USE CASE

BYOS

Zero-Trust Networking in Hospitals

Network security in hospitals is the most demanding of any industry

Ensuring the continuation of operations is a year-round endeavor. A vital part of that delivery is the infrastructure that supports these facilities. Network Security has become one of the highest priorities for hospitals and health systems.

Hospital facilities require complex and highly segmented networks for a multitude of applications and their supporting devices. These include:

- Private and Public WiFi VLANs
- Multiple VLANs
- 5G Connectivity
- Tele-Medicine
- Legacy Applications

With the expansion rate of IoT across hospitals, these IoT networks now carry data for a myriad of other devices including:

- Mobile Medical Devices
- Real Time Location Services
- Voice Over WiFi
- Lighting Controls
- Temperature Controls
- Smart TVs
- Smart Beds
- Fire Suppression Systems
- Elevator and Door Systems

Hospitals and health systems now have a threat surface area well beyond what was initially imagined - there is a clear need for more cohesive and comprehensive network security, that can cover the threat surface area that includes the visible IT Network and the vast, ever expanding OT network.

Most hospitals and health systems have lots of low-hanging entry points, are not aware of how many devices are connecting across their networks and so it's often easy for attacks to move laterally upon initial compromise.

The most pressing cybersecurity challenges facing hospitals

The only way to cure these challenges in securing hospital networks is to greatly simplify the management complexity and the components securing all the "moving parts". Hospitals' complexity challenges can be broken into three primary categories - **Threat Surface, SecOps, and Risk**. We architected our technology to address all three cohesively.

Threat Surface

SecOps

Risk

Reducing a sprawling threat surface

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

The **Byos Secure Edge™** is a microsegmentation technology that makes devices and networks invisible by letting devices communicate "on the network" without being connected "to the network". It isolates devices onto their own 'network of one' providing:

- **Inbound protection from malicious networking attacks:**
  - » "First-hop" protection across OSI Layers 1-5
  - » All attempts to scan, fingerprint, or enumerate the device are dropped at the Byos Edge.
- **Outbound traffic protection and control:**
  - » Network Access Control (NAC)
  - » Route enforcement
  - » Traffic anonymization through layer 4+ data encapsulation and exit node enforcement

By separating the network from every device's CPU and operating system, Byos prevents every device from revealing its identity to anyone or be able to be discovered by any other peer device on the network - preventing any lateral movement.

Key Differentiators

Byos is the only solution of its kind. Byos was created to solve the gap in protection that exists between network security technologies on the perimeter/in the cloud and the protections offered by security software installed on a device's OS.

Byos combines a mix of network and endpoint security capabilities into one solution that is easy to deploy and manage, including: segmentation, NAC, DNS + FW, policy administration, UTM, and malware protection.

Decreasing the complexity of SecOps

Security Operations teams operate in a challenging environment. It is extremely complex and difficult to have full control of the network because some devices simply aren't easily monitored or managed (IoT & Legacy).

The **Byos Management Console (MC)** aids SecOps teams in centrally controlling and managing their fleet of Byos-protected endpoints. The MC is cloud-based but can also be hosted in a private cloud or on-prem and enables:

- Real-time security policy provisioning to thousands of Byos Secure Edges
- Secure Remote Access to an endpoint in the Byos 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. This cuts internet access to the Byos-protected endpoint, but lets the Administrator still communicate with the endpoint through the MC.

Because devices are invisible to the network and control is maintained at all times, the need for a large number of tools & processes is reduced, shrinking the stack for effectively managing SecOps. Firewalls, VPNs and NAC were designed to protect devices inside the perimeter, but have created more work to manage. Fewer security technologies and less malicious network activity means a reduced number of logs, events and alarms in the SOC, allowing your team to be more proactive rather than reactive.

Minimizing Risk & Addressing Compliance

After conducting a risk assessment and knowing what is on your network, establishing access controls is the next step. Following Zero Trust principles and best practices, Byos enables true granular access control to the Byos-protected endpoints. Out-of-the-box, Byos helps organizations achieve "absolute least privilege" for users, roles, devices, ports and networks and is the first step in implementing zero trust networking.

Byos has implemented the best practice policy of default-to-deny in our administration & reporting modules. Administrators can create specific remote access policies without giving overly broad access to the network.

How does Byos get deployed?

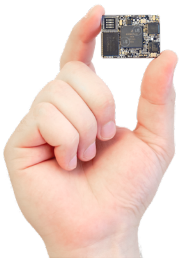
The Byos Secure Edge technology is deployed using different form factors for different use cases within Healthcare networks. The core premise of Byos is that all networking traffic needs to pass through Byos before reaching the underlying device's Operating System (OS).

For Hospitals:

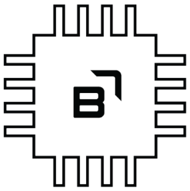
- **Secure Gateway Edge** - a plug-and-play IoT gateway applicable for deployment in existing networks. It has two modes:
  - » Ethernet for wired use cases
  - » Wi-Fi hotspot for wireless use cases

For Medical Device Manufacturers (MDM):

- **Secure Embedded Edge** - For custom and specific secure connectivity applications, the Byos System-on-Module can be embedded onto the medical device's motherboard, sitting between the Network Interface and the CPU.



- **Secure Firmware Edge** - For MDMs that want a full software deployment, the Secure Firmware Edge can be installed inside of the medical device, sitting between the OS and the network interface.



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

or connect with us at engage@byos.io

Medical Device Manufacturers have a unique set of challenges that requires them to properly secure their devices. They are also frequently faced with challenges in updating, and servicing their medical devices deployed inside of healthcare facilities.