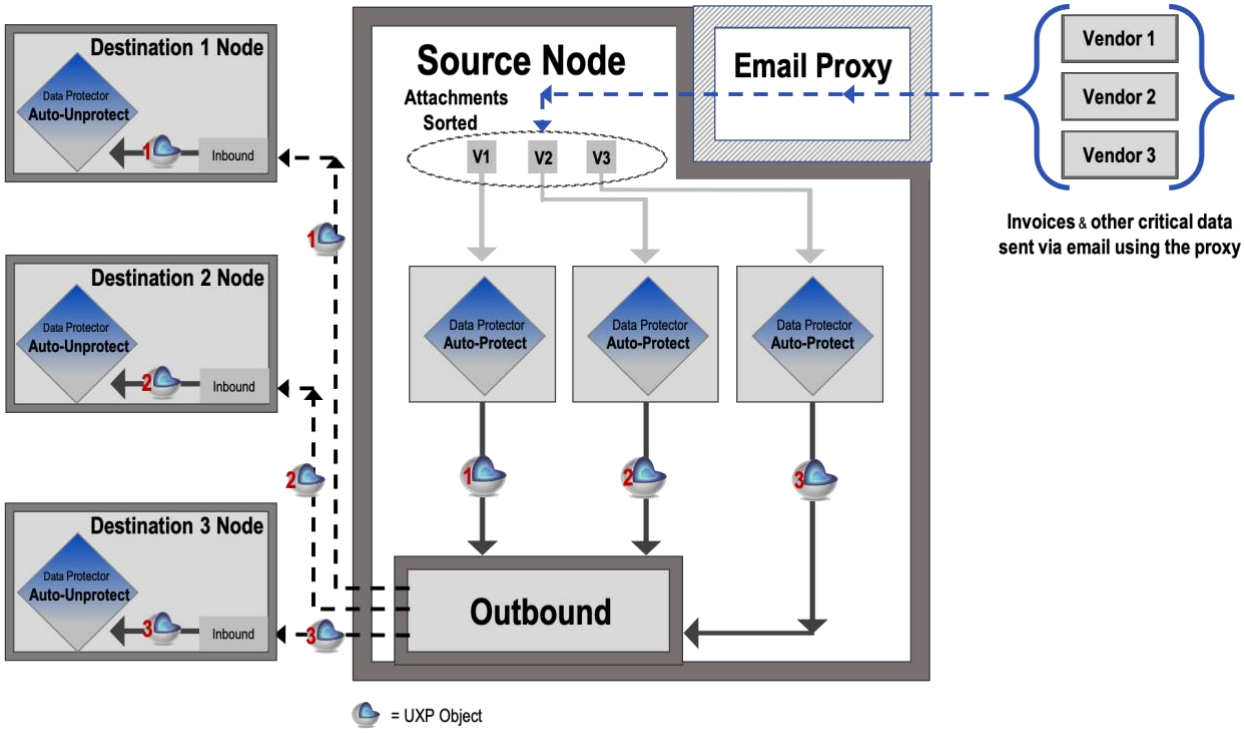

Figure 2. Data Protector workflow for invoice and financial attachments in email

RESTRICTIONS for DATA PROTECTOR SOLUTION

- Data Protector processes can't be significantly disruptive to the Vendor (sender).
- Email is utilized on the front end of the process.

IMPLEMENTATION REQUIREMENTS

- The Source Node (workstation) is owned by the Sertainty Customer.
- A new email proxy is created; the Sertainty Customer owns and manages the new proxy.
- The Sertainty Customer generates a new email address for each of their customers (Destination Nodes).
- Each Vendor is given the new email address that is associated with their respective customers.
- A process for sorting the incoming emails via the proxy and extracting their attachments is designed. This process is based on the intended customer (Destination Nodes).
- Each customer (Destination Node) has a designated folder on the Source Node for implementing a specific automated protection process. This process is managed by the Sertainty Customer. Each folder corresponds to a single Data Protector Auto-Protect Task unique for each recipient.
- Each customer (Destination Node) installs and configures locally a unique Data Protector Destination Node and generates an associated machine UXP Identity.
- The Sertainty Customer creates and manages a transport process to deliver the protected attachments in UXP Object format from the Source Node to its corresponding Destination Node.

DATA PROTECTOR SOLUTION

- The Data Protector is implemented on the Source Node and on each of the Destination Nodes.
- At each Destination Node, a UXP Identity is generated unique to the machine that will be accessing the UXP Objects. The attachments for each Destination are protected on the Destination's behalf using its unique Identity. The protected attachments in UXP Object format can only be authenticated on that machine at the Destination Node.
- Vendors use the new email address to send emails with attached invoices and/or financial statements to their intended customers.
- The new email proxy receives the emails.
- The emails are sorted. The attachments are extracted and placed in the corresponding customer folder on the Source Node.
- The Data Protector facilitates the Auto-Protect process for the contents in each folder using its corresponding Destination Identity associated with the intended customer (Destination Node). The Data Protector places the protected attachment file in UXP Object format in the outbound folder for transport (delivery).
- Each customer receives their protected attachment file in UXP Object format in their local Destination Node.
- The Data Protector facilitates the Auto-Unprotect process. This process is a non-disruptive authentication and extraction process when the UXP Object arrives at its respective location. The process uses the Destination UXP Identity for the Destination embedded in the UXP Object to authenticate
- The attachments are extracted and placed in a designated folder where the customer is able to read them in clear form.

Email us today:
tech-support@sertainty.com