Soliton LAP One™

Network Access Control for SMB – Without the Hassle!

Network Access Control – It's Not Just for Large Enterprises

It's easy to believe that smaller companies are less likely to be targets of attacks, but as large companies beef up network security, threat actors are increasingly focusing on mid-tier firms. And while the danger of outside attacks is all too real, most security breaches are not the result of malicious intent. Contrary to popular belief, most are accidental or the result of insiders' non-adherence to company policy.

Today's corporate networks serve a mobile workforce with a wide variety of traditional and non-traditional devices and other endpoints– everything from PCs, tablets and smartphones to devices that make up the Internet of Things (IoT). The challenge is that many small- to medium-sized businesses lack visibility into what devices – a number of which are not necessarily managed and controlled by the organization – are accessing corporate resources.

LAP One™ - Simple NAC, No Complexity

Network Access Control (NAC) can be an excellent tool to control and restrict access to network resources. In addition to supplementing a firewall defense strategy, it can protect against the possibility of an infected device getting on the network and spreading nastiness. However, because NAC was designed for larger organizations, it can be costly and complicated to deploy.

LAP One Changes Everything.

Purposely designed for mid-tier firms as well as enterprises with branch offices looking to manage remote devices and sub-networks, LAP One is easy to deploy, simple to manage and cost effective. It can be integrated into any infrastructure, so that you can start realizing the value within minutes of installation.

LAP One provides continuous monitoring and real-time visibility into devices that are already connected or are attempting to connect to your network – without the complexity and cost of traditional Network Access Control. Plus, it automatically detects and blocks unauthorized devices, regardless of location, time-of-day or endpoint type.

Take Back Control of Your Network

Keep unregistered devices off the network without the hassle of traditional Network Access Control.

- Detect connected devices as well as unauthorized and malware-infected devices trying to connect
- Determine whether devices are authorized to connect
- Block unauthorized connections and unregistered devices

Know What is On Your Network

Get real-time visibility of authorized and unauthorized devices the instant they access your network.

See all devices on the network

- Drill down on details of allowed and blocked devices
- Get information about host names, operating systems and IP addresses

Manage Device Access

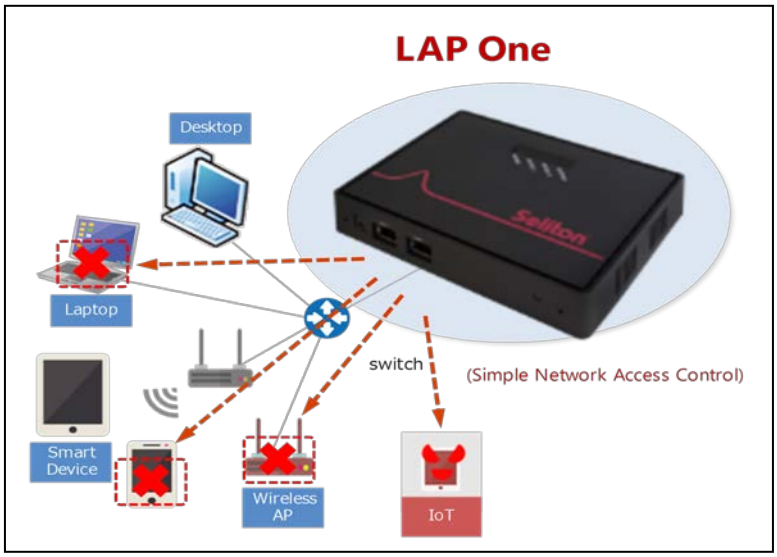
Get granular control over network devices – and allow access as you see fit.

- Enroll authorized devices quickly and easily
- Add unregistered devices from a simple web form
- Allow users to request access via email
- Notify users regarding blocked devices

Detect and block unauthorized devices that try to connect to your network without the complexity of Network Access Control.

Gain Visibility Into IoT Devices

From connected surveillance cameras and networked printers to Smart TVs and digital signage, Internet of Things (IoT) devices are proliferating. Users often don't ask for permission before connecting – but each new device that comes online represents another attack vector. The challenge is that most IoT devices are not designed with security in mind and are thus vulnerable to cyberattacks. Knowing what devices are connecting to your network has never been more difficult – and more critical. Trust LAP One for visibility into IoT devices connecting to the network.



Secure Networks at Remote Offices and Branches Outside of Headquarters

The LAP One Advantage

- Standalone Solution. LAP One offers flexible and affordable network access control.
  - Easy-to-use interface
  - ARP jamming
  - Up to 512 devices
  - One or two network segments
- NAC for the Mid-tier and Remote Office. LAP One acts as a mini enforcer to extend access control to locations with a small amount of subnets and users, and is ideal for mid-tier and enterprises that need to secure networks at remote sites.
- Plug & Play Installation. LAP One plays nice with your network.
  - Installs in under 15 minutes
  - Simple 3-step configuration with the RADIUS server
  - Integrates with NetAttest LAP Manager and ForeScout CounterACT
- Self-learning. LAP One initially starts in learning mode for network discovery, and automatically switches to jamming mode at a specified date and time. From then on, unknown or unregistered devices will be denied access until administrator action is taken.
- Device Jamming. LAP One offers two jamming modes:
  - Block access; Inform admin
  - Allow access; Inform admin
- Basic/Advance Modes. LAP One offers two operating modes:
  - Basic: LAP One looks only at the device's MAC address
  - Advanced: LAP One looks at the IP address, host name and device operating system
- Live Monitoring by Web Interface. LAP One continuously scans the network. Administrators receive an email notification when an unauthorized device is detected.
- Data Privacy. Complete privacy is guaranteed. LAP One does not send any data "outside" the network.
- Device Management. Simple, yet powerful, administration options allow you to:
  - Monitor all devices from a central console
  - Grant or deny access
  - Include remarks that identify the purpose of a device
  - Notify user of blocked device (don't notify, message only, message and offer request access form)

Contact Us Today to Learn More About Soliton.

Soliton Cyber & Analytics | +1-714-243-6121 | sales@solitonca.com

Soliton creates solutions that make complex problems simpler to solve. Our enterprise security and authentication solutions help organizations keep their data safe in today's challenging and uncertain world.