Bring Your Own (Exploited) Device

Your organization allows users to bring in their own devices. Or, another way to put it, they bring in their own exploited devices. The attackers use these devices to compromise your organization.

DETECTION

Firewall Log Review
Network Threat Hunting - Zeek/RITA Analysis

TOOLS

The completely asinine belief that somehow allowing people to bring their own devices in is a worthy cost savings.

https://www.blackhillsinfosec.com/pentesting-dropbox-on-steroids

CDV2_0421

Backdoors™ & Breaches™

INITIAL COMPROMISE