CYBERSECURITY & IoT:

4 THINGS

YOU NEED TO KNOW

We are experiencing an influx of

interconnected (IoT) devices

for enterprises as organizations link all of their digital assets together—not just servers and personal endpoint computers. IT workers will be faced with growing challenges to control and enforce the protection of these huge, interconnected systems.

#1

INTERCONNECTED SYSTEMS ARE ONLY AS STRONG AS THEIR WEAKEST LINK.

If a single weak element is compromised, the rest of the system can be as well, including those that are supposedly more protected.

EX: An HVAC machine was used as an entry point in the 2014 Target security compromise.

#2

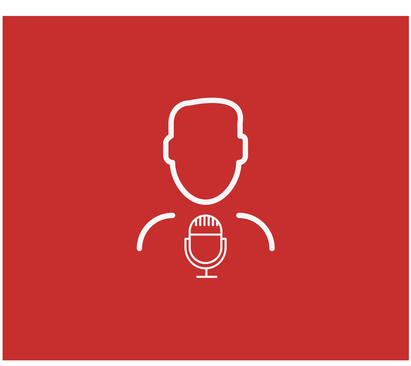
A PRODUCT'S SECURITY CAPABILITIES TAKE TIME TO DETERMINE.

Validation of any product's cybersecurity capabilities can only occur when a security product is deployed in a particular environment over time. Attackers must be given time to "test" a product's capabilities, so to speak.

#3

ENTERPRISES NEED A MORE HOLISTIC SECURITY APPROACH.

Security products should encompass a broader architectural view, including IoT. Solutions include a) leveraging the cloud and b) shifting focus to asynchronous environments, where applications can be disconnected when not in use.



#4

ENTERPRISES NEED TO PREPARE FOR A SECURITY BREACH.

Thorough and intelligent action plans are essential for handling PR and maintaining enterprise integrity when a cyberattack occurs.

Aragon Research