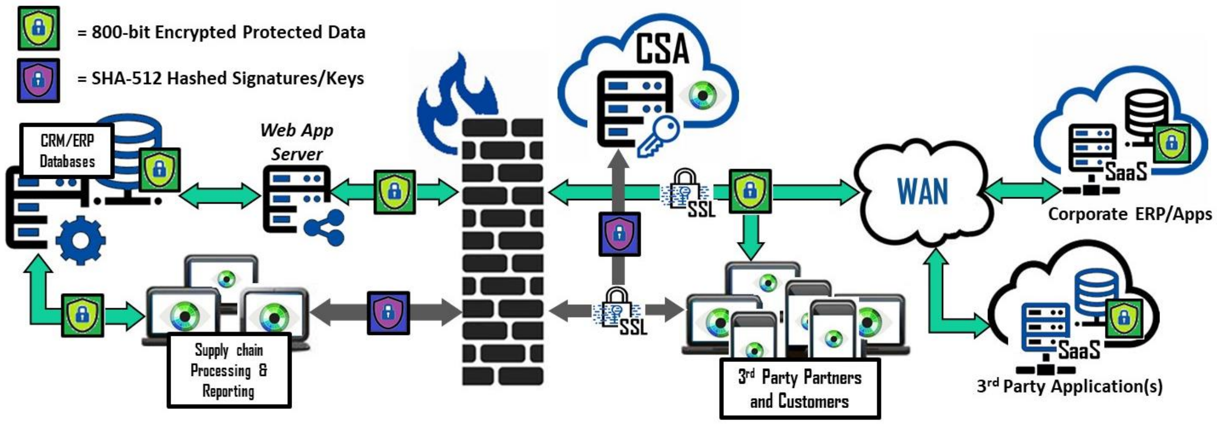
Use Case: Securing your Supply Chain

The Manufacturing industry is embracing change on many levels — among the notable trends, companies are shifting to a B2B2C model in an effort to better understand and serve their customers. The industry's supply chain infrastructure is key and is adopting automated technologies and IT-powered solutions into what some call Industry 4.0. Companies, however, do not operate in isolation. They participate in a global ecosystem where suppliers, value-adding resellers, and trading partners closely collaborate. This is not new. But what is new is the risks associated with collecting and sharing sensitive data driving this digital reinvention. A 2018 study by the Ponemon Institute found that 61% of U.S. companies have experienced a breach "caused by one of their vendors or third parties" — and that number is growing. More than 75% of organizations believe that third-party cybersecurity incidents are increasing. Early in 2020 the FBI sent a cybersecurity alert to the U.S. private sector warning of an ongoing hacking campaign against supply chain software providers. A key contributing factor is the growing complexity of the third-party landscape. As companies increase their reliance on partners, sub-contractors, and suppliers (according to Gartner, 60% of organizations are now working with more than 1,000 third-parties), it's critical that they manage the risk that these vendors can pose to the business.

The backbone for the Manufacturing industry's supply chain is the Enterprise Resource Planning (ERP) systems and the databases they contain. ERP systems have evolved to cloud based SaaS solutions that are highly integrated with CRM, MES, MRP, Financial and HR systems, opening a potential gateway for thieves to steal sensitive data about customers and/or employees. Bonafeyed's Data Defined Security protects this critical data whether on-premises, on the third-party's premises or in cloud base application. Data protection with diversified encryption can control access on a per record basis or between a manufacture and specific third party. In all cases, the data remains secure even as it moves between network domains and on customers' and suppliers' end-point devices.


= 800-bit Encrypted Protected Data
= SHA-512 Hashed Signatures/Keys
CRM/ERP Databases
Web App Server
CSA
SSL
SSL
WAN
SaaS
Corporate ERP/Apps
SaaS
3rd Party Application(s)
Supply chain Processing & Reporting
3rd Party Partners and Customers

Now more than ever, manufacturing supply chains needs protection, and the ability to receive and supply sensitive information to many different enterprises. From vendors to partners, these digital touch points allow for more efficient and effective operations. In a supply chain attack, a hacker will gain access to a partner or provider that has systems and data access. Through this relationship, the criminals can enter networks, steal data, and cause significant business harm. Bonafeyed demonetizes this shared data and prevents unauthorized access to supply chain data.

Contact us at info@bonafeyed.com for a demonstration or visit us at www.bonafeyed.com.