VOTIRO Zero Trust Data Security

Advanced Content Disarm & Reconstruction **for Email**

Ensure the Removal of Hidden Malware from Email Content Without Compromising Business Productivity

Overview

Votiro Zero Trust Data Detection & Response (DDR) is multiple data security solutions in one unified platform:

- Advanced CDR stops known and unknown file-borne threats in real-time, while maintaining full file functionality for over 200 file types.
- Active Data Masking protects sensitive data from exposure by obfuscating private data (PII, PCI, PHI) while it's still in motion, keeping enterprises compliant.
- Actionable Analytics provide IT teams with in-depth threat and privacy insights for a better security posture and proactive threat preparation.

Problems

Most security tools are reactive in nature	→	AV relies on known signatures. DSPM and DLP simply offer alerts and steps for manual mitigation.
GenAI has increased the sophistication of phishing	→	Artificial intelligence is being used to create convincing emails that even fool seasoned users.
Traditional defenses are no longer effective	→	IT teams spend hours each day quarantining and sandboxing, but threats can still get through.
Many security tools demand complex integrations	→	Enterprises spend more time and money in an effort to learn, update, and monitor tools.

According to reports by IBM and Verizon in 2024, email phishing and business email compromise continue to be primary threat vectors, accounting for the most costly data breaches year after year.

Solution

Votiro's Advanced CDR **Prevents Threats in Email Content**

Prevention for zero-days.
Built on zero trust principles, advanced CDR doesn't just detect hidden threats buried within files, URLs, and images - it only allows known-good elements to reach enterprise endpoints.

No time wasted investigating files.
Email serves as a critical business function, so there's no time for quarantining and sandboxing - which can still leave critical gaps. Automated threat mitigation allows IT to focus on more important tasks.

Protection for your ecosystem.
In addition to native connectors for suites like O365, Votiro is an open API that can be deployed as an SMTP relay. This allows IT to protect multiple channels, from email to collaboration tools to 3rd-party portals.

Fast, scalable, and functional.
Votiro's Level 3 CDR (aka Positive Selection®) is capable of processing 100,000+ files/hour - without flattening them into PDFs. This means good file elements - including active content like macros – remain intact for continued use.

Votiro DDR

Defense-in-Depth with Votiro Zero Trust Data Detection & Response

Advanced CDR

- Every file is disarmed and rebuilt to prevent zero-days
- 200+ file types are sanitized by Votiro's Positive Selection® technology
- Zero Trust equals less false positives and reduced noise in the SOC
- Active content, such as macros, remain intact
- Sanitization happens behind-the-scenes, in real time, and in just milliseconds

Active Data Masking

- Unstructured data is masked by Votiro's AI-trained technology
- Data is masked while it's still in motion
- Organizations remain compliant as data flows into and throughout endpoints
- Fine-grained security and policy controls keep IT in control of data being obfuscated
- PII, PCI, and PHI data remains in the hands of approved users - internal and third-party

Integrated Analytics: In addition to CDR and data masking, Votiro also provides actionable analytics via in-depth threat and privacy dashboards. IT can deep dive into key users, primary threat vectors, common file types, and more. This enables easier compliance, a better security posture, more-informed decisions, and helps IT prepare for future attacks.

VOTIRO **Book a Demo**

votiro.com

sales@votiro.com