

CYBER ATTACKS ON CONSUMER BANKING INCREASING!

5TH YEAR RUNNING

BANKS ARE TOP CYBER ATTACKED SECTOR

(Source: IBM X-Force, 2021)



238% SPIKE

In cyber attacks on banks in 1st six months of 2020 (Source: VintWire Black)

RANSOMWARE
ATTACKS to
shutdown systems
& extort big payouts

PHYSICAL FRAUD
like stealing cards

CYBER FRAUD BY
BREAKING INTO
systems and networks

MAN IN THE
MIDDLE ATTACK

when a cybercriminal attempts to hijack an operation on a self service device

JACKPOTTING

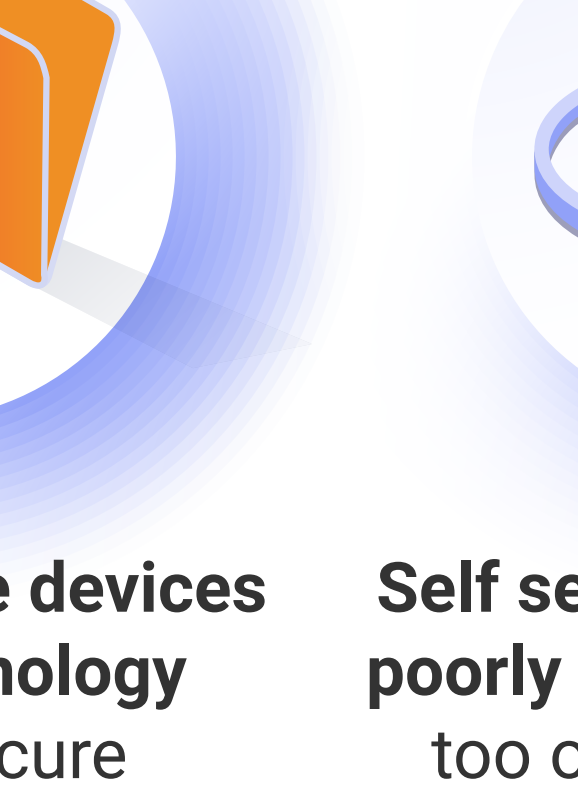
when a self service device is tricked into dispensing cash.

BLACK BOX
ATTACK

by connecting a device onto a self service devices



SELF SERVICE DEVICES ARE A SECURITY WEAK LINK



Self service devices contain sensitive data



Too many people have admin rights



Self service devices comprise lots of different hardware and software that make it difficult to get a full view of what's happening in terms of security



Some self service devices use older technology that's less secure



Self service devices are poorly monitored. Banks too often don't know how secure devices

A STRATEGY TO FIGHT BACK



1 **Control Operations**

- Fully control & reduce timing of on-site SW image deployment activities
- Fully control & monitor on-site self service devices maintenance activities

2 **PREVENT & MONITOR** unplanned onsite activities

3 **MAXIMISE SELF SERVICE DEVICES UP-TIME**

4 **PLAN FOR #NEXTGENBRANCH** securing digital banking channels, staff remote workstations and assisted self service terminals

5 **Adopt a holistic security solution to protect, monitor and control all banking endpoint assets.** Use a centralised multivendor security. Use LDM a centralised multivendor security offering with a layered protection model endpoint assets.

lookwise
DEVICE MANAGER

WHAT EFFECTIVE CYBERSECURITY FOR NEXT GEN BRANCH LOOKS LIKE



1 **Centralised and integrated multivendor security solution.** See, secure and manage all your endpoints including self service devices and ASSTs

2 **In real time you can see and protect everything with a layered protection model for self-service devices**

3 **Proactive monitoring, block, detect and solve fraud and security incidents fast, and effectively**

4 **Time and money saved thanks to remote and centralised cybersecurity operations on a single GUI**

5 **Strong cybersecurity doesn't get in the way of how to deliver easy to use, interconnected services**

6 **You can execute cybersecurity on devices remotely in a secure, controlled way**

7 **You enable modern, customer centric omnichannel next generation branch banking**

AURIGA the banking e-evolution

lookwise
DEVICE MANAGER