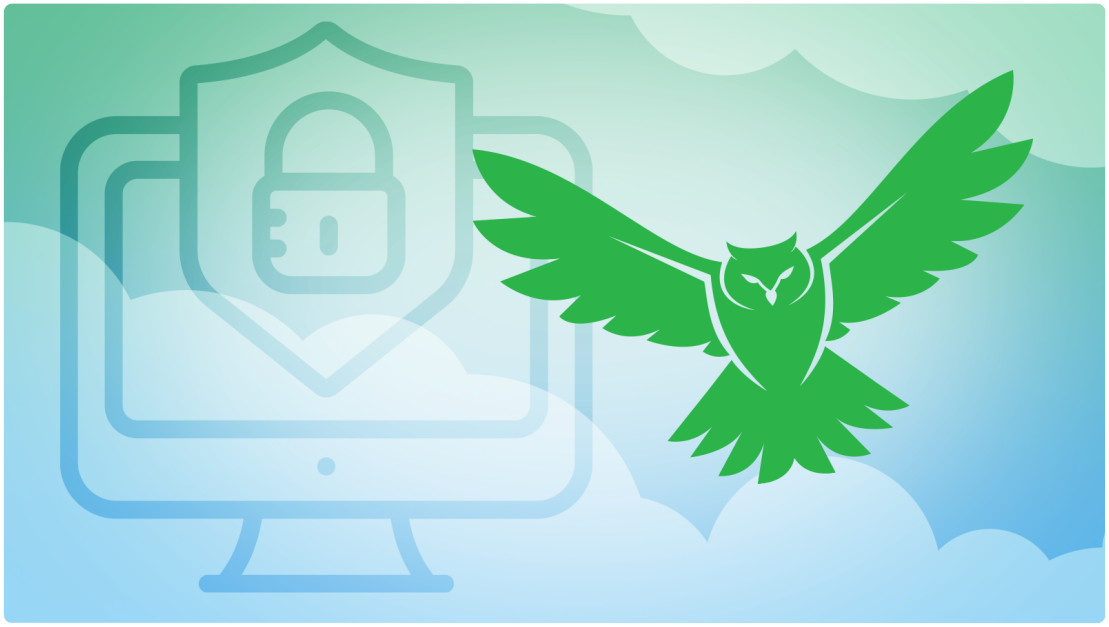
Cloud PLM: Dispelling myths about security

October 26, 2021 Posted by Selerant



Reliance on the cloud has particularly accelerated during the pandemic, in large part due to changes in the work environment. Still, several misconceptions continue to hold food manufacturers back from deploying SaaS PLM solutions. Quite simply, many food manufacturers don't want to give up control over their network and sensitive data.

However, the facts on cloud technology don't support the perception or contention that on-premises PLM is more secure than SaaS PLM. Cloud service providers (CSPs) invest heavily in physical and logical security controls, and typically to the degree to which many enterprises cannot afford.

To truly understand the strength of SaaS security, one also needs to look at the security risks inherent in on-premises PLM installations.

Other cloud PLM posts

When you do the math, cloud PLM beats an on-premises solution in cost
Streamline processes and reduce costs with cloud PLM

On-premises PLM security vulnerabilities

Security is customer-determined, which means constant monitoring and maintenance by system admins. Manufacturers will be able to configure the system the way they want, but may need a high level of expertise for installation and maintenance.

Complete security means network security as well as physical security. Network security must be kept up to date with the latest patches, and the data centers that house on premise applications must be well-secured to prevent unauthorized access and protect against damage from natural disasters.

Separate and sometimes costly security tools are needed to protect each enterprise architecture layer. Such tools need to address user authorization, user authentication, user role management, network or SQL injection attack prevention, and data recovery to be a fully secure solution.

Remote users create susceptibility to viruses. Without proper security solutions, remote user connections to on premise environments provide a gateway for viruses that give cybercriminals access enterprise devices and data.

What SaaS does better

Shared responsibility for security. In a SaaS cloud environment, security is the responsibility of both the enterprise and the SaaS vendor. This means there is less of a burden on the IT team, freeing it up to focus on other corporate strategic initiatives.

Security goes everywhere. Users are remotely located these days and use a range of networks to access data, which are out of a company's control. With cloud-based PLM, a security policy goes everywhere users go. Every device attached to the enterprise network must route its requests through the cloud security service, which ensures safe access.

Blocks threats in the cloud. Security risks and abnormal behavior are detected and resolved by the Cloud Solution Provider (CSP), well before they hit a manufacturer's network.

Added layers of security. Hosting vendors with high quality cloud solutions typically provide added layers of security, access and intrusion protection.

Wide range of security measures. High-quality SaaS PLMs utilize data encryption, multifactor authentication, customer isolation, and other security measures to keep their products secure for remote access. SaaS PLM companies also run continuous automated security testing, as well as manually conducting penetration tests that serve to detect vulnerabilities in their own systems.

Redundancy. Automatic failover and disaster recovery is provided in cloud solutions as achieved through redundant systems, ensuring that data is always protected and available.

Data center security. All data flowing across a public cloud global network is automatically encrypted at the physical layer before it leaves a secured cloud facility, which adds an extra level of protection.

Placing confidence in the cloud

SaaS solutions, including a cloud-based PLM, are likely more secure than an on-premises counterpart. Without significant financial investment, diligent IT practices, a broad array of solutions and backup services, along with strong policies for remote users, it would be difficult for most enterprises to keep pace with the security benefits of today's cloud environment. And even if you had all this security infrastructure at your fingertips, the total cost of ownership will almost definitely outpace the financial commitment to a cloud service.

TAGS: Product Lifecycle Management | Food & Beverage | Cosmetics & Personal Care | Specialty Chemicals | Blogs

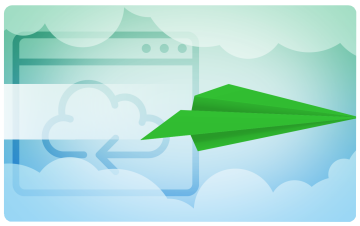
Related Posts

The three-step process for developing clean label standards

November 3, 2021

Global food security demands a strong food safety response

August 31, 2021



Streamline processes and reduce costs with cloud-based PLM

September 28, 2021