Netwrix Auditor
Data Discovery & Classification

Know Your Data. Protect What Matters.

Dave Matthews
Systems Engineer
Dave.Matthews@netwrix.com

Pradeep Kapil
Country Manager - India
Pradeep.Kapil@netwrix.com

Welcome

- All attendees are on mute
- Please ask questions
- Answers will be provided during Q&A at the end of the session
- A copy of slides and webinar recording will be available
- Up to 60 minutes

Agenda

- Briefly about Netwrix Corporation
- Our last 4 years in India
- What's New in Netwrix Auditor 9.8
- Product Demonstration
- How **Data Discovery and Classification Edition** can add value to your organization
- Netwrix Customer Centric Approach
- Q&A

Our Last 4 Years in India

- More than 70+ customer
- Growth of 135% + in last 4years
- 95% +Retention rate
- Wipro & HCL with more than 1,50,000 ++ Users are among the biggest wins we had in India

Why We Are Here

Data Growth

Increasing data generation ceases the ability to identify data that needs protection

DATA

has become the focal point of security efforts

Hybrid Infrastructures

Maintaining unified data security controls is a challenge

Increasing Threats

Breaches are becoming more frequent and receive more publicity

Evolving Compliance

New regulations impose stricter data confidentiality and privacy requirements

Board Visibility

Executives are more aware and want cybersecurity spending to be justified

How Netwrix Can Help

Netwrix provides a **data security platform** that empowers organizations to accurately identify **sensitive**, regulated and mission-critical **information** and apply access controls consistently, regardless of where the information is located.

It enables you to **minimize the risk** of data breaches and **ensure regulatory compliance** by proactively **reducing the exposure** of sensitive data and promptly **detecting policy violations** and suspicious user behavior.

What is new in 9.8: available in May 2019

New: Netwrix Auditor for Windows Servers

- remediate security gaps on your critical Windows servers
-

New: Netwrix Auditor for SharePoint

- reduce the exposure to threats in SharePoint

New: Risk Assessment Dashboard

- stay informed on your infrastructure configuration and SharePoint data access with the new metrics

New: Netwrix Auditor for Network Devices

- audit access and configuration changes on Juniper, Palo Alto and SonicWall network devices

New: Netwrix Auditor for User Sessions

- analyze user activity on critical servers using the report on user sessions

New: Search and Alerts

- Search and alert on activities performed outside the working hours or by users not in whitelisted group

New: Integration

- use a new add-on for integration with ConnectWise Manage system; simplify integration with SIEM solutions with a universal add-on for Event Log export

New: Netwrix Auditor Data Discovery and Classification

- updated built-in taxonomies (PII and GDPR)

Netwrix Roadmap

User and Entity Behavior Analytics

- Machine learning and customizable rules
- Detection of deviations from past behaviors and peer group
- Focus on compromised accounts, elevation of privilege, and data exfiltration

Wider Scope of State-In-Time Data

- Permission audit and configuration reporting for Office 365, Exchange Server, SQL Server and other systems

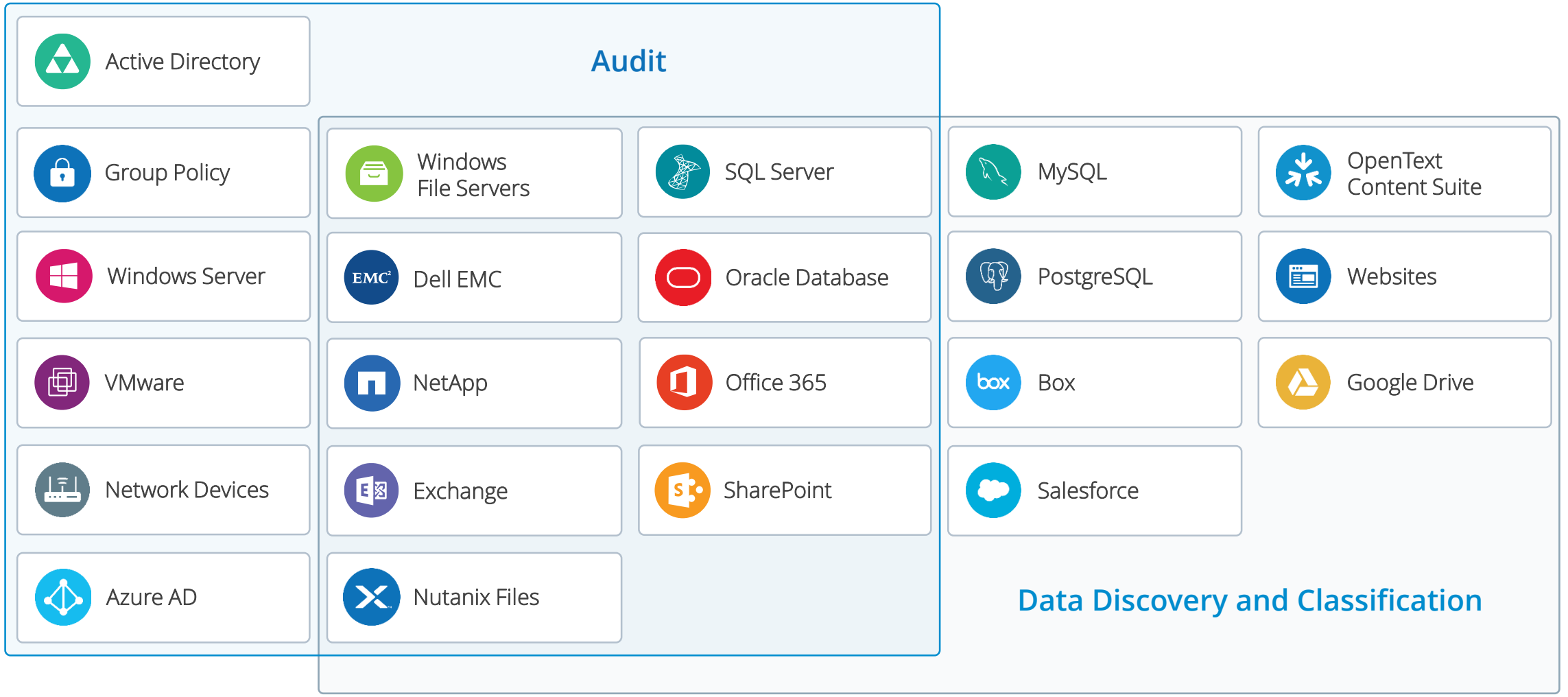
Broader Support for Enterprise Environments

- Scalability through distributed deployment
- Data-in and data-out add-ons and integrations

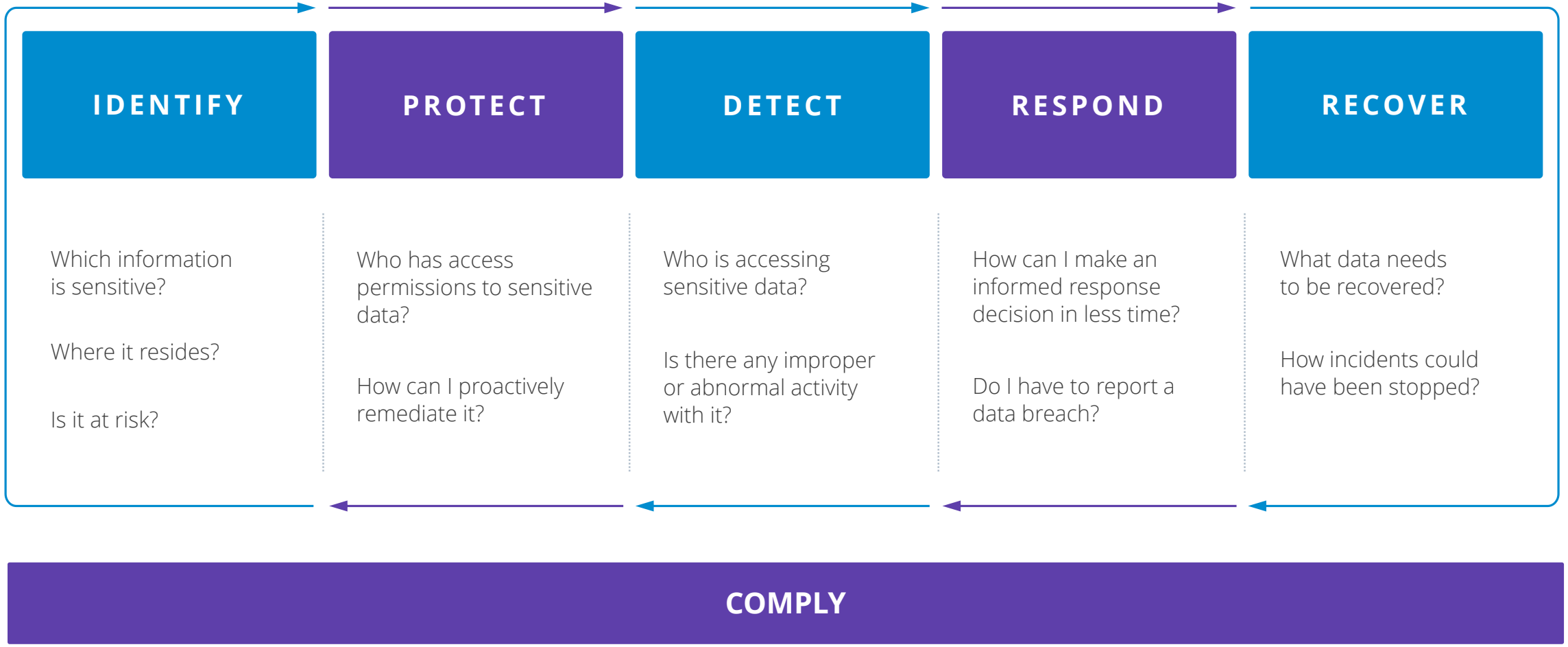
Audit-as-a-service

- Development of SaaS delivery model

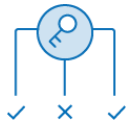
Netwrix Data Sources



Data Security Challenges Resolved by Netwrix



Identify



Prioritize the security of sensitive data across multiple data silos

Identify overexposed sensitive data

Assess data and infrastructure security risks

Structured data sources

- Oracle Database
- SQL Server
- **MySQL**
- PostgreSQL
- **Salesforce**

Unstructured data sources

- Windows File Servers
- Outlook data files
- Dell EMC
- **OneDrive for Business**
- NetApp
- Nutanix Files
- SharePoint, SharePoint Online
- **Box**
- Exchange, Exchange Online
- Google Drive

Protect

Automatically quarantine sensitive data to reduce the risk of a breach or loss

Immediately lock down sensitive data that is overexposed

Streamline regular privilege attestations

Redact sensitive information based on corporate policy

Increase the precision of your DLP solution

Detect

Establish strict accountability over the use of privileged accounts

Stay on top of privilege escalation

Detect compromised accounts and malicious insiders

Keep third-party activity under close scrutiny

Detect ransomware attacks in progress

Respond

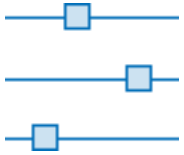
Streamline incident investigation

Reduce the mean time to respond

Determine and report the severity of a data breach

Recover

Understand the value and sensitivity of data to plan information recovery processes

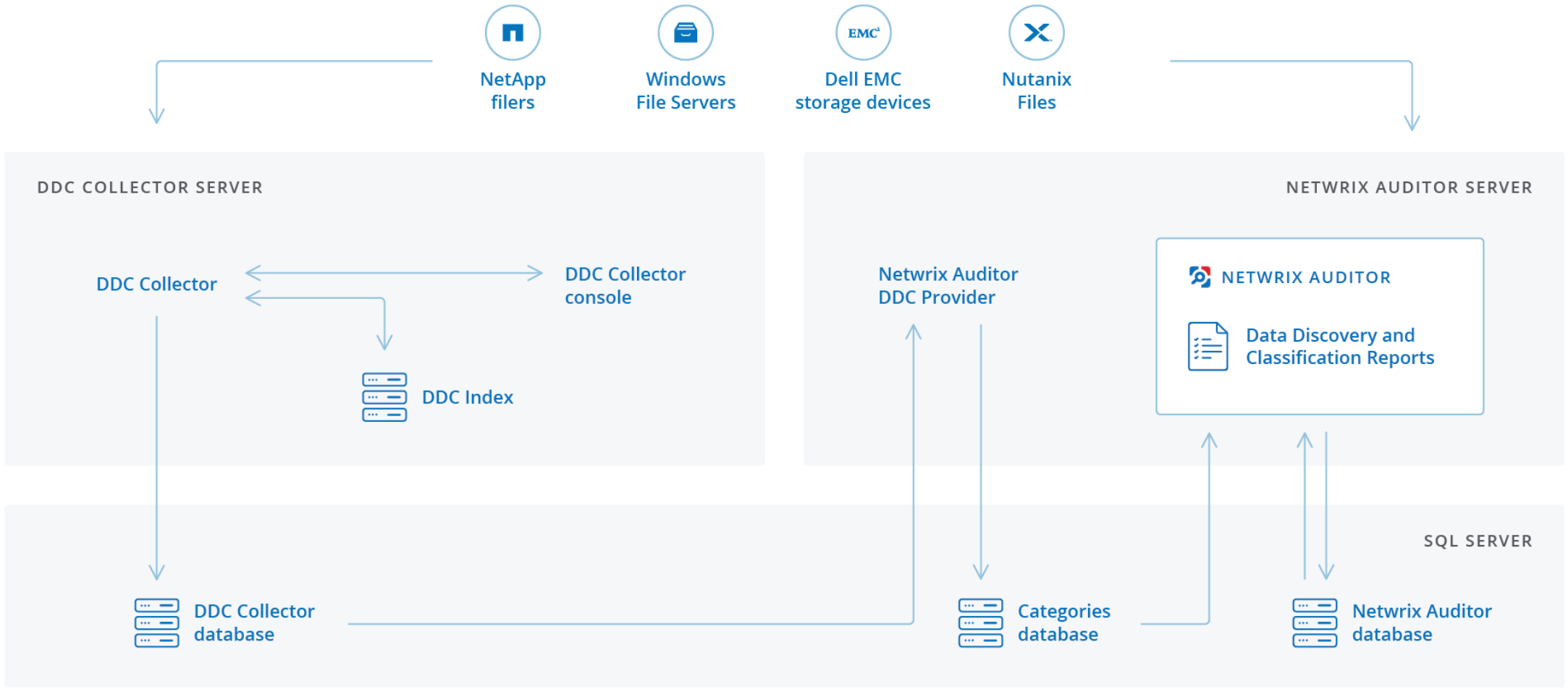


Get back up and running faster by prioritizing the recovery of key data

Incorporate lessons learned into your data security strategy

Demonstration

Netwrix Auditor and Data Classification Architecture



Data Discovery and Classification Benefits

Prioritize your data protection efforts

Identify the shares with the highest concentrations of sensitive data and detect any PII, PCI, PHI or IP that surfaces outside of a secure location, so you can respond appropriately.

Minimize the risk of a data breach

Verify that access rights to sensitive data are aligned with corporate policies and applicable regulations, and involve data owners in determining who should be able to access it.

Detect threats to your sensitive data

Get the full context around activity with protected information and ensure that user actions that threaten this data, such as improper permissions changes, are captured and reported on.

Prove your security controls are effective

Demonstrate to auditors that you know exactly where protected data resides and quickly provide evidence that only eligible employees can read, modify, share or delete your critical files.

Accommodate new security regulations

Easily discover the data that GDPR and other compliance regulations require you to protect, and establish a solid foundation for complying with future data security requirements.

Determine the severity of a data breach

Analyze how much data a malefactor had access to and which pieces of data were actually viewed, modified or deleted, so you can notify all affected parties.

What Makes Netwrix Auditor's Data Discovery and Classification Unique

- **High precision**

  Delivers accurate results so customers can focus on protecting their truly valuable data instead of wasting precious time sifting through false positives.

- **Powerful search of sensitive data**

  Empowers customers to quickly hone in on files containing personal data related to an individual, to comply with the GDPR's "right to be forgotten" — without any downtime or having to create new rules.

- **Reusable index**

  Eliminates the need to re-index the entire data repository whenever a classification rule is added or changed.

- **Non-intrusive architecture**

  Operates in agentless mode and does not interfere with your file system by updating content metadata. Instead, all index and classification information is collected, analyzed, stored and updated on a separate server.

Netwrix Customer Centric Approach

- India Technical support number +91-124-431-8-803
- 2 Sales Engineer + 3 L1 resource to support APAC region
- Half yearly product training session through partners
- At least 2 customer webinar from Netwrix experts
- Improved Customer portal – Video tutorials on Netwrix Configuration and best practices
- Netwrix Certification and Trainings

Questions
?

Thank You!

Dave Matthews
Systems Engineer
Dave.Matthews@netwrix.com

Pradeep Kapil
Country Manager - India
Pradeep.Kapil@netwrix.com