DATA PROTECTION & SECURITY

Who's accessing your data and how

THE PROBLEM

Lack of data visibility across fragmented and complex environments

Data has become one of the most valuable assets for modern organizations, but its protection remains a challenge. With the growing adoption of cloud services, complex data ecosystems, and remote work environments, sensitive data is now dispersed across various networks, endpoints, and applications. This widespread distribution makes it challenging to keep track of data, detect potential exposures, and respond quickly to threats. Traditional data protection tools are often limited to specific environments and lack a holistic view, leaving organizations vulnerable to misconfigurations, unauthorized access, and inadvertent data leaks.

AT A GLANCE

Types of Data

- PII - Personally Identifiable Information
- Financial Data
- Intellectual Property
- Health Data
- Operational Data
- Customer and Transaction Data
- Strategic Decisions supporting material

Common Locations

- Legacy systems on premise
- Cloud Storage and Applications
- Partner and Vendor transaction systems
- SaaS Applications

KEY CHALLENGES

Limited Visibility into Data-in-Transit

Many organizations lack real-time insight into how data moves across networks, both internally and externally. This limited visibility into data-in-transit makes it challenging to monitor sensitive information, detect unauthorized transfers, and prevent data leakage in real time.

Data Silos and Fragmentation

Sensitive data often resides in multiple, disconnected systems and platforms, from on-premises storage to cloud services and third-party applications. This fragmentation creates blind spots where data can be mishandled, misconfigured, or accessed without the organization's awareness.

No single pain of glass to monitor potential exposure

Without a pervasive view of data at rest and in transit, organizations struggle to identify potential exposure points, such as unencrypted data transfers or insecure network paths. This lack of visibility into where data might be at risk makes it difficult to apply consistent security measures.

Insufficient Monitoring of User-Data Interactions

Monitoring user/data interactions is critical for maintaining data security, as unauthorized or abnormal user behavior can be an early indicator of potential data breaches, insider threats, or policy violations. However, many organizations struggle with gaining clear visibility into how users interact with data, particularly as data moves through different systems, environments, and network segments.

Inadequate Real-Time Threat Detection

Existing data protection tools often lack real-time monitoring capabilities for data-in-transit. Without real-time threat detection, organizations cannot promptly identify and respond to suspicious activities, which can lead to delayed responses to data breaches.

Limited Context for Incident Response

When a security incident occurs, lack of visibility into where is the data, who accessed it and how, makes it difficult for security teams to understand the context of data flows and interactions. This limitation slows down incident response and forensic investigations, increasing the impact of data breaches.

DATA PROTECTION & SECURITY

Who's accessing your data and how

OUR SOLUTION

WireX Systems Ne2ition platform empowers organizations to strengthen their data security posture by delivering actionable insights that reduce risks and enhance compliance efforts. Ne2ition achieves this through continuous monitoring of all network interactions, including those with critical assets like databases, file servers, and domain controllers. This capability is further complemented by API integrations across various cloud environments, providing seamless visibility into data flows both on-premises and in the cloud.

With this holistic view, security teams can swiftly detect and respond to security incidents, gaining insights into data usage and potential vulnerabilities across the entire digital landscape. By identifying risks before they escalate, prioritizing critical areas of concern, and streamlining compliance, Ne2ition enables organizations to proactively protect sensitive information. This enhanced visibility into data interactions and patterns strengthens security readiness, helping organizations remain resilient against evolving threats and maintain a strong data security posture with minimal overhead.

KEY BENEFITS

1. **Unparalleled Network Visibility**
   Real-time visibility into data-in-transit, allowing organizations to monitor sensitive information across internal and external networks.

2. **Consolidated Data Insights**
   Manage and monitor data more effectively and eliminate blind spots with a single, unified view across all data security environments.

3. **Centralized Data Monitoring**
   Identify and mitigate risks proactively, preventing potential security gaps from becoming exploitable weaknesses.

4. **Enhanced User-Data Interaction Visibility**
   Gain visibility into user actions across applications and protocols, making it easier to detect abnormal or unauthorized behaviors that could signal security issues.

5. **Real-Time Threat Detection**
   Detect and respond to suspicious activity in real-time by identifying anomalies that may indicate security risks, like unusual data access or movement.

6. **Rapid Incident Response**
   Gain context-aware insights on data location, access, and usage, enabling security teams to contain incidents faster.