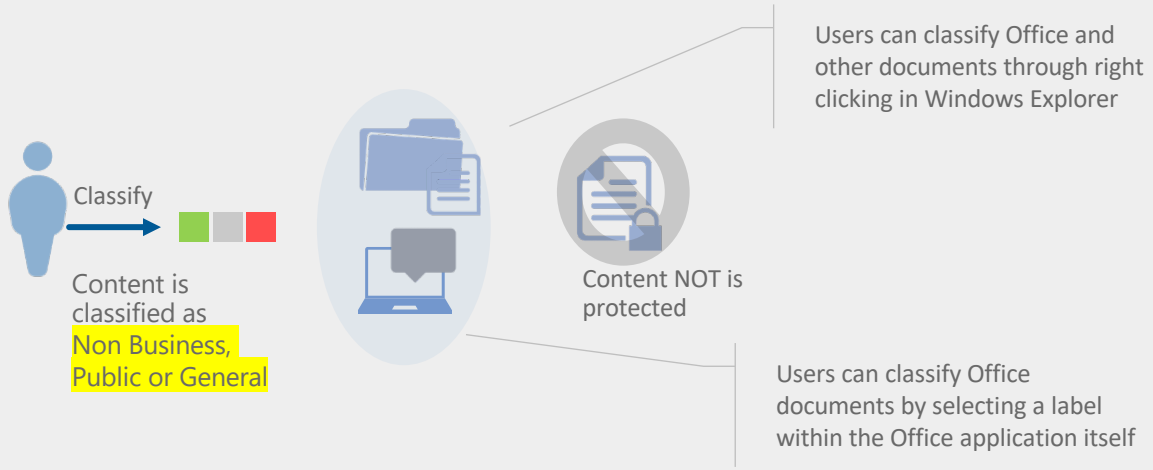
Basic Scenarios to implement Today!

User can classify documents and email

Document classification applies a label in cleartext to the metadata of the document and therefore travels with the document and can be inspected by various DLP engines



Key Benefits

Raising user awareness about security and the impact of accidental leaks of information can lower the risk profile of non malicious users reducing the propensity to accidentally leak information. Setting default classification labels and forcing the user to provide justification when lowering a label places the importance of confidentiality and privacy at the front of minds of users.

Start

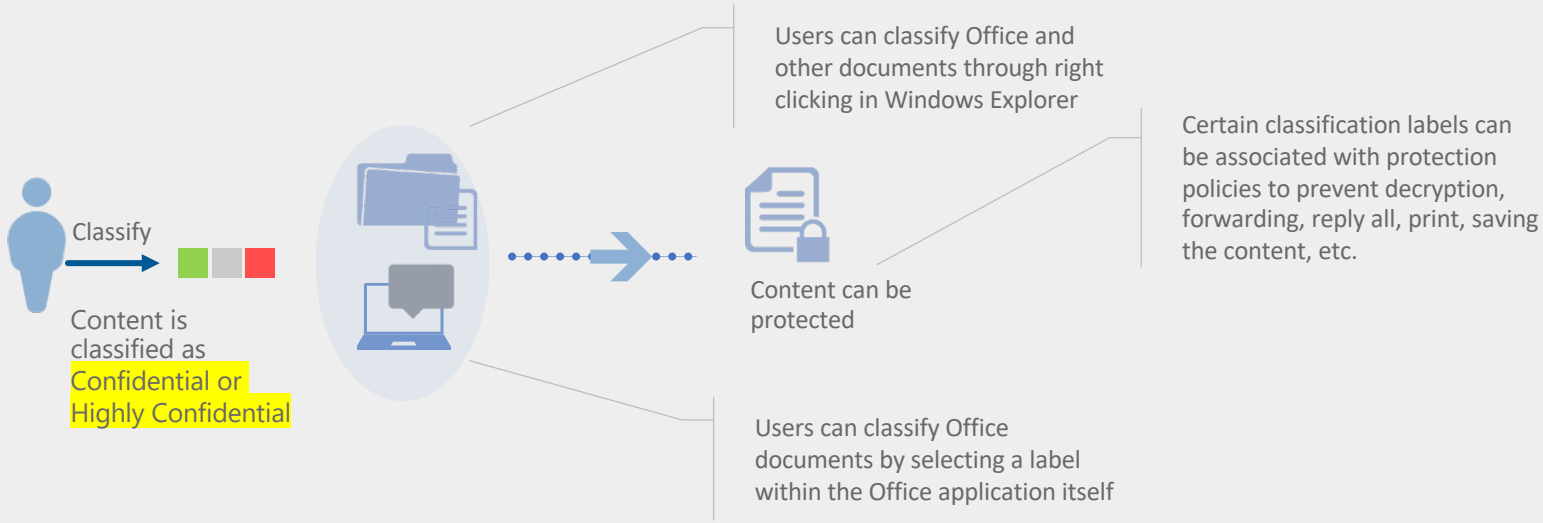
- ✓ Communicating to end users about the importance of confidential information, privacy and trust and showcasing how classification and labelling can assist users to stay compliant
- ✓ Setting default labels so that users become aware of the importance Contoso is placing on classification and labelling
- ✓ Ask users for a justification when lowering the level of a label.

Stop

- ❑ Using "Confidential" in the subject of an email or the title of a document to denote the classification levels. Of course this is fine to do along with the use of an information protection classification label, which will travel with the document wherever it goes.

User can protect content by applying a classification label

Setup labels that are associated with protection templates, applied via Azure RMS



Key Benefits

Users think more carefully about who they are sharing a document with, selecting the correct classification label to enable safer sharing. Content classified for internal use cannot be decrypted and consumed by external users.

Start

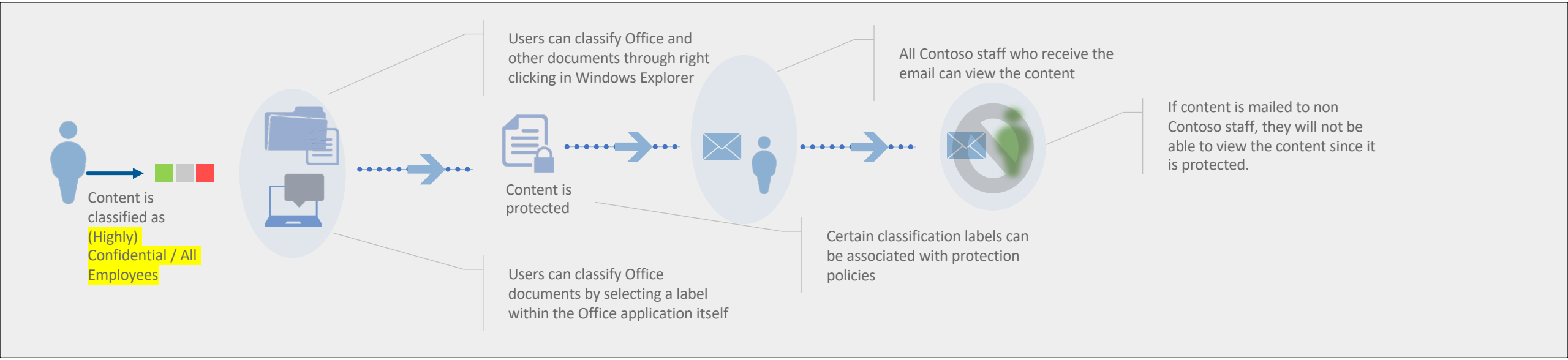
- ✓ Thinking about sensitive business data that could cause business harm if over shared
- ✓ Allowing your users to apply protection easily

Stop

- ❑ Treating all business data in the same way regardless of the business harm, which could be incurred of over-shared.

User can safely email sensitive content to any users internally

Sensitive content is protected and can only be accessed by Contoso staff



Key Benefits

Users think more carefully about who they are sharing a document with, selecting the correct classification label to enable safer sharing. Content classified for internal use cannot be decrypted and consumed by external users.

Start

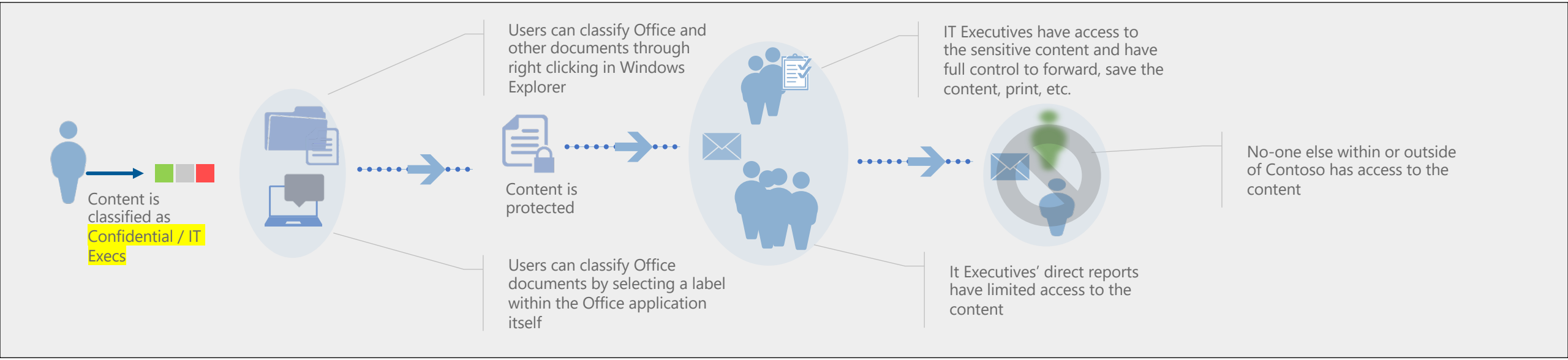
- ✓ Thinking about sensitive business data that could cause business harm if over shared
- ✓ Making it easy for your end user to collaborate securely

Stop

- ❑ Stop recipients of sensitive content via an email from oversharing or deliberately leaking the content outside of the org.
- ❑ Treating all business data in the same way regardless of the business harm, which could be incurred of over-shared.

Executives can safely send sensitive content to other executives and direct reports with limited access for direct reports

Executives lower the risk associated with sharing sensitive content



Key Benefits

Create specific and niche *scoped policies* that apply only to specific departments. Only users within that department will have access to the scoped policy. This allows for custom department level classifications, which do not impact on the overall usability of the classification system (i.e. users only see labels which have meaning to them).

Start

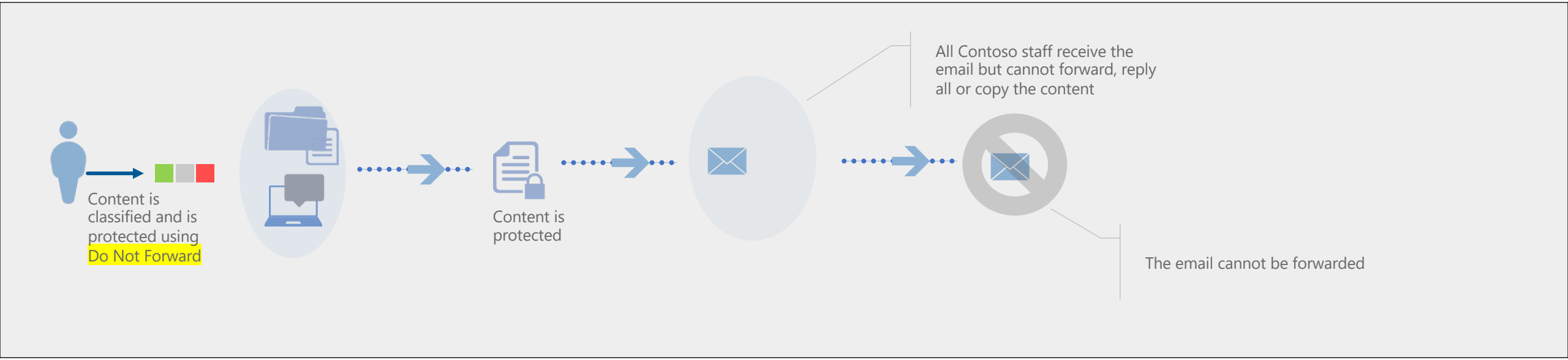
- ✓ Thinking about sensitive business data that could cause business harm if over shared
- ✓ Showing immediate value for executives in your company

Stop

- ❑ Stop recipients of sensitive content via an email from oversharing or deliberately leaking the content outside of org.
- ❑ Treating all business data in the same way regardless of the business harm, which could be incurred of over-shared.
- ❑ Confusing users with too many labelling options that do not apply to them

Ability send company wide communications to all employees with email restrictions such as Do Not Forward.

Can reduce the risk associated with sensitive corporate communications



Key Benefits

Communicating widely and internally in a secure way which makes sure that only Internal employees can read those communications and cannot even forward those communications to anyone else but still allow them to replay.

Start

- ✓ Thinking about sensitive business data that could cause business harm if over shared
- ✓ Communicate wide announcements in a secure and protected way

Stop

- ❑ Stop recipients of sensitive content via an email from oversharing and leaking the content outside of org.
- ❑ Treating all business data in the same way regardless of the business harm, which could be incurred of over-shared.