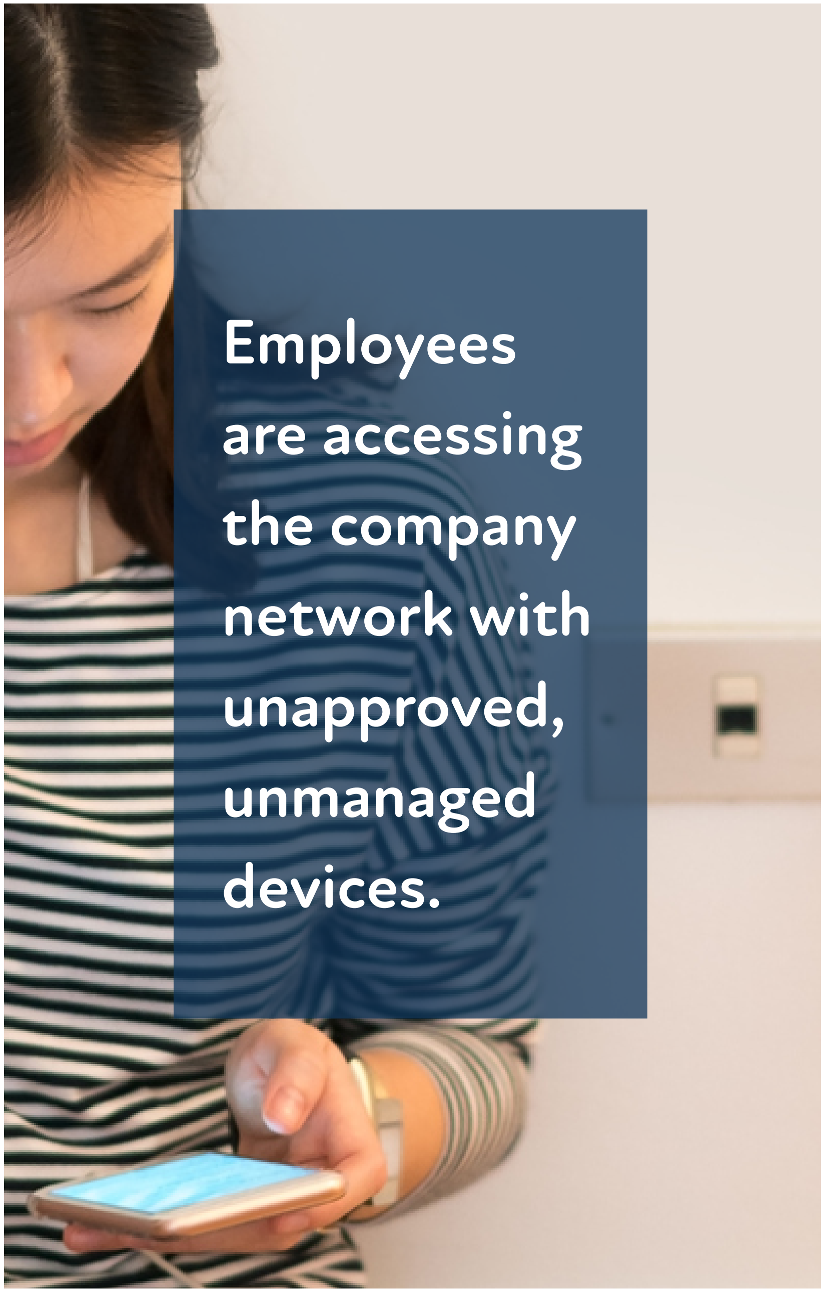
DO REMOTE WORK RIGHT.

THE 5 WARNING SIGNS YOU HAVE POOR SECURITY

Ovatio



Employees are accessing the company network with unapproved, unmanaged devices.

#1 SECURITY WARNING SIGN

Covid-19, forcing many people to quickly pivot working remotely, has lead to an increase in the global workforce's use of unapproved and unmanaged personal devices. While born out of necessity, the byproduct of these actions leaves your business vulnerable to malicious activity, serious reputation damage and costly fines.

#2 SECURITY WARNING SIGN

There is no ability to track when, where, and how your company data is moved or shared.

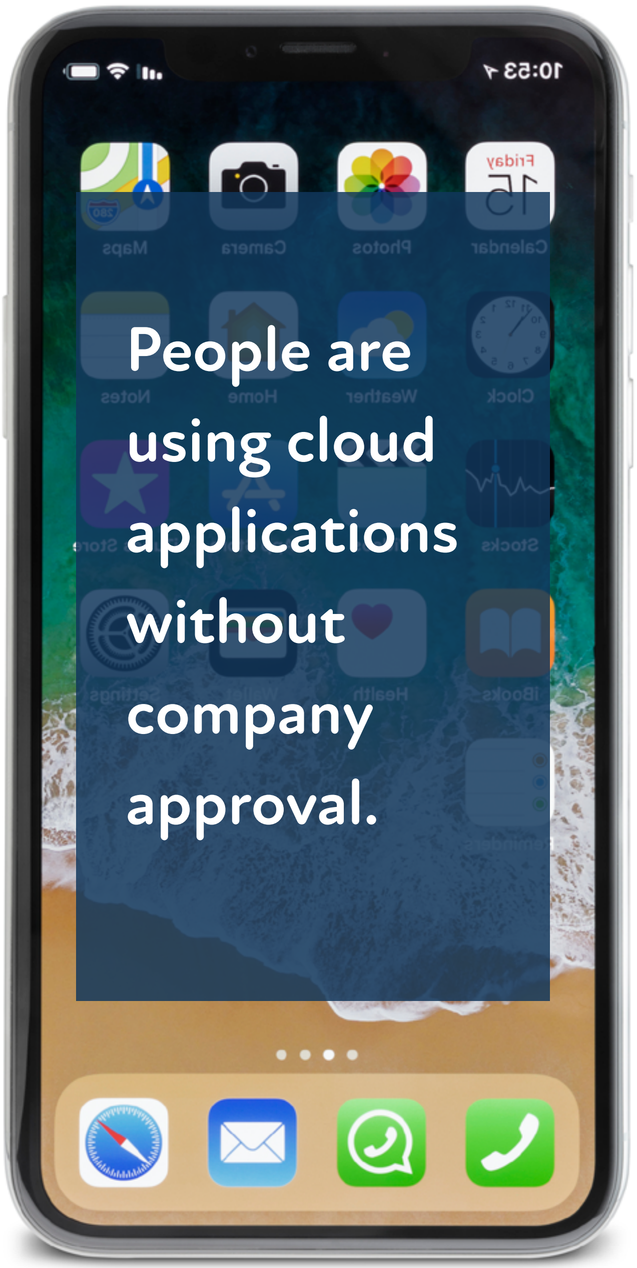
Do you know who downloaded files today? Do you know where the data went after they downloaded it? Do you know if they shared it and with whom? If the answers are “No,” or “I don’t know,” this should be one of the first security flaws you address. Tools can provide you with automated intelligent alerts of the when, where, how – and even who – is moving or sharing your data.

Employees primarily share files with one another using email.

#3 SECURITY WARNING SIGN

Primarily using attachments to share and work upon documents is not only a drain on productivity, it is also not the most secure practice. Attachments are a prime target for embedding malware, in fact, 92% of malware is delivered by email! Nefarious groups are highly-skilled at crafting phishing emails, mirroring the writing nuances of the people you converse with regularly. These types of targeted emails trick people into trusting the source, leading to the opening or downloading of malicious attachments.

#4 SECURITY WARNING SIGN



People are using cloud applications without company approval.

Trying to do a job as efficient as possible from home (especially during COVID-19) has organically lead to employees finding creative workarounds including using unapproved cloud solutions to share, store, and collaborate on data. Not knowing which applications employees are using also means you don't know what or who is accessing or moving your data.

There is no formal policy for working remotely or cybersecurity training.

#5 SECURITY WARNING SIGN

People are your weakest vector point in the fight to keep the company secure, educating them is one of the best tools you have to prevent a breach or leak. Without comprehensive policies and training, people's behaviors and practices are left to chance. Don't take it for granted that people can identify the signs of a suspicious email, or that using their personal computer or phone to access company data leaves the business open to serious security issues.

Is your business working remotely the right way?

Know for sure – take the free *Remote Work Right Maturity Assessment* and receive a personalized report.

LEARN MORE. >

Ovatio

ovatiotech.com | 978.294.9711