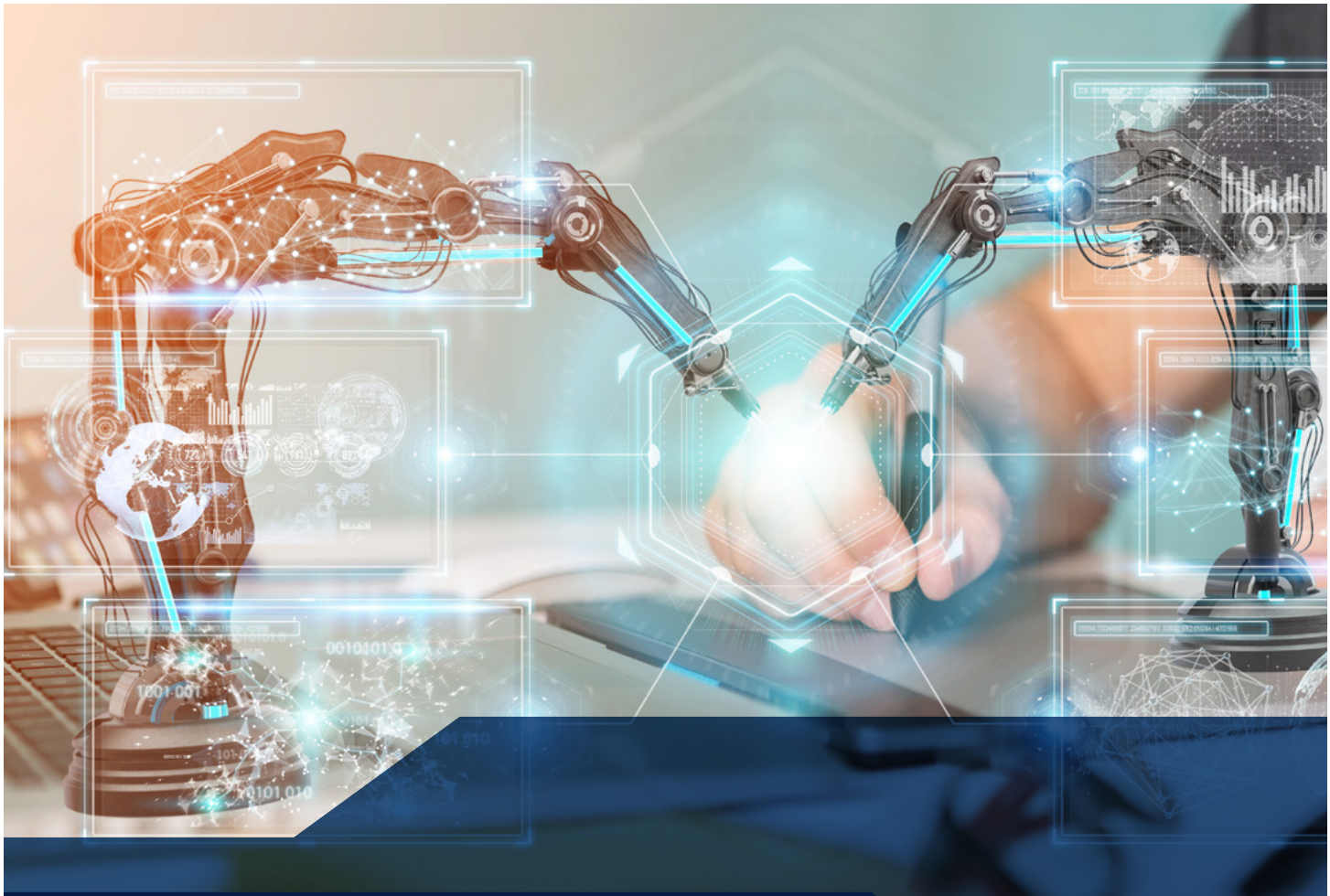
WHITEPAPER **2020**



Email Security for Manufacturing Industry

www.**trustifi**.com

Trustifi

When the common employee thinks of which industries need email security and cybersecurity, most envision the healthcare and financial industries. In reality, that's not always the case -- and the manufacturing industry is now a prime target. Many manufacturing employees believe that cyber criminals have no interest in targeting manufacturers. In the past that may have been true, but now that manufacturing devices and operations are on the Internet, times have changed..

Industry 4.0 is upon us, and it has changed the game. The fourth Industrial Revolution is data, artificial intelligence, and automation becoming a vital part of manufacturing. More devices are connected to the Internet than ever before, and this extends to the manufacturing sector where intelligent devices are quickly becoming integral parts of lines. Manufacturers are installing more of these 'smart' devices in their facilities as they seek to improve their operations in any way possible. However, these benefits do not come without consequence.

This new age of connected devices has made cybersecurity that much more important in the manufacturing sector. There are more vulnerabilities in manufacturers' systems as the number of devices that are connected to the internet have skyrocketed. Hackers could completely compromise manufacturing lines and technology by exploiting weaknesses in employee knowledge and computer systems.

Manufacturing employees are susceptible to attacks from cybercriminals, and phishing schemes often target employees who are trusting of outside parties.

Stop Leaking Confidential Information

Manufacturing employees are primed with key information about manufacturing processes and technologies. Sending intellectual property to outside parties is often necessary in supply chains. This presents a prime opportunity for phishers to exploit employee trust and extract pivotal information from key employees who might unknowingly send information which is compromised.

Trustifi has developed a series of strategies that help prevent employees from sharing key information with untrustworthy outside sources. An AI-powered ranking system scans incoming emails and helps users identify if the party that they are corresponding with is genuine or or spoofing attacker. After an email is scanned, Trustifi will label it with a safety ranking which ranges from 'Authenticated', where the party actually is who they are, to 'Impersonation Attack,' where the party is pretending to be someone they are not.

The second form of security is an inbound protection system that works behind the scenes to detect and mitigate any potential threats. Administrators can create custom rules to guide the system on how to handle every type of threat. Once the rules are set, potentially malicious emails that would normally end up in a user's inbox will be safely redirected into a quarantined area. Both of these measures will help employees identify and avoid potential phishing schemes.

On the outbound side, Trustifi provides email security with our industry leading email encryption platform. Manufacturer's sensitive information can be extracted if transmitted through networks where the contents of an email are not encrypted. Employees may forget to encrypt an email or may not even be aware that it is necessary to encrypt sensitive information.

Email Encryption Made Easy

Encrypting emails sounds like a confusing process that employees may struggle to grasp, butTrustifi developed an email encryption system that even the most computer-illiterate employee will be able to use. Trustifi scans all outgoing messages, so that even if an employee forgets to encrypt an email or attachment with valuable manufacturing secrets, all potentially sensitive data will be detected. Once the system detects the sensitive data, the email is automatically encrypted to ensure that your employees follow proper cybersecurity guidelines.

Trustifi also scans emails in real time as they are being composed to automatically alert the user to choose an encryption option in order to secure sensitive data. Additionally, Trustifi utilizes a multi-factor authentication system to identify the receiver of the intended email. The email recipient does not need to install any software, create logins, or generate passwords either which makes the entire experience seamless. All of these AI systems work to make your organization's email as secure as possible.

Trustifi can ensure that your organization's supply chain remains intact by improving your email security. Your relationships with suppliers and purchasers will improve as they will be able to trust your organization with sensitive materials.

Trustifi

256-Bit AES Encryption

NSA grade protection over your data and files

Extra Security Features

- One time access to files/emails
- Block access to print files
- Delete or edit messages after they have been sent

Inbound Protection

Stay protected from malicious links and files, viruses, phishing and spoofing attacks, ransomware attacks and even Spam.

Multi-Factor Authentication

on the recipient- You can choose to lock an email by adding a pin or a question that can only be unlocked by the intended recipient for an extra layer of protection

No Log-in Portal or Account Necessary

one click authenticate and decrypt allows your recipients to open your emails and also reply encrypted without ever having to sign up or login to anything

Contact Trustifi today to learn more about how our robust email security solution will keep your manufacturing organization safe.

www.trustifi.com
1-844-235-0084
info@trustificorp.com