



Better to prevent than pay

Fujitsu's data-driven ransomware strategy

Cyberattacks, especially with ransomware, increasingly threaten the success of digital transformation (DX) in many organizations. The economic damage caused by ransomware has been growing rapidly from year to year, and every 11 seconds a business enterprise falls victim to a ransomware attack. Experts estimate that by 2031, ransomware attacks will occur every two seconds and annual damage will skyrocket from about \$20 billion today to \$250 billion.

Since data is the heart of intelligent enterprises, successful digital transformation depends more and more on the ability to develop a unified data management and protection architecture for modern multi-cloud infrastructures. But how can your business become cyber secure?

First and foremost, cybersecurity must be seen as a key aspect of your overarching business goals. As a digital enterprise, you also need to embed security at the core of your systems and processes, and create digital value chains that reliably protect the data of your customers and partners. A secure and convenient user experience should be a top priority here.

The challenge is undoubtedly complex, as cybercriminals are now targeting even backups – the last line of defense against ransomware – to limit their victims' recovery options. If an attacker gains access to your backups, your organization has little chance to defend itself against paying ransom.

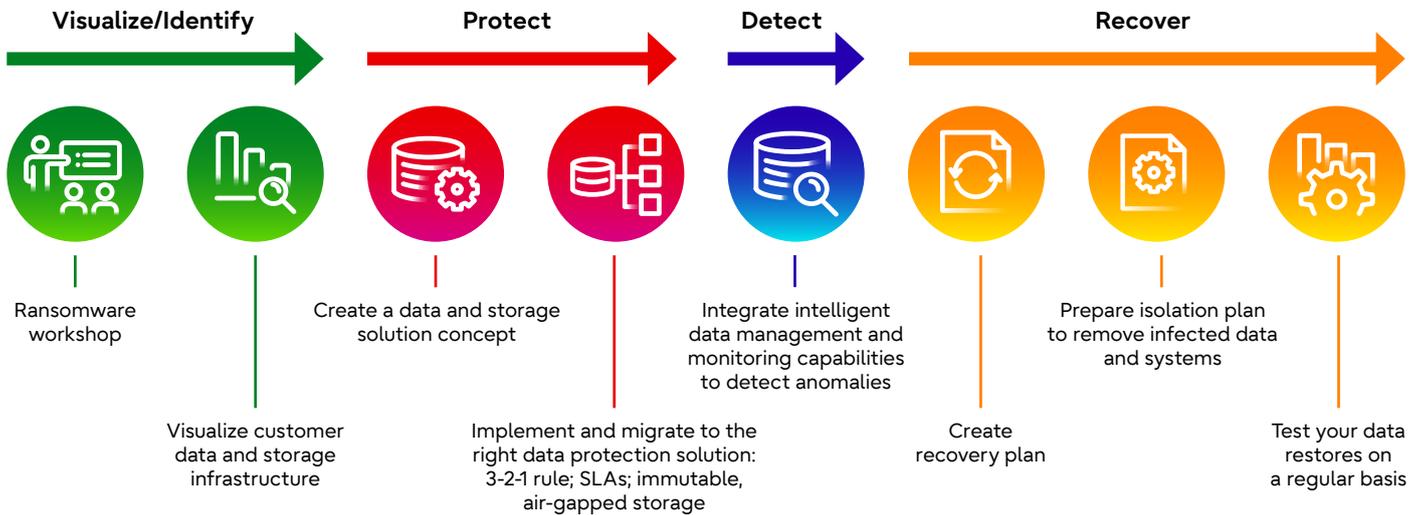
However, you can effectively counter these threats with a multi-layered approach to protecting your data. This requires comprehensive knowledge and regular training so that you can stand up to cybercriminals. That's why you should work with an experienced and trusted partner like us. We'll guide you on your journey toward a cyber-secure IT infrastructure, making sure your business takes full advantage of new cybersecurity methods and technologies.

What is ransomware?

Ransomware is malware that attacks your business via the network – targeting mainly production servers, but also backup data. It encrypts critical files, making them inaccessible until the demanded ransom is paid. Ransomware directly leads to system downtime and thus loss of business, and it subsequently damages the reputation of the company, resulting in loss of confidence among customers and partners.

Safeguarding business against cybercrime is vital in the digital world

We provide a data-driven ransomware strategy to help you strengthen your resilience against ransomware attacks and improve the security of your data – on-premises, in the cloud, or anywhere else. With our strategy, we assist you in implementing data and storage solutions that prepare you for cybercrimes like ransomware attacks. First, we begin with a thorough examination of your business needs and existing ransomware gaps. We then work with partners to help you build a secure and modern infrastructure. In subsequent steps, we show you how to protect your IT against any hackers who might be targeting your data.



Unlock the full potential of best practices and solutions



Protect your data with the 3-2-1 approach (3 copies of data on 2 different media, with 1 copy kept off-site) so that at least one copy survives even if the other two are lost, destroyed, or encrypted by a ransomware attack.



Safeguard your data with immutable storage. Should ransomware penetrate your organization's front line of defense, data written to an unchangeable, non-network accessible storage pool is safeguarded against encryption or deletion, thus making it available for recovery.



Leverage the power of offline backup and air gaps. Creating offline copies is an essential step in a data security plan to reduce the risk of a successful malware attack. Air-gapping your data with a physical barrier realized with tape storage is the most cost-effective way to store and protect your data and recover after a ransomware attack.

Play it safe

Prevent criminal cyberattacks with our ransomware strategy. Our extensive data protection ecosystem includes solutions for identifying, protecting, discovering, and recovering your data at any point in its life cycle. Visit www.fujitsu.com/dataprotection for more information.