Lucent Sky AVM accelerates and scales the identification and remediation of more than 20 categories of application vulnerability, such as those in OWASP Top 10 and PCI-DSS. It is compatible with applications developed for .NET, ASP, Android, C/C++, iOS, JDK, PHP, Python and most database systems, and integrates with popular IDEs and ALMs. Lucent Sky AVM is broadly accessible, and includes a web interface, IDE plugins, CLI and API.

Compliance

Lucent Sky AVM allows users to review and alter mitigation libraries, as well as to upload their own. That means nothing will be inserted in source code without prior approval. Such an approach allows for increased compliance and automation.

Lucent Sky AVM help organizations meet the following PCI Data Security Standards: 3.1, 3.2, 3.4, 4.1, 6.3, 6.5 and 6.6.

Lucent Sky AVM is Officially CWE-Compatible.

System specifications

Enterprise Edition Appliance
Two 3.0 GHz 12-core processors
CLEAR Engine (3840-core)
512 GB memory
Four 1 TB solid state drives, RAID 10
Windows Server 2016

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

Vulnerability categorizations

- CWE
- OWASP Top 10 (2010, 2013, 2017), Mobile Top 10 (2014)
- PCI-DSS (v3.2)
- SANS Top 25 (v3.0)

For a complete list of supported vulnerability categories, their CWE IDs and mappings to lists such as OWASP Top 10, PCI-DSS and SANS Top 25, visit http://lsky.co/kb685905.

Application frameworks and languages

- .NET Frameworks 2.0 - 4.7 (C# and VB.NET)
- Active Server Pages 3.0
- Android SDK 10 - 28 (Java and Xamarin)
- C89 - C11 and C++98 - C++14
- iOS 6 - 12 (Objective-C, Swift and Xamarin)
- JDK 1.5 - 8
- PHP 4 - 7.2
- Python 2 - 3.7

Database

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

IDE, ALM, CI and revision control

- Visual Studio 2012 or higher
- Eclipse 4.4 or higher
- TFS 2012 or higher, including Visual Studio Online
- MSBuild, Maven, CruiseControl, Jenkins and other build systems and ALM and CI systems
- CVS, Git, Mercury, Subversion 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 hackers can exploit.

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


Application source code and libraries 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 and binary analysis, and proprietary mitigation algorithms, to identify vulnerabilities and insert Instant Fixes into an application's source code.
- 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 upload and configure Lucent Sky AVM to use their own security libraries. This allows Lucent Sky AVM to work with pre-approved mitigation 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, or Instant Fixes, to common security vulnerabilities such as SQL injection, cross-site scripting, path manipulation and privacy violations.
- Monthly updates to support new frameworks and the latest technology stacks you are using.
- Includes industry-standard security libraries such as ESAPI and WPL, as well as customizable security libraries.
- Built for use by application developers and security experts alike.
- Tightly integrates with your software development lifecycle—efficiently secure applications without changing your current workflow or development tools

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 the IDE or 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
886-2-872-20179