Managing Information Security and Data Compliance in Nutanix Files

NUTANIX READY • AHV •

1 Identify Red Flag Risks

Identify Risks:

Identify compliance and security risks, sensitive content types, and access permissions for users and groups.

Involve Stakeholders:

Bring stakeholders such as senior management, IT, information security, privacy and compliance officers, human resources and business units together to conduct a risk assessment and to suggest policies for the organization.

2 Establish the Security Strategy

Publish a Data Security & Compliance Strategy:

Determine what areas of risk to address and align these with the business strategy. Use stakeholder knowledge to define your policies and procedures against the business strategy. Automate policy enforcement and proactively mitigate risk with NC Protect™.

3 Design Policies, Categorize Users & Deploy

Design Policies:

Define policies, business rules, policy officers, access rules, notifications and workflows using NC Protect. The same business rules and policies can be applied to a Nutanix Files environment to centrally manage content security.

Categorize Users:

Use available resources to identify your users without defining new groups i.e. AD attributes, User Profile Services, company databases, address books, and extract information such as department, employment status, clearance levels, team membership, country, and citizenship.

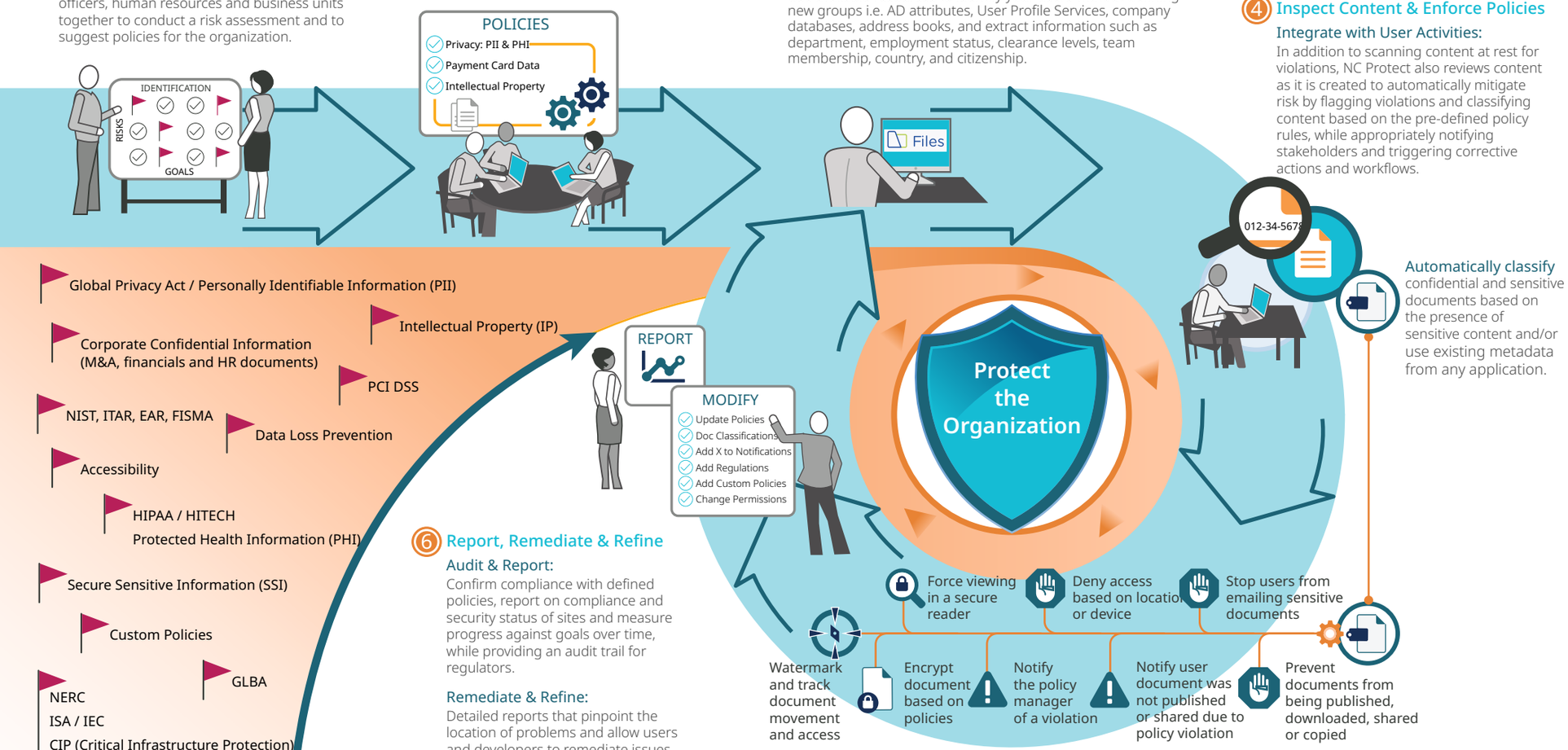
Deploy:

Deploy NC Protect to scan and classify content to automatically detect issues, dynamically apply permissions, and take corrective actions to prevent breaches and mitigate risk.

4 Inspect Content & Enforce Policies

Integrate with User Activities:

In addition to scanning content at rest for violations, NC Protect also reviews content as it is created to automatically mitigate risk by flagging violations and classifying content based on the pre-defined policy rules, while appropriately notifying stakeholders and triggering corrective actions and workflows.



Automatically classify confidential and sensitive documents based on the presence of sensitive content and/or use existing metadata from any application.

- Global Privacy Act / Personally Identifiable Information (PII)
- Intellectual Property (IP)
- Corporate Confidential Information (M&A, financials and HR documents)
- PCI DSS
- NIST, ITAR, EAR, FISMA
- Data Loss Prevention
- Accessibility
- HIPAA / HITECH
  Protected Health Information (PHI)
- Secure Sensitive Information (SSI)
- Custom Policies
- GLBA
- NERC
- ISA / IEC
- CIP (Critical Infrastructure Protection)

Discovery:
- Policy
- Copyright
- Inappropriate Content

5 Dynamically Secure Content & Apply Restrictions

Secure:

Restrict access to, encrypt, force viewing in a secure reader, apply dynamic watermarks, and prevent the publishing of content based upon the presence of sensitive or non-compliant information.

Control:

Workflows can be used to remediate compliance issues and/or task the proper individual(s) in the organization to review and potentially quarantine, remove, classify or re-classify the content. Central workflow also allows policy officers to override approvals, user actions, and adjust classifications.

Track & Monitor:

NC Protect tracks and monitors the movement of confidential and sensitive documents; including who views, prints, and emails the documents.

6 Report, Remediate & Refine

Audit & Report:

Confirm compliance with defined policies, report on compliance and security status of sites and measure progress against goals over time, while providing an audit trail for regulators.

Remediate & Refine:

Detailed reports that pinpoint the location of problems and allow users and developers to remediate issues quickly. Accurate reporting also allows policy managers to modify policy and workflow rules based on user interaction and compliance trends.

Tips for Successful Information Security & Compliance

- Ensure your information security and compliance strategy aligns with the organization's overall strategy.
- Change your security approach - instead of defining groups, refine user attributes and claims.
- Have key stakeholders review the strategy regularly for changes, new policies and laws.
- Implement a solution to continuously audit content and user actions, detect violations and enforce policies to maintain data integrity, security and compliance in Nutanix Files, Office 365 apps, Dropbox and Windows file shares.

Protect Your Data with Dynamic Discovery, Classification & Security

- **INSPECT CONTENT**
  Scan content at rest and in motion to detect non-compliant data and violations.
- **CLASSIFY**
  Classify data at the file level based on pre-defined policies or users can manually classify data using pre-defined values.
- **RESTRICT ACCESS**
  Set file permissions based on metadata and utilize user claims in combination with item metadata to dynamically filter the content displayed in list views, search results or when using an item URL without changing item permissions.
- **ENCRYPT**
  Further secure sensitive content by encrypting it immediately so only properly credentialed users will be able to read the content—whether inside or outside of Nutanix Files.
- **CONTROL DISTRIBUTION**
  Prevent users from publishing, distributing, or emailing confidential and sensitive documents. Stop users from adding non-compliant content. Trigger workflows to alert users to fix issues, get manager approvals and quarantine documents.
- **TRACK**
  Track and monitor the movement of confidential and sensitive documents; including who views, prints, and emails the documents.

NUCLEUS CYBER
www.nucleuscyber.com