CEO-VISION
Technology made simple

POST

• DATA SECURITY • DIGITAL WORKPLACE • COLLABORATION • FILE SERVER

The Open Source Digital Workplace at the service of your IS security

CEO-Vision is the publisher of the GoFAST Digital Workplace solution: an innovative and Open Source alternative to Office 365, SharePoint, Teams.

For 10 years, CEO-Vision has been supporting GoFAST users to reconcile good security practices with new uses: simple and anytime access to their tools, documents and business processes, without depending on a VPN or a professional PC, in the office or teleworking to collaborate with colleagues and external partners.

The main target of ransomware: the classic file server

Among the most vulnerable systems, the classic Windows file server is the target of most ransomware attacks, with **catastrophic consequences**: several days to several weeks of service interruption. Examples include Ryuk, Egregor, Ragnar Locker, Clop, Maze, Wanna Cry, Petya1 ransomware...

Significant improvement in document management

Reduction in the exchange of documents by email

Optimal data security

Many cities have been affected in recent months, as well as hospitals, Dassault Aviation US, Sopra-Steria, Wagons-Lits, CMA-CGM, etc. In general, this type of attack is triggered after **an email or attachment is opened** on a workstation that does not have up-to-date antivirus software. The entire file server is then locked and a large ransom is demanded (sometimes several millions) to recover the data. According to ANSSI in October 2020, Ryuk is responsible for **75% of attacks on the healthcare sector**, a sector it has been attacking since early 2019.

In some cases, data is also stolen and hackers threaten to release sensitive content. The operators of the Ragnar Locker ransomware had released data stolen from the aircraft manufacturer Dassault Falcon Jet (an archive presented as weighing 3.5 GB and named Falcon 6x project Archive.7z).

GoFAST Digital Workplace to protect data against ransomware

Data security depends on both technologies and the type and location of hosting, but also on the best practices of users. The GoFAST Digital Workplace concept takes these key factors into account for an optimal level of security against ransomware.

First of all, access to the platform and therefore to the documents is done directly via the web browser, completely separate from the workstation. **This significantly reduces the risk of contaminating the document base from a file that would be present on the workstation.**

GoFAST does however allow the mounting of a Windows network drive (WebDAV). Some users can therefore create a link between their workstation and the platform. Very practical in the case of data recovery, this usage is strongly discouraged in normal times.

In all cases, **fine management of access to collaborative spaces limits the risk.** Indeed, document management by business managers is separate from system administration. Therefore no user-account has access to the entire warehouse! In the event that a ransomware hits the platform, it would only affect a limited part of the documents (depending on the access of the victim user account).

[1] https://attack.mitre.org/techniques/T1486/

The benefits of using GoFAST Digital Workplace

- The dedicated GoFAST platform **"Cloud Act free"**: either On Premise or in sovereign SaaS: SecNum Cloud hosting possible with our partner Outscale
- Secure access to documents, business management separate from GDPR system administration
- Automatic **versioning** of file changes and in case of encryption, it is possible to recover previous versions,
- **Zero attachments**: files shared via secure links (audited, time-limited),
- Management of **authentication** delegated to the internal directory (AD/LDAP) to comply with your password management or SSO policy.
- **Open Source Technology**: Audit your platform down to the sources ("white box")
- Offer that includes **security monitoring, automated audits and hotfixes** required on all Open Source components. This relieves IT departments of a very important task and avoids having vulnerable obsolete components.

About CEO-Vision

CEO-Vision is the publisher of GoFAST: the Digital Workplace at the service of organizations and their users to gain in productivity. It is a unique and open source alternative to Office365, Sharepoint, Google Workplace... Its motto: "technology made simple". Its know-how is focused on Open-Source technologies:

- **Drupal** for Portals (CMS),
- **Alfresco** for Document management System (DMS),
- **Element and Jitsi.meet**
- (instant messaging and web conferencing)
- **Bonitasoft** (Workflows),
- **OnlyOffice** (Collaborative Office Suite)
- **Solr Apache** (Search engine)

Ransomware encrypts documents to block access, but because GoFAST automatically backs up each version, it's always possible to recover previous, unencrypted versions. Unlike a file server attack, not only are the documents recovered, but the day's work is preserved.

According to our security policy on the protection of the GoFAST server, it includes many protections such as an antivirus, an IDS (Intrusion Detecting System), a Mandatory Access Control permission system (MAC) based on "selinux", and many other protections, firewall and integrated reverse proxy.

Solution audits for ever greater security

GoFAST Enterprise comes with a very strict update policy, particularly in terms of patches for potential exploitable vulnerabilities, with regular audits (Web Application Vulnerability Scanner from the leading company Tenable) to quickly detect any known vulnerabilities. Similarly, the very present Open Source community contributes to the strong reactivity in their identification and updates of the technologies integrated into GoFAST, which is rarely the case on internal file servers. For GAFAM solutions, it is not possible to do white box audits, as the sources are not available.

Note that the "payload" (offensive part of the malware) is often carried by VBA macros in MS-Office office files ("transport" part, i.e. the Trojan Horse). In these cases, as long as users only view the preview of the document on the web interface, without editing it with their MS-Office, there is no risk.

So the only remaining case is a user without an up-to-date antivirus who uploads an infected file to GoFAST, and then it is opened for editing by another user, who also has an out-of-date antivirus. If there is no network editing, there is no damage to the other files stored on GoFAST.

GoFAST therefore provides many additional protections compared to a Windows file server, even when the basic security of the workstation is compromised.