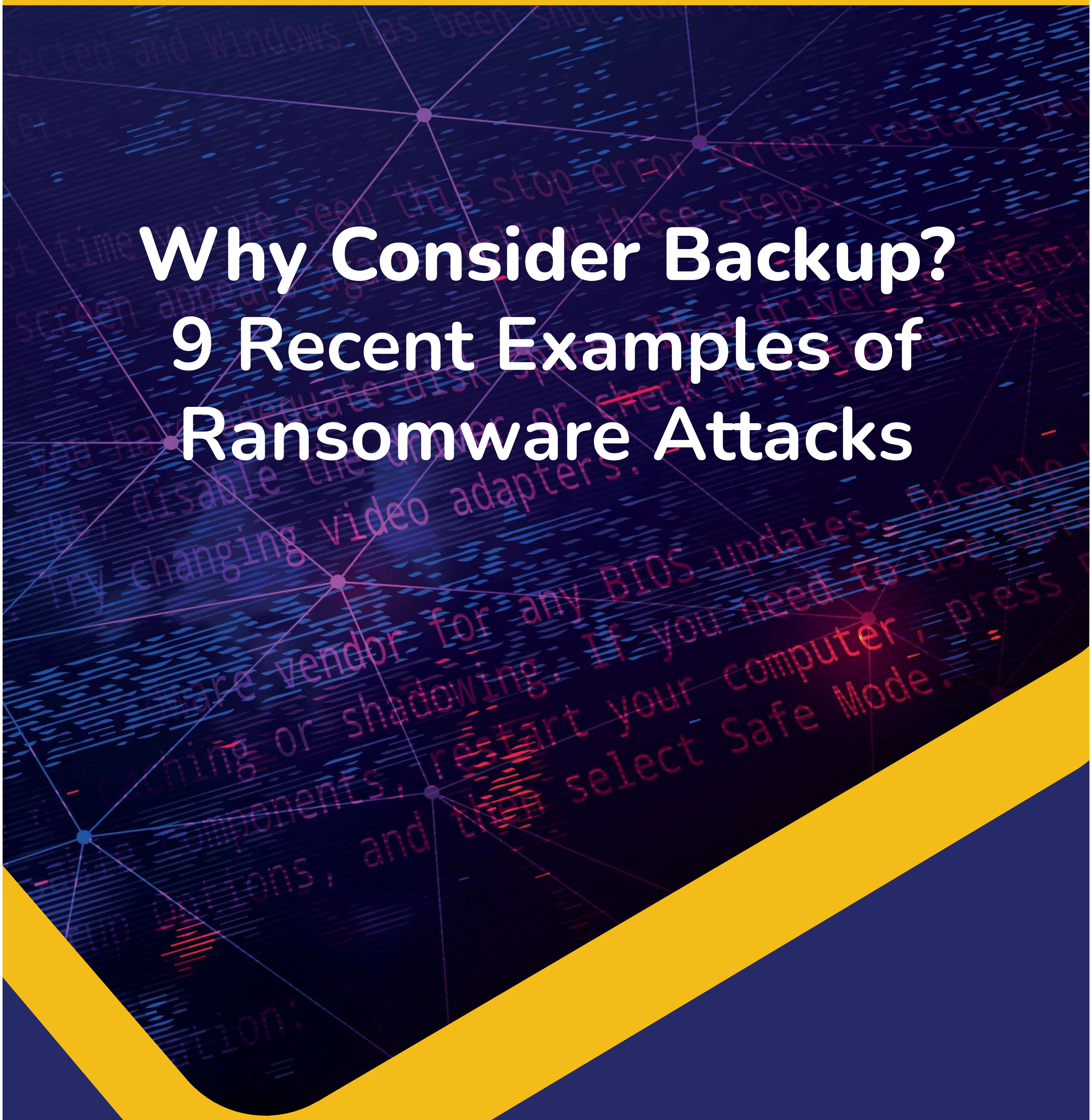
Why Consider Backup? 9 Recent Examples of Ransomware Attacks



cloudficient

EMPOWERING DIGITAL TRANSFORMATION

Contents

Introduction

This guide will help you understand the importance of creating a secure, independent backup even when your organization has transitioned to the cloud. Your move to the cloud might include:

- Email
- End user files and documents
- SharePoint libraries and sites
- New application usage, eg Microsoft Teams

We will start by reviewing several recent ransomware attacks and how businesses were impacted before moving on to the discussion of how a backup solution could help organizations that are targeted.

What will your end-users do without access to key information, files, messages and data during that time?

What is Ransomware?

According to the US Governments Cybersecurity and Infrastructure Assurange Agency ransomware is:

"an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid."

That means that hackers performing the attack take advantage of weakpoints in your organizations network or firewall security to steal sensitive data or lock (encrypt) files. Your organization will only be able to recover and decrypt the files (and give users access to them again) if the ransom is paid.

Of course, there is always the possibility that you pay the ransom and multiple days or weeks pass by before the decryption happens.

The true cost of ransomware attacks may never be known. It’s not just the cost of the ransom but loss of income during the attack, bad publicity, and the cost to recover from the attack.

Ransomware attacks don’t just happen to companies in a particular industry sector; they happen across every type of industry. You might be thinking that there is just a handful of attacks, or even a few dozen. You would be very wrong - there are millions! Sonicwall reported that there were approximately 500 million attacks in the first nine months of 2021. This is up by 148% compared with 2020.