# CLARINET BY HARMAN

**THE MOST COMPREHENSIVE AND EXTENSIBLE FRAMEWORK FOR INFRASTRUCTURE SECURITY AGAINST VULNERABILITY**

## KEY FEATURES

1. Security Patch Checks & Vulnerability Assessment
2. Use of NIST, DoD, and other SCAP-based Security Content Automation Files
3. Configuration Remediation & Undo
4. Standards-Based Assessment System
5. Security Reporting & Data Export
6. Metadata validation and aggregation

## INTRODUCING CLARINET

Security is always a primary concern for enterprise IT managers, with a constant need to ensure that systems are kept updated and properly configured to prevent exploits. Clarinet is a new generation security compliance and remediation solution that offers standard for automating vulnerability management and policy compliance with mandated security configurations.

Harman releases security definitions and patching tools every month that gets used to scan machines for compliance check and patching them when vulnerabilities are discovered, ensuring complete security and compliance of the machines. Clarinet integrates with endpoint management tools like Marimba to offer comprehensive Auditing, Management and patching. Clarinet uses big data engine for archival data. It provides out of the box integrations with Kibana. Clarinet comes with a management console for advanced reporting and targeting.

## USE CASES

1. Security Configurations
2. Vulnerability Assessments
3. Security auditing and compliance
4. Scap 1.2 validations
5. Audit and Drift

## PLATFORM SUPPORT

- ✓ Windows: Windows 10, Windows 8.1, Windows 7, Windows XP, Windows Server 2003, Windows Server 2012, Windows Server 2016
- ✓ Linux: RHEL 5+, Fedora 14+, SUSE Desktop 10+, SUSE Enterprise Server 9+, Ubuntu 8.10+, Debian 6.0+
- ✓ Apple: OSX Snow Leopard+
- ✓ IBM AIX 6.1+, RHEL 6+ on System Z
- ✓ Oracle Solaris 8+
- ✓ HP-UX 11.23+