EXTERNAL USB CYBER THREATS, CONTROLLED WITHIN

Global Manufacturer Utilizes Honeywell SMX Solution For Better Protection Against USB-Based Hardware Attacks

Case Study

Honeywell

FAST FACTS

79%

of threats found with SMX have the potential to cause major disruption to operations

PLUGGED-IN PROBLEMS

Sometimes, it's simply about control. Control over your organization's cybersecurity. Its systems, processes, policies and hardware. But these days, that control needs to extend beyond internal systems. Organizations need to control any kind of threats that might enter the system via portable devices, especially USB drives.

This is why our client, a global building materials producer with billions in revenue, chose Honeywell Secure Media Exchange (SMX) to help protect their systems. The customer recognized the need to improve their USB storage and device-security program. They found themselves struggling to manage the different users on site and the USB devices that were plugged into their production machines. They knew that USB threats are increasing and a major threat vector in operational technology (OT).

Knowing they needed to improve their security posture, especially when it comes to portable media – they began to search for the right solution. And they chose Honeywell. This was because they appreciated a USB security feature unique to Honeywell: device control. They liked the ability to provide a list of devices they want to allow and then to block everything else. This 'USB firewall' would allow their technical staff to get granular with the level of control on most physical devices.

GAINING CONTROL

Another benefit to our solution is the ability to install this SMX Client software on non-Honeywell Programmable Logic Controller (PLC), monitoring, and control systems. For this client, these included workstations, servers, and other hardware. Administrators can implement highly customizable rules on how USB devices are handled.

Our Honeywell SMX Client Dtriver (also known as TRUSTV2) offers additional features to enforce the scanning policy and granular control over exactly which USBs are allowed to connect. This rule configuration ensures seamless support for the list of authorized dongle-based license systems, cell phone, keyboard and mouse, USB extenders and hubs, allowing specific USB devices. This is easily tailored to the customer's needs. For example, this client didn't want any impact to their production, down-time, or interoperability issues with non-Honeywell plant control systems or security solutions.

So the implementation team had to move fast. Our team performed the SMX client software deployments, rules configuration, and ensure functionality in less than 15 minutes to ensure the shortest possible down-time for the customer. This is due to Honeywell's domain expertise and the flexible modularity of the SMX solution. Because of the pandemic, we were unable to visit the customer site to assess or perform the installation. However, our cyber experts were able to walk the customer through each step from the assessment to a successful installation through video call. The client then took advantage of our SMX change management program to help in the adaptation of the solution and the project was considered a success.

By controlling the access of incoming portable devices – and the potential threats that came in with them – this client achieved more than heightened security. They were able to achieve some peace of mind in an otherwise unpredictable cybersecurity landscape.

SMX can help to protect from more than just malware. SMX better protects critical networks from both malware and USB Attack Platforms (UAPs). UAPs can be used to log keystrokes, provide remote access and more!

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.becybersecure.com

Honeywell