

# Keeping It Under Wraps

## *How Corda's CenterView™ Enterprise Dashboard Secures Critical Data*

### Introduction

For executives and IT administrators, no consideration holds as much weight as that of securing the enterprise. The lack of solid security renders even the most flourishing businesses vulnerable to an attack on the company network, and without reliable security measures the best business tools become virtually useless. Security considerations have particular significance with regards to applications that can access important company data. Such data frequently pertains directly to the company's well-being and ability to function smoothly.

Enterprise dashboards provide a unique way for companies to access data from multiple sources across the enterprise and convert it into an easy-to-understand format. For C-level officers responsible for making the crucial decisions for an organization, the ability to view Key Performance Indicators (KPIs) driven by real-time, up-to-the-minute data is invaluable. This ability helps them to make informed and intelligent decisions for the company. However, an enterprise dashboard would lose its value completely if a company did not have total confidence in the security of the dashboard and the privileged information contained therein.

Corda Technologies' CenterView dashboard solution adheres to the highest security standards, recognizing the necessity of securing critical data. In developing CenterView, Corda sought to create a dashboard with enough security measures to put executives and IT administrators alike at ease. While each company has unique inner workings and operations, those that choose to implement an enterprise dashboard, such as the CenterView dashboard solution, share common enterprise security objectives. CenterView successfully meets and even exceeds each of these objectives, which comprise four primary topics:

- Security Environments and Authorization
- Role-based Access and Control
- Validated HTTP requests
- Browser cookies and Unauthorized Access

### Security Environments and Authorization

First and foremost, enterprises that implement a dashboard require the system to grant access only to authorized individuals. It is vital that unauthorized users cannot gain access to the data contained within the dashboard system.

Most companies have security environments existing prior to the implementation of an enterprise dashboard system. These security environments provide safety measures and security for the company's data sources. The three most common environments found in the enterprise are LDAP (Lightweight Directory Access Protocol), Windows Active Directory or a single sign-on environment. Companies utilizing Unix are more likely to employ LDAP, while companies running on Windows likely use Active Directory. Large companies with many employees often choose to implement a single sign-on system to simplify the process of allowing employee access to the company network.

Companies that already have a successful security environment in place don't necessarily want to build protective measures from scratch when securing authorization for a new application in the enterprise, such as a dashboard system. Rather, they require the dashboard to integrate seamlessly with their existing security procedures. This kind of integration provides reassurance that a functioning security system will extend to a newly implemented dashboard system, as well. With such integration, company executives and IT administrators can feel confident that only those who are authorized to access the dashboard system will be able to do so.





### **Role-based Access and Control**

It is not sufficient, however, for a dashboard system to ensure that only authorized individuals will have access to the system as a whole. Depending on how the dashboard system is developed, it can contain multiple dashboard sites that address various KPIs or other business indicators that may or may not be appropriate for all levels of employees to view or utilize. A member of the human resources department, for example, needs to know and understand different information from a sales manager. For that matter, neither of these employees would need the kind of overarching access that a chief executive officer or president might require.

In order to have a fully secure dashboard system, that system must provide the ability to restrict user access based on a role or group. The dashboard's administrator must have the ability to restrict users' access to specific dashboard sites within the system or even specific information within a dashboard site. Without this kind of role-based access and control the company would have no way to ensure that sensitive data was not falling into the wrong hands, even within the company. It would, for example, be problematic if sales people within a company could easily access private information about their peers, such as compensation.

### **Validated HTTP Requests**

After ensuring secure authorization and role-based access, companies must still guard against threats associated with a web-based application, such as an enterprise dashboard. These threats may come from external sources but, as dashboards are often used behind a company firewall, the threat could often come from an internal source. Employees who want access to information or data they aren't authorized to view may attempt to gain access by disrupting the system's HTTP requests in one of several ways.

Such an employee might attempt to browse the files in the dashboard directory to access unauthorized data. They might use another method, such as SQL injection, using an out-of-bounds or spoofed variable or cross-site scripting, to grant them unauthorized access. If any of these techniques were to succeed, queries into the dashboard system would likely allow the unauthorized individual to get information that under normal circumstances they would not be able to obtain.

Companies implementing a dashboard need to know that the system has solid, reliable guards against file browsing and that it provides query string validation. It is not enough to simply focus on securing authorization and authentication. Large companies, in particular, need to have the reassurance that a web-based application properly validates and "scrubs" query strings for SQL injections, cross-site scripting, out-of-bounds and spoofed variables.

Another less common but potentially very damaging security threat that could arise from HTTP requests is that of cross web servlet invocations, meaning that an individual could attempt to use the dashboard application to compromise another application running in the same class loader as the dashboard. This threat would likely originate from a member of the IT department attempting to gain access to information on another application. In essence, this employee would "hijack" the dashboard system to use it as a backdoor into that other application. Although this is not a widespread security threat, a company seeking the most secure dashboard system available would want a guarantee that the system was able to protect against such a risk.

### **Browser Cookies and Unauthorized Access**

A final enterprise security objective, particularly for large companies, is that of securing the dashboard against unauthorized access resulting from browser cookies. As a web-based application, the dashboard raises the concern as to whether the use of cookies in the browser will open up access to the dashboard, or to a specific site within the dashboard system, to someone who should not have that access. A secure dashboard system would provide a guard against this kind of unauthorized access.

### **CORDA Technologies' CenterView Dashboard: Fulfilling and Exceeding Enterprise Security Objectives**

CenterView, Corda Technologies's enterprise dashboard, monitors real time data and turns it into actionable information. It centers data from all corporate sources into a single graphical view of the most important indicators, giving executives the power to validate their instincts and make critical decisions with confidence. Its click-down capabilities allow executives to see the big picture, as well as the details.

Whether supply chain management, sales numbers, production figures, staffing status, financial

reports, or manufacturing through-put, CenterView puts critical information in front of the people who need the most up-to-the-minute company data.

In this age of massive amounts of information generated from multiple data sources, CenterView goes well beyond other competitive dashboards and provides a competitive advantage for executives in running their global operations.

Even the best dashboard, however, loses all its appeal and competitive edge if it does not fulfill the key enterprise security objectives that companies require. Corda knows and understands the vital importance of dashboard security and, as a consequence, has equipped the CenterView dashboard with all of the right security features.

### **Secure Authorization and Seamless Integration**

CenterView provides companies with the benefit of allowing dashboard administrators to easily integrate the dashboard system into their existing security environment, whether it is LDAP, Windows Active Directory or a single sign-on system. CenterView fits seamlessly into any of these systems and even takes security a step further, using the existing system without actually replicating the user directory.

CenterView can also save valuable time for administrators. Companies often have their user directories broken down into groups based on roles within the company. These roles dictate what access those users have. These groups might be “executive” or “management” groups, for example. CenterView allows IT administrators to make these groups available to the dashboard system, enabling it to reflect the groups that have already been put into place by the company’s security environment. For example, they can make certain dashboard sites available to certain groups predetermined by LDAP or Active Directory.

The CenterView set is extendable in nature, meaning that, in addition to including LDAP and Active Directory in CenterView’s configuration options, the dashboard system also provides the company with a robust user directory Application Program Interface (API). Dashboard administrators can write code against this API that will work in the dashboard system and allow the administrators to connect where, when and to what they want, rather than having to start from scratch when implementing the dashboard system. This robust user directory API can also be used to integrate within a single sign-on environment.

Even a company that has no security environment or procedures in place, or simply does not wish to integrate CenterView into that existing environment, can rest assured that the dashboard system will be secure. CenterView’s built-in log-in has the ability to provide a secure access and control mechanism, regardless of the company’s security environment. The CenterView log-in’s administrator module allows the administrator to configure the user access structure in a way specific to the company organization. In this manner, companies can secure and protect CenterView without plugging into another security environment or an existing single sign-on. The built-in log-in can provide group based or single user log-in access and even offers anonymous access.

### **Secure Data Access**

The CenterView dashboard system relies on one of two ways to obtain the data that drives the charts and graphs within a specific dashboard site. One of the ways the dashboard obtains data is by connecting to a company database. Most IT departments have controlled access to that data, based on groups or roles. This user access structure must be maintained and respected within a dashboard to ensure that only the appropriate individuals have access to certain types of data.

CenterView allows a company’s database administrator (DBA) to set up all of the normal, existing roles and groups within the system. CenterView can then query data back to display while respecting all the current policies set by the DBA. It doesn’t circumvent any of the access policies but plays right into them, thus eliminating the risk of giving individuals unauthorized access to particular kinds of data.

CenterView accomplishes this task by passing credentials set up by the DBA through the connection to the database, allowing the database to determine the role of the user and make appropriate adjustments. Consequently, the dashboard delivers role-based or group-based views to the user, giving them access only to certain dashboard sites within the system. These views might be even more specific, allowing users to only see certain data driving a chart or graph or no chart at all for specific KPIs.

Some environments, however, do not have an existing access structure based on roles or groups and sometimes the company does not want to put one into place. In this case, the dashboard system cannot rely on the databases it pulls information from to have controlled access and there-



fore prescribed role-based views. In such an instance, the developer responsible for creating the dashboard content can dynamically generate queries that are specific to whichever user is logged onto the system. These dynamic queries will only return data that the user is authorized to view. Such queries, found in the SQL, may raise questions as to how CenterView prevents them from being tampered with or violated.

### Secure HTTP Requests

In terms of securing HTTP requests within the CenterView system, CenterView does not allow directory indexing, meaning that users cannot see an index of files in the directory. The dashboard system filters all file requests so that the dashboard will only deliver files from accepted file extensions. This list of acceptable file extensions is configurable for the IT department.

CenterView further secures HTTP requests by only accepting variables or values from a prescribed list of those that are allowable. Any out-of-range or invalid variables will not be accepted. These variables are dynamic per dashboard.

Companies want to know that the dashboard system will not take variables at face value, and CenterView provides this assurance through the rigorous validation process it applies to every variable or value. The system also guards against variable spoofing by obfuscating text in the URL.

In the event that an individual attempted to filter on a servlet request, the dashboard system has built-in measures that prohibit anyone from executing a servlet that is not a CenterView servlet, specifically named, owned and allowed by the system.

### Secure Browser Cookies

Companies that worry about browser cookies storing information that can later be used to give unauthorized users access to data they shouldn't be able to view need not worry with CenterView. The system does not store any user information in browser cookies. While a session I.D. is stored, this cookie cannot be used to identify the user or to allow one user to masquerade as another.

### Conclusion

The CenterView dashboard solution from Corda Technologies meets and often exceeds the requirements of each of the four enterprise security objectives. From restricting access to the general dashboard system, to determining what role-based views those users have access to, to protecting against internal or external security threats, CenterView provides all the right security features to ensure that the critical data driving KPIs and helping key decision makers stay on top of the game does not fall into the wrong hands. With CenterView, executives, IT administrators and their companies enjoy a dashboard system that not only gives a competitive advantage in running the business, but also makes the question "Is this data secure?" a thing of the past.

### About Corda Technologies

Corda Technologies is the leading provider of enterprise applications for creating dashboards and interactive data visualization solutions that enhance smart decision-making. For a decade, Corda has led the evolution of data visualization from static charts and graphs to interactive, intuitive executive dashboards. Its award-winning solutions include developer tools, enterprise server products and professional services that improve business performance and enable customers worldwide to enhance bottom-line results. For more information regarding Corda, its customers, awards and partners, please visit <http://www.corda.com> or call (801) 805-9400.

