Protecting Company Data in a
WORK-FROM-ANYWHERE WORLD

The effects of cyberattacks

Paying the price
Not only are businesses obligated to pay a hefty price to keep their data private, but it's possible they may lose valuable information that can never be recovered.

4.4 MILLION
The Colonial Pipeline's CEO confirmed that the **company paid hackers $4.4 million in ransom.**

Restoring valuable data
During a ransomware attack, hackers steal valuable data and threaten to delete or leak that information if a ransom is not paid. In some cases, data is unable to be retrieved if companies do not have a back-up in place.

100 GIGABYTES
During the May 2021 Colonial Pipeline cyberattack, **hackers stole 100 gigabytes of sensitive data,** shutting down the 5,550 mile gasoline pipeline.

Employees out of work
Many businesses rely on technology to collaborate and operate efficiently. Without the ability to access critical files or stay connected with team members, operations slow and money is lost.
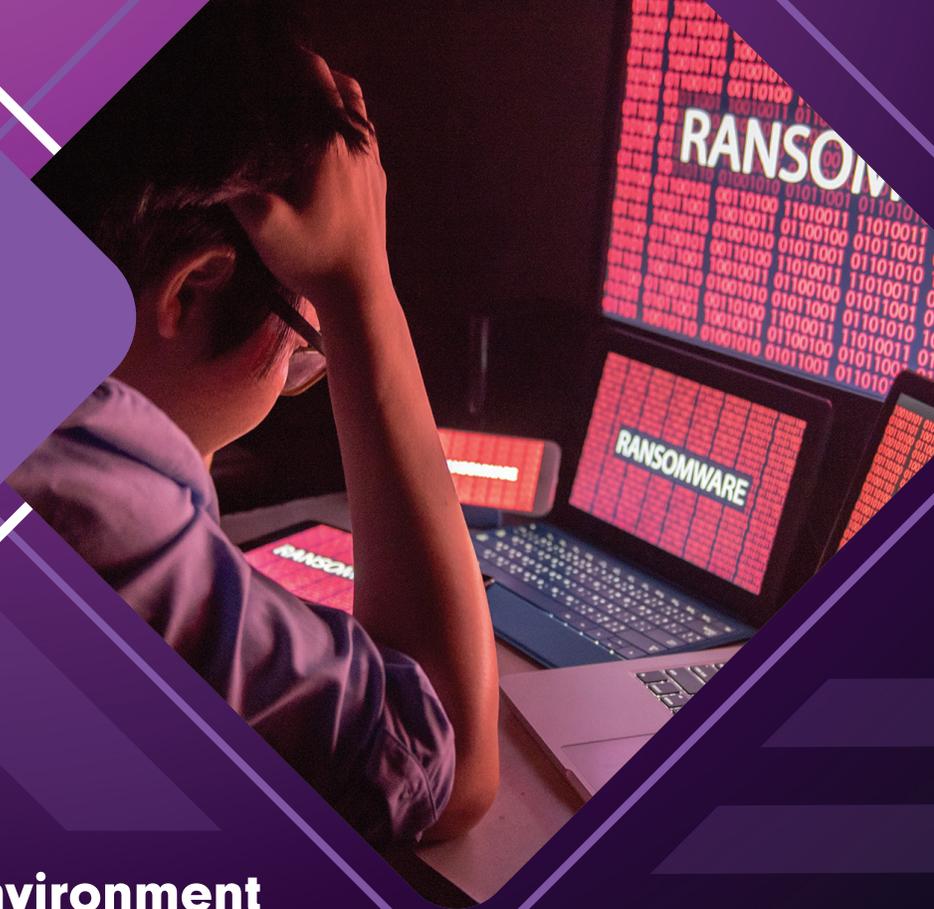
OVER 8.4 BILLION
During the Colonial Pipeline cyberattack many accounts were compromised. **User credentials each contained valuable private data for over 8.4 billion individuals,** causing significant disruption to their lives.

We're here to help you implement security protocols and solutions to keep you and your data safe. Don't let your business fall victim to costly cyberattacks!

PROTECT YOUR BUSINESS
from ransomware attacks

Defend Your Entire IT Environment
Our security cluster provides aggregate solutions for you to grow in a flexible and customizable delivery model through:

According to Robert McKay, SVP of Risk Solutions at Neustar, cybersecurity experts predicted that

there will be a cyberattack incident every 11 seconds.

This growth in attacks has been double or even quadrupled year over year.

Secure Access
Protect your email environments through encryption, decryption, and scanning of emails for spam, viruses, and anomalies.

Secure Services
Employ services to monitor, detect, analyze, and respond to security threats in real-time, allowing your IT staff to manage vulnerabilities proactively.

Secure Management
An increase in users and devices means a higher chance of digital attacks. Enforce full device encryption, user access standards, policies, and procedures across your entire organization.

Secure Endpoint
With remote workforces and businesses practicing BYOD, it is becoming increasingly more important to protect every entry point to safeguard against malware and other threat attempts.

Secure Email
80% of successful data breaches use email as an entry point; protect your employees and clients!

Now is the time to ensure that your sensitive data is protected from this new wave of insidious cyber-attacks. Contact us today to discuss security solutions that will keep your sensitive data protected!