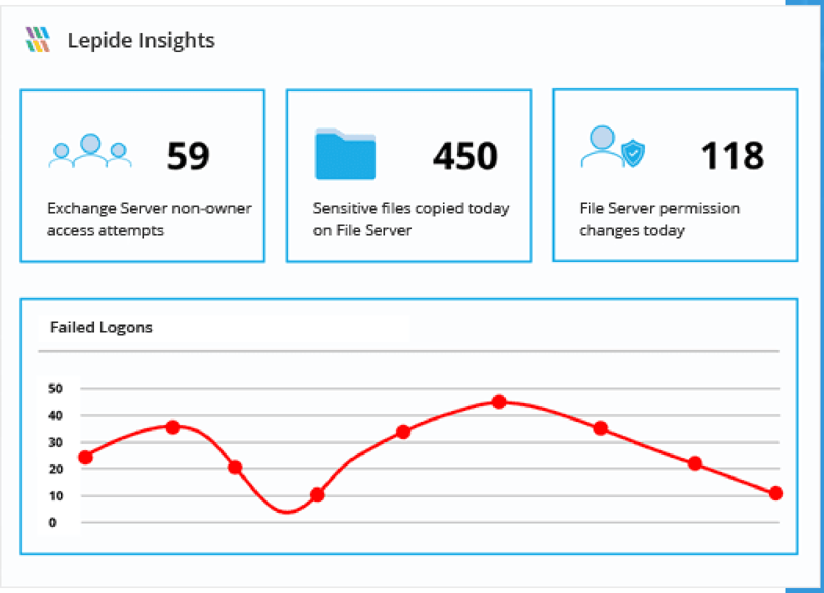
Lepide

DATA SECURITY PLATFORM

Market leading coverage, risk reduction, behavioral analysis and more. Protect your data, meet compliance and react to threats with the Lepide Data Security Platform.

Discover, Analyze and Protect Sensitive Data

Lepide leverages Data-Centric Audit & Protection for enterprise-level insight into your data and the surrounding systems, whether on-premise or in the cloud. We help all members of the IT and security teams get value, from fixing technical, point problems to proving that your data is secure for compliance audits.



Lepide Insights

59 Exchange Server non-owner access attempts

450 Sensitive files copied today on File Server

118 File Server permission changes today

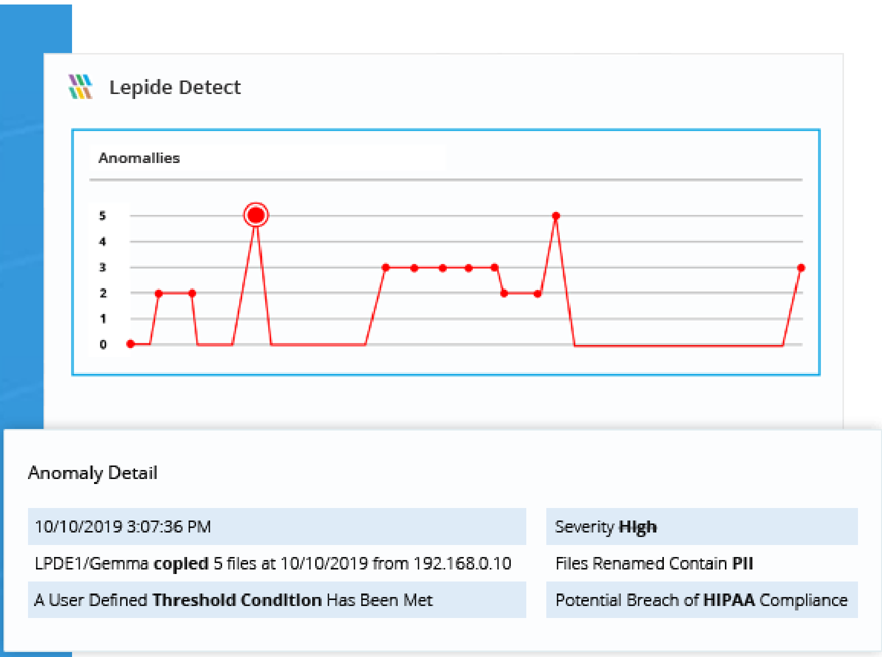
Failed Logons

Track User Interactions with Data

Audit, report and alert on changes being made to sensitive data in your hybrid environment.

Roll back unwanted changes and restore deleted objects to maintain system integrity.

Track any changes and modifications users are making to critical files and folders.



Anomaly Detail

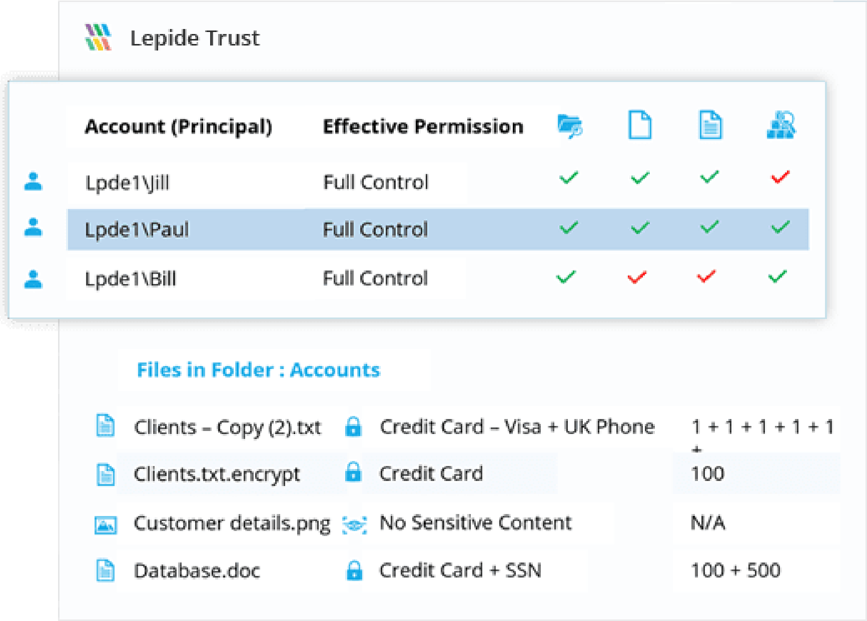
10/10/2019 3:07:36 PM	Severity **High**
LPDE1/Gemma **copied** 5 files at 10/10/2019 from 192.168.0.10	Files Renamed Contain **PII**
A User Defined **Threshold Condition** Has Been Met	Potential Breach of **HIPAA** Compliance

Detect and React to Threats with Automated Response

Machine Learning backed anomaly spotting technology will allow you to determine when one of your users becomes an insider threat.

Hundreds of threat models, tailored to specific data security threats, generate real time alerts when the security of your data is in jeopardy.

Automated threat responses can be triggered to perform any number of threat mitigation actions, including shutting down an affected computer or server or locking out the user in question.



Lepide Trust

	Account (Principal)	Effective Permission				
👤	Lpde1\Jill	Full Control	✓	✓	✓	✓
👤	Lpde1\Paul	Full Control	✓	✓	✓	✓
👤	Lpde1\Bill	Full Control	✓	✓	✓	✓

Files in Folder : Accounts

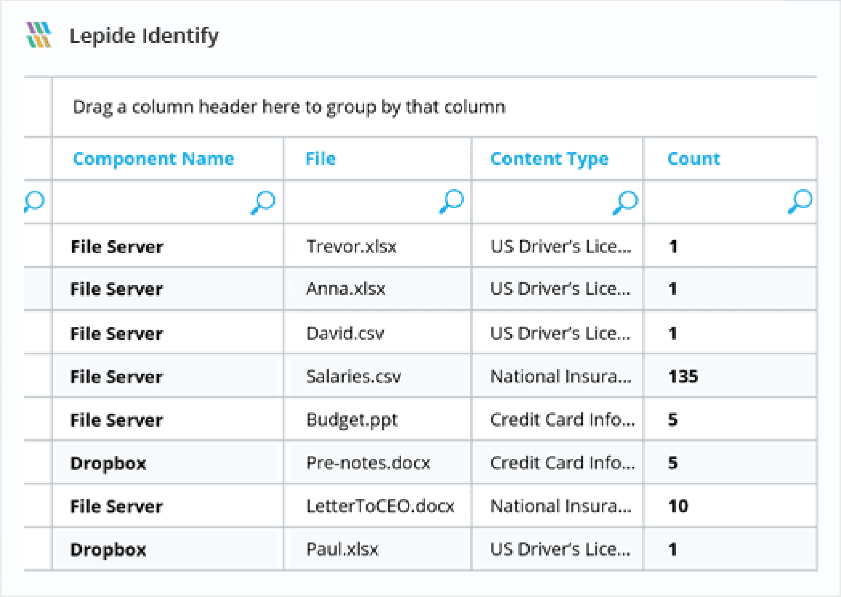
Clients – Copy (2).txt	🔒	Credit Card – Visa + UK Phone	1 + 1 + 1 + 1 + 1 + 1 +
Clients.txt.encrypt	🔒	Credit Card	100
Customer details.png		No Sensitive Content	N/A
Database.doc	🔒	Credit Card + SSN	100 + 500

Spot Excessive Permissions and Govern Access to Data

Report on who has access to your most sensitive data and how they were granted that access.

Specific reports for users with excessive permissions enable you to spot which users are most likely to be insider threats.

Maintain your zero-trust policy by spotting when permissions change and reversing them.



Lepide Identify

Drag a column header here to group by that column

Component Name	File	Content Type	Count
File Server	Trevor.xlsx	US Driver's Lice...	1
File Server	Anna.xlsx	US Driver's Lice...	1
File Server	David.csv	US Driver's Lice...	1
File Server	Salaries.csv	National Insura...	135
File Server	Budget.ppt	Credit Card Info...	5
Dropbox	Pre-notes.docx	Credit Card Info...	5
File Server	LetterToCEO.docx	National Insura...	10
Dropbox	Paul.xlsx	US Driver's Lice...	1

Discover and Classify Your Most Sensitive Data

Automatically scan, discover and classify data at the point of creation to help you stay on top of where your sensitive data is located.

Remove false positives with proximity scanning technology. This helps to improve the accuracy even further than most classification solutions.

Categorize and score data based on compliance, risk, occurrence, monetary value, and more to stay on top of your most sensitive data.

Some Key Features

Hundreds of Threat Models

Execute automated responses when the solution detects ransomware, malware, insider threats and more.

Real Time Alerts

Get alerts on user behavior and changes delivered to your email or mobile in real time.

Intelligent SIEM Integration

Seamlessly integrate with SIEM solutions to add context to reports and streamline your threat response/investigations.

Enterprise Scalability

Divert resources to individual pieces of functionality as required to ensure smooth and reliable scalability.

Universal Auditing

Best in class platform coverage for on-premise and the cloud through syslog and restAPI integrations.

AI/Machine Learning

The Platform gets smarter the longer it runs, detecting and reacting to threats more accurately.

Data Stores (On-Premise)

Active Directory

Audit changes to AD, including before & after values, with the ability to rollback changes and recover objects.

Group Policy

Track and rollback all changes to Group Policy objects as well as the policies within, including local policies, password policies.

Exchange Server

Audit changes to Exchange objects and attributes in AD, the configuration, security, and use of Exchange, as well as mailbox access.

SQL Server

Monitor and report on all logins, administrative changes, and client use of SQL Server instances.

SharePoint Server

Audit all use and changes to farms, servers, sites, storage, security, and content.

File Server / NetApp Filer

Track access attempts and changes to your files and folders with granular who, what, when and where information. Understand when your users are copying your files to help maintain security and integrity of data. Real time alerts, threshold alerts and pre-defined reports for all security and compliance needs.

Data Stores (Cloud)

Azure AD

Track’s configuration changes, monitor privileged users/groups and provides a full audit trial of every user authentication.

Dropbox

Track changes to file and folders, insight into Dropbox link sharing, monitor permissions to critical data.

Exchange Server Online

Audit changes to Exchange objects and attributes in AD, the configuration, security, and use of Exchange, as well as mailbox access.

OneDrive for Business

Track file and folder level changes, track security groups and configuration changes.

SharePoint Server Online

Audit all use and changes to farms, servers, sites, storage, security, and content.

MS Teams

Monitor User Activities in Microsoft Teams. The collaboration that MS Teams provides creates unique security challenges that many solutions cannot cope with. Lepide enables you to get real visibility over how your users are engaging with Teams and when sensitive data is being shared, to help you respond to threats and prevent breaches.

Data Stores (Cloud) Continued

G Suite

Track changes made to data and administrative changes (such as privilege escalation) made to the surrounding applications in G Suite.

Amazon S3 Auditing

Audit Amazon S3 Buckets to determine who’s accessing data within the buckets, and who is making configuration changes.

Universal Auditing

Configure Lepide to monitor any platform through either restAPI or Syslog including Box, IBM, Rackspace, Linux, EMC, VMWare, Network Devices and more.

Out of the box templates will help to get you started with proprietary storage and infrastructure such as Box, Coda, Ignyte, Launchdarkly and Open Drive