LiveAction

LiveNX Hardening Document

QUICK GUIDE

ver. 24.2.0a

Summary

LiveAction is committed to providing our customers with secure applications and secure infrastructure that hosts our applications. LiveAction provides a single software image (or appliance) that incorporates everything including applications, infrastructure, tools. LiveNX is a hardened system using Ubuntu Linux 22.04 LTS

LiveAction takes ownership of keeping this image secure including latest relevant security updates. The LiveNX software image has been hardened following industry best practices. These include a minimal set of dependencies and services, restricted user access, and a secure set of firewall rules for the LiveNX software image. In addition, the LiveNX software image has been constructed as a read-only environment, with most changes stored temporarily in memory.

Any third-party software or files installed outside of persistent data stores, such as /etc, /home, or /var, will be completely lost on reboot or shutdown. Customers will not be able to customize the LiveNX software image

Software Infrastructure

- LiveAction includes the latest OS software packages for every build, ensuring the OS has all the latest security updates at the date and time of the build.
- Some third-party software packages are upgraded by LiveAction only after determining the upgrade is consistent with LiveAction software operation, but LiveAction ensures all third-party software passes LiveAction's vulnerability scans for every software release.
- LiveAction software images/appliances are essentially read-only. Although LiveAction cannot prevent users from installing additional software, all added software will not persist a system reboot, thereby returning the system to the secure state in which it was shipped

Security Patching and Timing

LiveNX release are issued every quarter.

- CVSS high (7-10) vulnerabilities identified prior to release, through internal testing or from an external source, is remediated immediately.
- CVSS medium (4 - 6) vulnerabilities identified after a release will be patched in minor release.
- CVSS low vulnerabilities will be patch on subsequent quarterly release.

Secure Development

- LiveAction utilizes a 3rd party external firm for yearly penetration testing.
- LiveAction utilizes CodeQL and Qulalys to continually scan LiveNX code in addition to 3rd party external testing.

Penetration Testing

Penetration testing is performed regularly by a certified penetration tester on LiveAction's security team or an independent third party.

Findings from a vulnerability scan and/or penetration test are analyzed by the Security Officer, together with IT and Engineering as needed, and reported through the process defined in the next section.

Security Findings Reporting, Tracking and Remediation

LiveAction follows a simple vulnerability tracking process using Jira. The records of findings are retained for 7 years.

Product Security Practices

- 256-bit AES encryption for application settings and network device credentials.
- Hard-coded passwords are not supported.
- Network Device credentials are encrypted when stored locally using 256-bit AES.
- Server to Node communications are encrypted via TLS 1.3.
- Client to Server communications are encrypted via TLS 1.3 if supported, otherwise TLS 1.2.
- Underlying databases are not remotely accessible.
- LiveAction offers the option of self-encrypting drives (SEDs) in our appliances to address the need to encrypt data-at-rest. Non-encrypting hard drives are the default configuration

Network Protocol Requirements

The following table is a list of required network protocols for normal operation of the LiveNX platform. This can be used as the basis for any firewall rules required.

Network Port Requirements

Port	Protocol	Usage
22	TCP	SSH
161	UDP	SNMP Polling
443	TCP	User Access to Web
2055	UDP	Netflow export
6343	UDP	sFlow export
7000	TCP	Java Client access
7026	TCP	Server to Node communication
8092	TCP	Web Server
8093	TCP	Rest API
8443	TCP	HTTPS for LiveAdmin
9443	TCP	Cloud Monitor API

IDRAC (out-of-band LiveNX Management)

Port	Protocol	Usage
22*	TCP	SSH
23*	TCP	Telnet - recommend blocking
80*	TCP	HTTP - recommend blocking
161*	UDP	SNMP
443*	TCP	HTTPS
623	UDP	RCMP/RCMP+
5900*	TCP	Virtual Console Keyboard & mouse redirection
5901	TCP	VNC

* indicates configurable ports

Attack Protection Vectors

- The kernel and operating system have been hardened with industry best practices.
- The appliance is a read-only environment with a temporary in-memory file system mounted over '/'.
- All changes to '/' are lost on reboot/upgrade.
- Exceptions apply; changes to /etc, /home, and /var. All persistent data is stored in dedicated partitions/ volumes.
- The appliance is constructed using a minimal number of software dependencies and tools. In addition, only services dedicated to the functioning of our product are running by default.
- LiveNX cryptographic modules deployed for TLS and SSH communication (through OpenSSL system library), are configured with WolfCrypt FIPS 140-2 certified cryptography module (certificates #4605)
- The appliance is shipped with a restrictive set of firewall rules which reduce the public facing attack surface.
- LiveNX and its dependent services, such as InfluxDB and MongoDB, run under non-root system level accounts. This prevents these services from having sudo level access to the underlying system.
- All upgrades are manually triggered events, which require user input, to properly upgrade the appliance. This would prevent automatic supply chain attacks like the SolarWinds attack.
- Each release of the products will always be updated to address any security vulnerabilities as of the day of software release. Vulnerabilities found after software release will be addressed as outlined in the section titled Security Patching and Timing.
- On AWS and Google Cloud deployments, SSH password-based authentication is disabled, allowing only key based authentication. Azure gives users the option to choose password or key based authentication. All appliances ship with root account disabled

LiveAction Recommendations

- In general, LiveAction strongly recommends users avoid installing and running third-party software on LiveAction appliances. Installing third-party software could have unintended consequences in the functioning and/or performance of LiveAction software and will jeopardize support of the product. Adhering to this policy ensures better system reliability and proper functioning of the software while maintaining a consistent system for future updates.
- LiveAction recommends all security scans be scheduled and performed with agent-less, network-based scanning tools. This will guarantee the appliance is not affected in any negative way with the addition of third-party software while providing the necessary security insight of the installed system. Should a security-related issue be found, a necessary product update will be made available through the supported update mechanism.
- LiveAction recommends that you update the default firewall settings after deploying LiveAction software to close any unused ports.