USE CASE

BYOS

Byos' HANA-based Network Security for Retail

Retailers face a number of challenges in securing their networks

Retail networks have the widest scale of any industry, in terms of geographic dispersion, the sheer number of people served and customer data potentially exposed.

- Complex, remote, and highly dispersed networks with network equipment and ports that are often fairly accessible to visitors
  - » Legacy devices and restrictions on device patching & upgrades
  - » PoS & handheld equipment, sensors, cameras, physical security
  - » A network of devices shared amongst employees
  - » Access needed by vendors and more & more third parties
- IoT is expanding at as fast a rate as any other industry.
- Fast evolving technologies adds to the complexity
  - » Customer tracking & monitoring
  - » Self-service & guest access
  - » Asset & inventory tracking

Retail networks have multiple points of entry and it's often easy to move laterally upon initial compromise.

Addressing Complexity in Retail Networking

The ultimate accomplishment in reducing the threat surface is to make it completely invisible.

Byos' Secure Edge™ connects devices to the network so that they are invisible to all other devices on the network, as well as any bad actors trying to access them. This protection ensures that Byos-protected devices are only communicating with other credentialed and fully authorized devices. Any attempt to ping, scan, fingerprint, or interrogate a device is blocked by Byos, meaning widespread lateral movement from ransomware attacks is prevented.

Decrease Complexity for SecOps

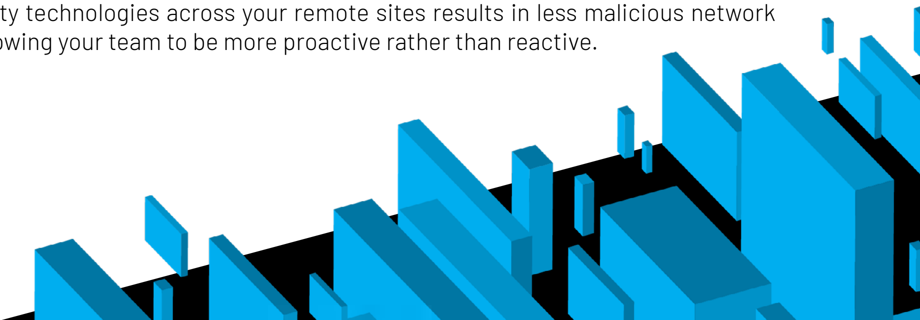
Security Operations is challenging. It is difficult to have full control of the network because of its distributed nature. Some devices simply aren't easily monitored or managed, particularly IoT & legacy devices.

Byos' Management Console aids SecOps teams in centrally controlling and managing their fleet of Byos-protected endpoints. The management console can be cloud-based or hosted privately/on-prem. It enables:

- Real-time policy provisioning of thousands of edge devices
- Secure remote access to endpoints inside the Byos-concealed network, without having to expose the network to the internet like traditional remote access technologies
- Instantaneous quarantining using a "ransomware killswitch" in the event of a security incident. The killswitch disconnects the Byos-protected endpoint from all network access , while allowing administration from the management console.

Because devices are disconnected, control is maintained. The need for remote access tools & processes is reduced, *shrinking the stack* for effective incident response. Not only are endpoints protected. Most Byos retail customers are making their network infrastructure - switches, routers, firewalls, etc. - invisible with administrative-only access.

Firewalls, VPNs, NAC, CASB, and Anti-DDoS are designed to protect devices inside the perimeter. At the same time, they created more work to manage. Reducing the number of security technologies across your remote sites results in less malicious network activity, reduced log events and alarms for the SOC, allowing your team to be more proactive rather than reactive.



How does Byos get deployed?

Byos' Secure Edge is deployed using different configurations for various retail use cases. Byos' core premise is that removing the network security stack from the CPU and operating system prevents the stack from being bypassed, disabled or modified. This approach is what allows Byos to block both the inbound and outbound traffic that reveal a device's existence to untrusted entities.

For Retailers:

- **Secure Gateway Edge** - a plug-and-play IoT gateway applicable for deployment in existing networks. It has two modes:
  - » Ethernet for wired use cases
  - » Wi-Fi hotspot for wireless use cases

The Secure Gateway Edge can be deployed with a number of different types of devices:

- » PoS devices
- » Workstations
- » Security Cameras
- » UPS systems
- » Fire Alarms
- » Compressors
- » PLCs, RTUs, HMIs, Industrial PCs

Key Outcomes:

- Reduced risk of a network-wide outage by preventing the spread of malware and ransomware
- Secure, Controlled remote access by third-party contractors
- Secure Resource Management and Monitoring

If you'd like to learn more about Byos visit us at byos.io

or connect with us at engage@byos.io