

The solution you need for continuous IT application security compliance. The evidence you need for security audits and application risk management.

- Accelerates compliance audits and ATO's with automation and evidence – eliminates manual verifications with screen captures
- C2VS pluggable architecture is designed from the ground-up to deliver a comprehensive compliance solution tailored to your highly custom application designs and deployments
- Provides out-of-the-box compliance controls and NIST 800-53 reports for OS, application servers, databases and cloud resources
- Continuously identifies misconfigurations between multiple environments at scale
- Assists information Security, Configuration Management, DevSecOps, and Application Developers in identifying and remediating mis-configurations

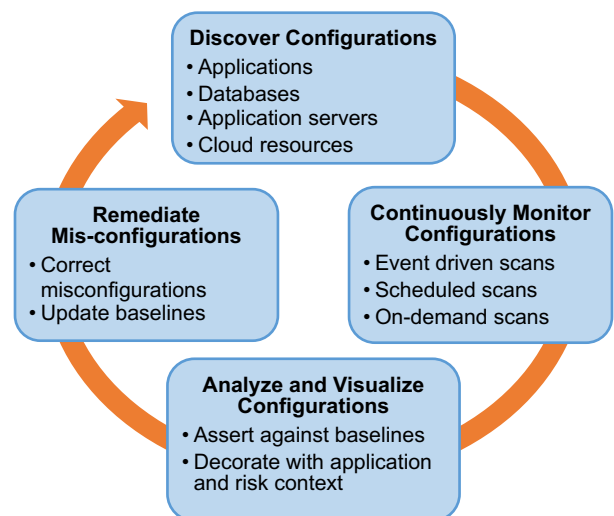
Do You Treat App Configurations as First Class Citizens?

- Does it take a long time and manual steps to conduct security audits?
- Do you have continuous visibility into your application configurations?
- Do you have the visibility into your database configurations that are specific to your application needs?
- Do you know the gaps in hardening vendor product installations and configurations in your environment?
- Can you assess the risks associated with security misconfigurations at all times?
- Can you compare two application environments?
- Can you track the drift in configurations in your environments?
- Can you understand the context of a misconfiguration and identify the root cause immediately?

If the answer is "NO" to one or more of these questions, C2VS is the answer

U3C - Our Solution Model

Our model is a Unified Capitis Configuration Compliance (U3C) solution that connects all layers of security



Cloud Native Apps Config Overload – Misconfigurations Challenge

- Defense-in-depth strategy is leading to new security controls with more configurations
- More environments are created at higher frequencies
- Modern microservice architectures promote more deployable units
- Infrastructure-as-Code and Platform-as-Code creates more configuration properties
- Daily and weekly release candidates are becoming a common practice
- More configuration parameters for performance tuning and efficiency

C2VS is a Highly Customizable Independent Compliance Solution Designed to Identify your Application Specific Misconfigurations and their Root Cause Automatically and Repeatably.

C2VS Use Cases and Value Proposition

ATO approval process	Information Security Audits	Continuous monitoring of production environments	Integrate with CI/CD pipeline	Consistency between environments
<ul style="list-style-type: none">• Scan environment to be approved• Provide evidence that configurations are correct• Expedite the ATO process• Eliminate manual effort & errors	<ul style="list-style-type: none">• Scan production environments• Analyze C2VS scan results• Remediate any issues immediately• 100% coverage verses manual spot checks	<ul style="list-style-type: none">• Trigger scans whenever configurations are changed• Analyze results and compute risk posture• Notify security and Ops engineers for immediate action	<ul style="list-style-type: none">• Initiate C2VS scans following the deployment of every Dev, QA or Prod environment• Identify misconfigurations and remediate	<ul style="list-style-type: none">• Initiate scans concurrently in Active and DR sites• Identify inconsistent configurations between the two environments• Remediate before the disaster occurs

At a major financial institution, our solution automates hundreds of thousands of compliance checks saving 1,000's of hours of manual compliance efforts per year.

Engagement Model

- Capitis professional services team customizes C2VS for your custom applications and CI/CD pipeline
- Configuration compliance coverage increases from a few spot checks to 100% continuous coverage
- Capitis transfers knowledge to your team for on-going operations and maintenance

Out-of-the-box Compliance

- Java Stack: Tomcat, Apache web server, Linux OS
- .NET Stack: IIS, .NET Apps, Windows OS
- Databases: Oracle, SQL Server, MySQL, Postgres
- AWS Cloud : EC2, ECS, Lambda, RDS
- AWS Integration: Config, Aurora, Security Hub, Systems Manager
- Red Hat: Ansible Tower and Open Shift

C4S-Analytics and Visualization Application

- Customizable dashboards
- Filter by scans, environments & compliance categories
- Drill-down capabilities for root cause analysis
- Detailed information for failures
- Summarized errors with risk impact classification
- AWS resource inventory dashboards linked to C2VS scans

