AIRGAP

Securing the Pharmaceutical & Biotech Industries

SOLUTION BRIEF

Companies in the pharmaceutical and biotech industries need better security controls. The top threat overall is ransomware. These industries face high volumes of attacks that are often as simple (and successful) as attacking a remote laptop or desk and securing the device.

Once secured, attackers may have access to critical applications, research databases or devices, even build servers. In research labs, for instance, disruption and downtime can severely delay a project while one or multiple devices needs to be revalidated. If these devices have not been patched, they are even more vulnerable.

The manufacturing environment in these industries is sensitive and complex, and often cannot withstand delays for downtime. Devices that may function properly but are dated and naively trusted by the network are not able to withstand malware attacks.

And even the common devices of the branch, campus or remote office are considered valuable targets for ransomware efforts. From smartphones to HVAC systems to cameras, compromised IoT devices that may not even contain sensitive data can be desired launch pads.

Airgap sees to it that the attack stops at the initial compromised device. With the Ransomware Kill Switch, all communication to and from any infected device is stopped.