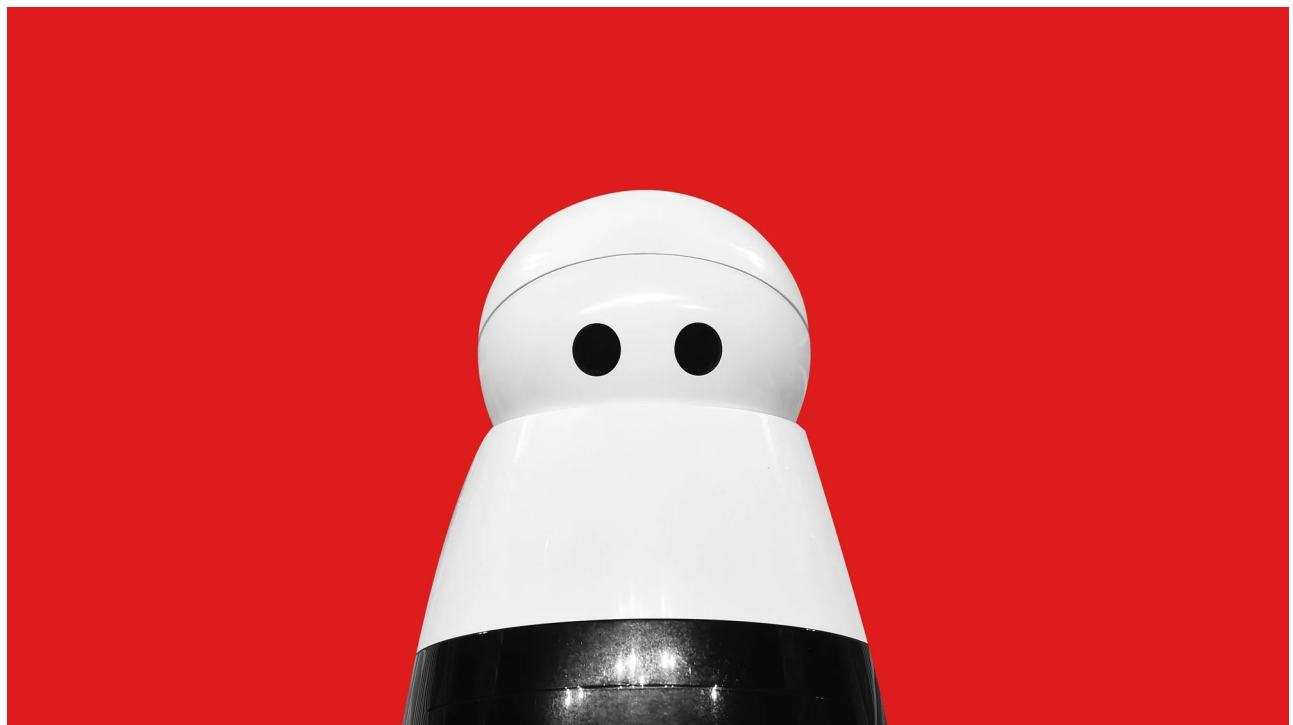




LILY HAY NEWMAN SECURITY 09.12.2019 08:00 AM

# It's Time for IoT Security's Next Big Step

Connected devices are more secure than ever. That's still not nearly enough.



IoT manufacturers are more responsive than ever to security bugs. Now it's time for phase two. PHOTOGRAPH: GETTY IMAGES

The [Internet of Things security crisis](#) has persisted for decades, producing a seemingly endless stream of under-secured consumer gadgets, corporate phones, printers, networking equipment, medical devices, and critical infrastructure sensors and controllers. By now, every industry has an IoT albatross around its neck. And though new devices are increasingly equipped with basic security protections, those minimum standards are just the beginning.

At the DerbyCon security conference in Louisville, Kentucky, last weekend, researchers stressed the need for connected devices to step up security beyond the basics. That means more visibility and logging features, along with better techniques for manufacturers, companies, and consumers alike to spot malicious activity. Protecting a device

[BUSINESS](#)[CULTURE](#)[GEAR](#)[IDEAS](#)[SCIENCE](#)[SECURITY](#)[SIGN IN](#)[SUBSCRIBE](#)



[BUSINESS](#)

[CULTURE](#)

[GEAR](#)

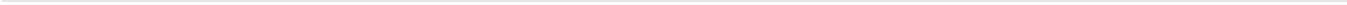
[IDEAS](#)

[SCIENCE](#)

[SECURITY](#)

[SIGN IN](#)

[SUBSCRIBE](#)



[BUSINESS](#)[CULTURE](#)[GEAR](#)[IDEAS](#)[SCIENCE](#)[SECURITY](#)[SIGN IN](#)[SUBSCRIBE](#)

[BUSINESS](#)[CULTURE](#)[GEAR](#)[IDEAS](#)[SCIENCE](#)[SECURITY](#)[SIGN IN](#)[SUBSCRIBE](#)