UPLOGIX

> Solution Brief

Open or Closed Appliances in Your Network

Do you really have to choose flexibility over security and reliability when choosing a console server?

Uplogix is the most intelligent, secure out-of-band platform

When it comes to putting an appliance in your network for out-of-band management, you want to think carefully about whether that appliance is based on an open or closed platform. It might just be the difference between locking up network security and being open for business for hackers.

Building on Linux: Open source doesn't have to mean open access

A Linux platform lends itself to building an out-of-band management appliance, but an important decision is what's more important—flexibility or security and reliability.

If you keep the appliance open, it's possible to access and tweak OS settings and create and run scripts on the platform. You can install other programs that can run alongside the OOB management software, and you can patch Linux functionality without patching application software.

However, this flexibility to install other apps means that things can go wrong too. On the non-malicious side of the equation, these could be changes that modify or delete files critical to normal operation of the appliance and impact performance. But truly bad things could happen as well. Scripts and software can be installed through an encrypted SSH session, with changes made to the appliance outside of the application. This means they could be undetected and not show up in logs or audits. Encrypted passwords and keys can be accessed and exported.

Not all security threats are outside the firewall

Suddenly you have a device that you might not be able to trust that is connected directly to your network infrastructure over the console port, which isn't monitored by your IDS/IPS systems. Sounds scary, right?

Uplogix Key Security Capabilities

- Maintain and enforce AAA (Authentication, Authorization and Accounting of the state of the network. Under normal circumstances, Uplogix Local Managers (LMs) integrate with remote multifactor authentication mechanisms, such as TACACS and Radius, but if connectivity is lost, the LM can failover to other AAA servers before falling back on cached authentication data to maintain authorized access.
- Prevent unauthorized user access by automatically closing idle sessions, eliminating a potential security gap. Uplogix also ensures that the right users have the right access by enforcing granular, role-based permissions.
- Enable audit and compliance reporting by constantly logging all changes made to managed devices and the results of these changes.
- Eliminate modem security issues with CallHome™ connectivity. Uplogix appliances always "dial-out," never allowing in-bound dial-up requests, to restore connectivity when the primary network connection goes down, closing common security holes.
- Improve overall security by restricting access to specific IP addresses and encrypting passwords stored in the database, and by automating management functions related to security enforcement, like updating the access passwords on hundreds of managed devices at once.

Find out more at uplogix.com.

Uplogix extends role-based administrative access policies to devices with detailed auditing and reporting for compliance when the network is up, or down.

Uplogix is a closed platform

Uplogix is a secure, closed appliance. The underlying Linux OS does not have root access, ensuring:

- No direct access to the OS for higher security and reliability
- Secrets are kept from users (passwords and keys)
- Non-approved scripts and software cannot be installed
- The application software and configuration integrity is maintained

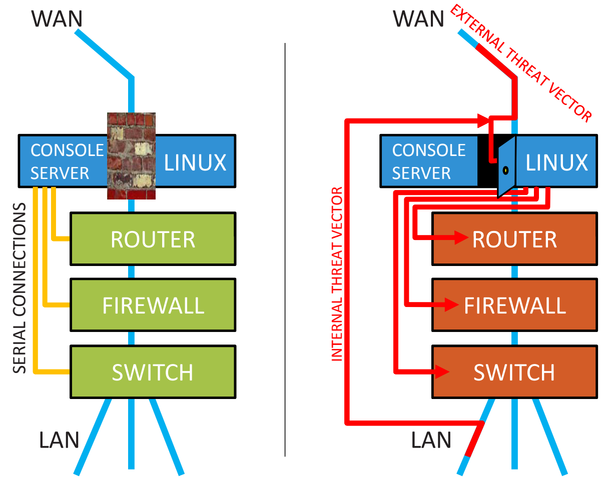
Beyond the separation from the OS, the Uplogix platform is FIPS 140-2 Level Two Certified -- not just a component of the solution like a FIPS-certified Open SSL library. Our solid state hard drives are available with AES-256 disk encryption, and only the SSH port is open by default.

FEDERAL INFORMATION PROCESSING STANDARD
FIPS 140-2
★ LEVEL 2 CERTIFIED ★

With Uplogix, all product configuration and features are governed by powerful and granular authorization features with every activity and change logged and archived to the NOC. With features that automate device monitoring, maintenance and recovery, scripting isn't necessary, avoiding another threat vector.

We take you out of the danger zone

Network security is more critical than ever. These are the security features initially demanded by and developed for customers in finance and the military. You need to know that your network is locked down inside and out and be able to prove it. With the average cost of a security breach increasing yearly, what business today doesn't need reliable network security?



Uplogix is a secure, closed appliance. The underlying Linux OS does not have root access, which eliminates threat vectors possible with an open console server.

About FIPS 140-2 Certification

The Federal Information Processing Standard (FIPS) designates requirements for hardware and software components used by federal agencies and departments.

The Uplogix Platform meets the requirements for FIPS 140-2 Level 2 certification from the National Institute of Standards and Technology (NIST).

Enhancements to the already-significant security features in Uplogix meet or exceed government standards for the protection of data and information captured and stored by Uplogix appliances. Addition physical requirements include tamper-evident seals and visual obstructions.

ABOUT UPLOGIX // Uplogix provides the industry's first local management solution. Our collocated management platform automates routine administration, maintenance and recovery tasks—securely and regardless of network availability. In comparison, traditional network and systems management depends on the network, uses multiple tools, and remains labor intensive. Uplogix puts the power of your most trusted IT administrator everywhere, all the time.

Uplogix is privately held and headquartered in Austin, Texas. For more information, please visit www.uplogix.com.

www.uplogix.com | Headquarters: 7600B N. Capital of Texas Hwy. Suite 220, Austin, Texas 78731 | US Sales 877.857.7077,