Lucent Sky

Lucent Sky AVM accelerates and scales the identification and remediation of common categories of application vulnerabilities, such as those in OWASP Top 10 and PCI DSS. Source code, binary, and software composition analysis identify vulnerabilities in source code, libraries, and external components. Remediation algorithms then automatically generate secure code replacements that functionally fix those vulnerabilities.

Lucent Sky AVM is compatible with most web, server, mobile, and desktop applications, as well as static websites and database systems. It is accessible through a web interface, IDE extensions, CLI, and API, and integrates with ALM and CI systems.

Compliance

Lucent Sky AVM follows industry standards and best practices to remediate vulnerabilities. Users can also review and modify the security libraries used for remediation or even use their own. This approach enables increased automation while maintaining compliance.

By strengthening application security, Lucent Sky AVM helps organizations meet standards such as PCI DSS and HIPAA and regional regulations such as GDPR and CCPA.

Lucent Sky AVM is Officially CWE-Compatible.

System specifications

Enterprise Edition Appliance
Two 4.0 GHz 16-core processors
CLEAR Engine (6,144-core)
ML coprocessor (192-core)
512 GB memory
2 TB solid-state storage
Windows Server 2022

System requirements

Standard Edition
Two 1.6 GHz x64 processors
4 GB memory
40 GB hard disk space
Windows Server 2012 or newer

Enterprise Edition
Two 1.6 GHz x64 processors
16 GB memory
40 GB hard disk space
Windows Server 2012 or newer

Security standards and vulnerability categorizations

- CVSS
- CWE, CWE Top 25, and CWE/SANS Top 25
- OWASP ASVS, OWASP Top 10, and OWASP Mobile Top 10
- HIPAA, MISRA C/C++, PCI DSS, and other industry standards

Application frameworks and languages

- .NET (C# and VB.NET)
- Active Server Pages (VBScript)
- Android (C#, Dart, ECMAScript, Java, and Kotlin)
- C and C++
- Go
- iOS (C#, Dart, ECMAScript, Objective-C, and Swift)
- Java (Groovy, Java, and Scala)
- PHP
- Python
- Ruby
- Visual Basic
- Other cross-framework languages and data interchange languages

Database

- SQL Server and SQL Azure
- MySQL
- Oracle
- Access, DB2, PostgreSQL, and other database systems

IDE, ALM, CI, and revision control

- Visual Studio, Visual Studio Code, and Eclipse-based IDEs
- Azure DevOps, BitBucket, GitHub, GitLab, Jenkins, Team Foundation Server, and other ALM and CI systems
- Ant, Gradle, Maven, MSBuild, sbt, and other build systems
- Git, TFVC, and other revision control systems

LUCENT SKY

Lucent Sky AVM accelerates and scales the remediation process

96% of applications have vulnerabilities—known security risks that bad actors can exploit.

The main hurdle of implementing any security process is the actual remediation of vulnerabilities found. Developers and security engineers simply don't have the capacity to resolve vulnerabilities efficiently.

Application's source code, binary files, and external components are scanned for vulnerabilities.

Instant Fixes are automatically generated for identified vulnerabilities and false positives are removed.

Remediated code is reviewed by developers, then sent to testing and deployment.

How does Lucent Sky AVM work?

- Lucent Sky AVM uses a combination of source code, binary, and software composition analysis to accurately identify vulnerabilities in source code, libraries, and external components. Patented remediation algorithms then automatically generate Instant Fixes — secure source code that functionally fix these vulnerabilities.
- The generation of an Instant Fix has two parts: finding the ideal location to fix a particular vulnerability, and generating actual code replacement using industrial standard security practices and security libraries.
- Users can configure Lucent Sky AVM to use their own security libraries. This allows Lucent Sky AVM to work with pre-approved security libraries in settings requiring strict adherence to compliance requirements.

Every SSDLC is different. Lucent Sky AVM is built for versatility: whether integrated with your automatic CI process, or manually run directly before an external security audit

- The only solution that provides automatic code-based remediation, "Instant Fixes", to common security vulnerabilities such as SQL injection, cross-site scripting, and privacy violations.
- Vulnerabilities are remediated using industry best practices and proven security libraries such as ESAPI and WPL, with support for custom enterprise security libraries.
- Includes binary analysis, source code analysis, and software composition analysis to find and fix vulnerabilities in internal source code and external components.
- Built for software developers and security experts alike, and tightly integrates with SDLC to secure applications efficiently without changing workflow.

Whether at the start, middle or end of the SDLC, Lucent Sky AVM accelerates and scales the process of securing application source code

Development lifecycle: Remediate vulnerabilities as they are identified, in the comfort of development environments and before new code is checked in.

Security review: Provide actionable reports to developers when vulnerabilities are found in security review.

External audit: Scan and secure code prior to an external audit. Instant Fixes allow developers to resolve vulnerabilities right after a scan to greatly increase application security. Vulnerabilities are prioritized to allow developers and auditors to focus on the most pressing issues.

Lucent Sky

United States
717 Market Street, Suite 100
San Francisco, CA 94103
United States
1-415-377-9797

sales@lucentsky.com

Asia Pacific
207 Dunhua S. Road Section 2, Floor 16
Taipei 10602
Taiwan
886-2-8722-0179