Wissen Baum

Key Solutions for Data Loss Prevention

DLP in Nutshell

WHAT

DLP is a set of technology tools and processes that ensure sensitive data is not stolen or lost.

HOW

DLP detects and protects your organization's sensitive data by:

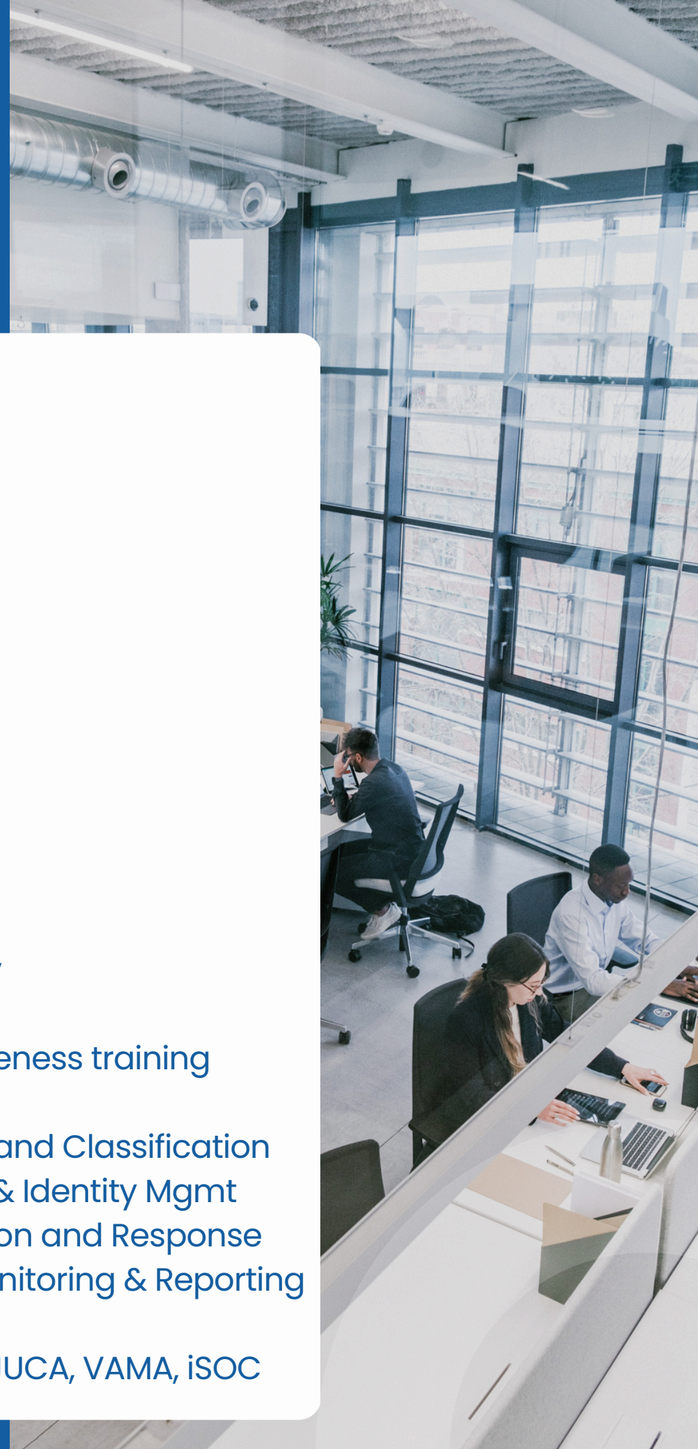
- Scanning data in motion, in use and at rest
- Identifying sensitive data that requires protection
- Taking remedial action—alert, prompt, quarantine, block, encrypt
- Providing reporting for compliance, auditing, forensics and incident response purposes

WHY

Accidental (i.e. employee error) or malicious actions (i.e. cyber criminal breach) put your organization's data at risk.

DLP Solutions Alignment

At Wissen Baum DLP solutions to secure data across Endpoints, Networks, and Cloud environments with Policy, Pepole, and Processes.



	Endpoint DLP	Network DLP	Cloud DLP
Area	• Desktop • Laptop • Mobile phones • Tablets • Removable Storage (CD's, DVD's) • Portable Storage (USB, Hard Drives, etc.)	• Firewall Logs • Internal External Traffic • Vulnerable Port Monitoring • Create signature for Day Traffic • Firewall Rule Allow/Deny • Source & Destination IP, Port traffic • Non Business Hour activity monitoring	• Microsoft Azure • AWS • Google Clous • Amazon S3 • Office 365 • iOS, Android • G Suite
Policy	• Endpoint DLP Policy	• Network DLP Policy	• Cloud DLP Policy
People	• Endpoint DLP awareness training	• Nework DLP awareness training	• Cloud DLP awareness training
Process	• Data Classification • Data encryption • Data Monitoring • Incident Response & Reporting	• Policy Development • Monitoring and Analysis • Incident Response • Network Traffic Analysis Report	• Data Discovery and Classification • Access Control & Identity Mgmt • Incident Detection and Response • Compliance Monitoring & Reporting
Product	• ASSETIE, NETRA, JUCA, iSOC	• ASSETIE, NETRA, VAMA, JUCA , iSOC	• ASSETIE, NETRA, JUCA, VAMA, iSOC

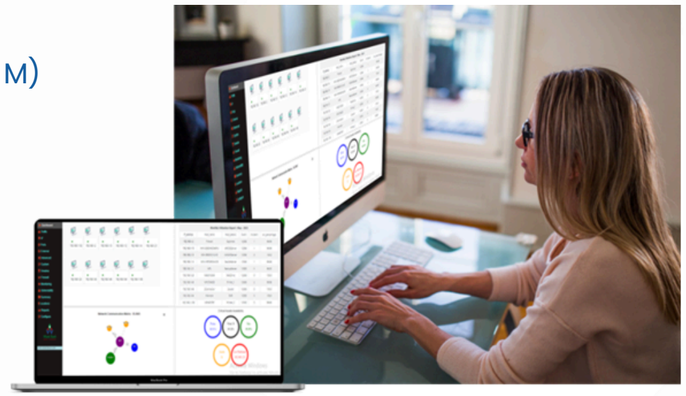
Our Product Alignment for DLP

Area	Locations	Public	Process	Technology	WBES Align
Data at Rest	• Databases • Local computers • Controlling access ports (e.g., USB drives) • Intranet/internal websites • Internal directory shares • Organizational data and email archives • Mobile devices (e.g., laptop at home) • CDs and DVDs • Printed/hard-copy reports • Fax machines • Copiers • File cabinets	• Security Admins • End Users • IT Staff • Compliance Officers	• Data Classification • Data Retention • Secure Disposal • Data Backup • Access controls and permissions • Implement encryption for data stored • Deploy mobile device management • Monitor System event Logs • Implement Document Handling Policy • Monitor Fax Logs • Implement Authentication mechanism • Implement Physical Security Measures	• Data Encryption • Access Controls • Data Masking • Data Loss Policies • Data Classification • Data Backup • Mobile Device Mgmt • Data Encryption • Data Loss Policies • Secure Fax Transmission • Secure Copying • Physical Security	• ASSETIE • NETRA • JUCA • iSOC • Awareness Training
Data in Motion	• Email (organization and personal) • Web/Internet • File transfers • Data sharing • Social media (e.g., Facebook, Twitter, etc) • Instant messaging (IM) • Blogs (Internet and intranet) • Website hostings • Paper mail with sensitive data	• Security Admins • IT Staff • Compliance Officers	• Data Loss Policies • Acceptable Use Policies • Secure Protocols • Secure Collaboration • Employee Training and Policies • Implement session management • Monitoring and Reporting • Enable SSL/TLS encryption • Secure Document Handling	• Email Encryption • SSL/TLS • VPN • IAM • Data Loss Policies • Encryption • Data Loss Policies • SSL/TLS • Secure Courier Services	• ASSETIE • NETRA • VAMA • iSOC • Phishing • Awareness Training
Data in Use	• Workstation • Server • Mobile device/endpoint	• Security Admins • IT Staff • Compliance Officers	• User Activity Monitoring • Data Integrity Monitoring • Mobile Security Policies	• Endpoint Security • Firewall Rules • Mobile Application Management	• ASSETIE • JUCA • NETRA • iSOC • Awareness Training

Our Product Solutions

ASSETIE

- Asset Real Time Monitoring
- Asset Discovery
- Asset Utilization Report(D, W, M)
- Asset Notification

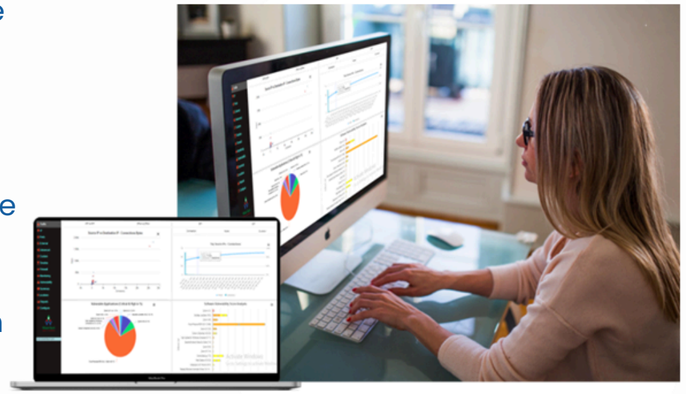


NETRA

- Maintenance, Monitoring and Analysis of Audit Logs
- Environmental Controls
- Network Management and Security
- Secure Configuration
- Data Leak prevention strategy
- Risk based transaction monitoring
- Port Monitoring

VAMA

- Application security life cycle (ASLC)
- Vendor risk management
- Preventing execution of unauthorized software
- Patch/Vulnerability & Change Management
- Vulnerability assessment & Penetration Test & Red Team Exercises



iSOC

- Audit Log settings
- User Access Control Management
- User / Employee/ Management Awareness
- Authentication Framework for Customers
- Anti-Phishing
- Incident Response & Management
- Customer Education Awareness
- Secure mail and messaging systems
- SME Support

Wissen Baum

THANK YOU

FOR YOUR ATTENTION

April 2024

sales@wissenbaum.com

www.wissenbaum.com