Two incidents, solved in minutes, for a US supermarket chain.

A US supermarket chain deployed Rebasoft, through a US partner, to see who and what was on its network and how it behaved. Two incidents show why: call-centre phones dropping out, and a zero-day outbreak that got its email domain blacklisted.

2
incidents traced to their source

Minutes
to find infected PCs after activation

≤ 2
devices per port: the policy that found a rogue switch

2015–18
annual renewals

THE INCIDENTS

- Call-centre phones randomly dropped out, so calls could not be made or received.
- A zero-day exploit turned PCs into spam senders and the email domain was blacklisted.
- The outsourced WAN monitoring could not see inside the firewall and only showed top users.

HOW REBASOFT FOUND THEM

- Phones: the user's phone showed IP addresses from both voice and data ranges, and a devices-per-port policy found the hidden switch bridging them.
- Zero day: NetFlow enabled internally, a profile of authorised email senders, and alerts for anything else sending email.

WHAT IT SHOWS

User to device to port
Users, devices and ports tracked over time, ready for troubleshooting.

Beyond Top-N
Infected PCs sending little traffic found by behaviour, not volume.

Security data, ops value
Data gathered for security solved operational problems.

Rogue edges found
An unmanaged five-port switch found under paperwork and removed.

No agents
Zero-day detection without depending on software on the PCs.

Automate next time
Policies can detect and remove offending devices automatically.

The outcome: two business-stopping problems traced to a single device each, in minutes rather than days.

WHY IT MATTERS FOR RETAILERS

Keep stores trading
Find the cause fast when systems fail.

See inside the firewall
The device, not just the site.

Behaviour, not signatures
Catch what antivirus misses.