SOPHIC INFO

CybergymIEC

Sophic Info

Securing the most sensitive file transfers is a key challenge when dealing with critical infrastructure operators. The transfer path is the highway used by attackers to penetrate and exploit vulnerabilities. As a result of the increasing need to overcome these vulnerabilities, the Israel Electric Corporation, as one of the most cyber-challenged companies in the world, has applied its exclusive knowledge and over 25 years of battle-proven experience, to develop a proposed and perfectly adaptable secure file sanitation and transfer solution for ICS critical infrastructure operators across the globe.

Sophic Info™ provides easy to use secure SaaS solution, based on unique know-how that integrates highly effective technologies for preventing known and unknown threats, including zero-day targeted attacks and threats, and is an integral part of our Sophic Suite.

Key benefits:

- Unique ATP (Advanced Threat Prevention) using multiple Security layers.
- Reduce operational costs via full SaaS automated and scalable infrastructure, along with fully Secure Cloud hygiene – accessible from anywhere.
- Sophic Info™ provides maximum visibility of all inbound files transfer while helping you to stay compliant with the regulations.
- Battle-proven solution.

  Sophic Info™ has been 100% operational for many years within Israel Electric Corporation's critical network infrastructure.

Use Cases

Remote Firmware install/update for any device within the critical infrastructure

With Sophic Info™, your ICS vendors will be able to send you installation and update files, regardless of the file type and with NO file size limitation, in the most simplified and secure manner.

IT 2 OT & OT 2 OT Secure file Exchange of sensitive files

With Sophic Info™ you will be able to transfer sensitive files between different segregated networks within your internal critical network infrastructure.

Maintain business continuity especially during these times when working from home has become so necessary.

Thanks to the unique security and file sanitization, employees with major ownership in the ICS critical infrastructure can also send critical patches or updated configuration files, from home.

Main capabilities

- **Strong user authentication**

  Using a strict on-boarding process supported by MFA (Multi-Factor Authentication).

- **3-Dimensional file inspection**

  To protect the critical infrastructure from Advanced Threats, each file will pass through a dedicate file inspection process, based on its true type and policy definitions. File inspection includes:

  - CDR (Content Disarm and Reconstruction)
  - Multi-Engine AV scanning
  - Threat emulation including both Static and Dynamic Analysis.

- **Powered by Data Vaulting technology**

  Sophic Info™ protects all sensitive files with strong encryption at transit and at rest, ensures strict access control and provides full tracking and visibility of all activities and file transfers.

- **File signature validation**

  Transferring files securely is not enough. It is important to make sure that files are not modified during transit. Modified or corrupted files might introduce security risks and moreover, can cause an operational disaster when installed on OT devices. Therefore, Sophic Info™ performs integrity checks on files before arriving at their target destination.

- **Unidirectional Data Transfer**

  Sophic Info™ allows data to travel only in one direction to ensure a strict route for each sensitive file, whether its incoming or outgoing.

- **Central security monitoring and analytics**

  Sophic Info™ provides full visibility into all file activity within its Dashboard. With this information, security operations professionals detect anomalies, identify security incidents, and drill down to respond to those incidents.