VOTIRO

Solution Brief

Zero Trust Data Detection & Response

Real-time Data Security for Preventing File-borne Threats and Masking Private Information

From browser downloads to email attachments to third-party uploads and collaboration tools like Microsoft Teams, OneDrive, and SharePoint, **data remains the biggest threat to enterprise security**. With files and unstructured data flowing through endpoints, between stakeholders, in and out of applications, and with threat actors gaining momentum with the help of GenAI, protecting the Cloud and on-prem locations has become near impossible for IT and SOCs.

Without a proactive, defense-in-depth solution in place, **malware can infiltrate secure environments** and **private data can leak to unapproved parties** - causing mass breaches, non-compliance, hefty fines, lost time, and significant distrust.

Votiro DDR solves this problem with a three-fold approach to data security.

Active Data Masking

Unstructured data is masked in real-time as it flows into, throughout, and is stored within endpoints. By discovering, identifying, and obfuscating data in motion, based on fine-grain policy controls, private data remains in the hands of approved users, both internal and third-party.

Actionable Analytics

In-depth threat and privacy analytics are provided via easy-to-use monitoring dashboards as files and data flow in. With insights into user behavior, threat vectors, and popular data types, organizations are able to make informed decisions and increase security posture.

Advanced CDR

AI-trained CDR technology automatically disarms and reconstructs all file content to ensure malware, ransomware, and zero-day threats never reach endpoints. Unlike reactive tools, this zero-trust approach equals less time quarantining and blocking for IT, while also reducing noise in the SOC.

Modern Data Security Demands Zero Compromises

With active data masking and advanced content disarm and reconstruction under one unified platform, Votiro gives organizations access to a data security solution that disarms threats with no known signatures and masks sensitive information in real time.

Gone are the days of reactive threat mitigation and non-compliance with complex and ever-changing regulations. With Votiro, data is kept private and threats are kept at bay.

Remain compliant and keep private data private:

- Obfuscate personal, financial, and healthcare data while it's in motion and at rest
- Avoid non-compliance with complex regulations like GDPR, HIPAA, etc.
- Receive actionable insights into threat vectors, user behavior, file types, and more

Safely download, upload, and share 200+ file types:

- Users maintain productivity as Votiro keeps essential macros intact, preserving intended file fidelity and functionality
- Sanitize zips, archives, and password-protected files
- Break apart and reassemble safely using patented Positive Selection® technology

Plug critical security gaps left behind by other tools:

- Signature-based tools like antivirus (AV) can't prevent zero-day threats
- Reactive tools like Data Security Posture Management and Data Loss Protection offer visibility and alerts, but fail to prevent malware before it can cause harm
- Sandboxing and quarantining are time-intensive and can still miss threats

Protect multiple environments at once:

- Votiro is an open API with native connectors for collaboration suites like Microsoft O365 (Teams, OneDrive, SharePoint)
- Also deployable as an SMTP relay, Votiro protects multiple channels including email, 3rd-party portals, web browser downloads, and more