SOLUTION BRIEF

Cherwell Security

cherwell

Cherwell Security Overview

Ensuring security is an essential part of service management spanning security of the underlying software products, access to the application, data stored, hosting where applicable, and even security management itself. At Cherwell, one of our top priorities is the security of customer data stored in our software or hosting locations. We continually monitor and evaluate all datacenter locations, applications, and technology platforms against the ever-changing security threat landscape.

This document provides an overview of Cherwell Software security from the corporate perspective based on the principles of ISO 27001:2013, through capabilities provided in Cherwell products, to hosting, and the Cherwell Information Security Management System (ISMS) solution. This is only an overview and there are additional resources with more details including regional differences.

Cherwell Corporate

Cherwell holds an independent ISO 27001:2013 certification and continually monitors company processes and systems for continued compliance and enhancements. A third party conducts this audit annually. ISO 27001:2013 covers examination of an organization's information security risks, the design and implementation of security controls, and an overarching management process to ensure that the controls continue to meet information security needs on an ongoing basis. In the U.S., Cherwell Software has also been independently assessed and authorized as HIPAA compliant using National Institute of Standards and Technology (NIST) guidelines. Additionally, Cherwell is committed to processing protected data in compliance with all obligations of Processors under GDPR.

Cherwell Software Products

Cherwell Service Management and Cherwell Asset Management can each potentially contain sensitive information that should require secure access. Both products can be deployed on-premises, in a public cloud such as AWS or Azure, or hosted by Cherwell. Protecting and securing data is a shared responsibility between Cherwell, the customer, and potentially a public cloud or managed service provider. Here are some details on the roles:

- Cherwell is responsible for the application. When hosted by Cherwell, we are also responsible for securing the underlying infrastructure that supports the cloud and our access to the data.
- Customers are responsible for maintaining appropriate role-based access in the application for the organization's users. And when hosted, customers are responsible for securing connections to the cloud.

Cherwell Service Management has robust security controls at both the group level and at role levels governing rights to data and function access. As users authenticate to the system, they are assigned a role within a group. Programmatic access via RESTful APIs has similar controls.

Customers access the Cherwell Service Management application through a three-tiered encrypted connection to customer data over the Internet, either via the rich client, the end-user service portal, or the mobile platform. Client connectivity using any of these methods is encrypted and digitally signed to and from the application server using SSL over HTTP.

Users authentication can be provided by either SAML 2.0 or LDAP. To alleviate the need for VPN's in hosted environments, Cherwell also provides Trusted Agents. Details on SAML, LDAP, Trusted Agents, and Microsoft Active Directory integration are in the Cherwell online documentation.

Cherwell Service Management also supports encryption at the field level to protect sensitive data in records. This requires the use of encryption keys, and the ability to manage encryption keys depends on security rights within Cherwell Service Management. All attempts to decrypt and view encrypted field values are tracked (enforced) or logged (optional).

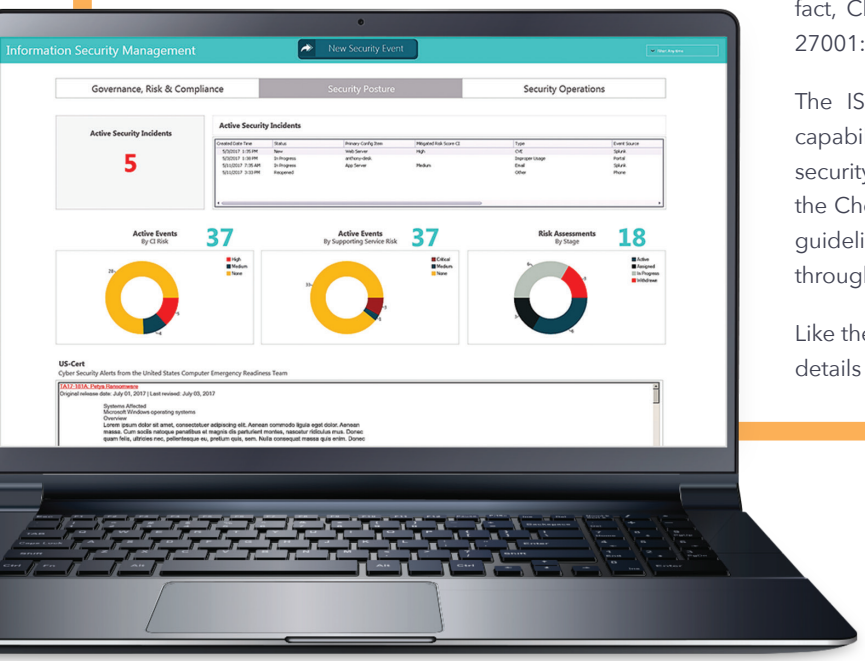
Hosting

Cherwell hosting is provided locally in multiple regions to ensure that U.S., Canada, EMEA, and APAC data is geographically separated and customers' data remains in its designated locations. The hosted datacenters meet several international and regional security certifications and industry standards including SAS 70 Type II/SSAE 16/ISO 27001 compliant datacenters.

Cherwell has more detailed and regional hosting documents covering physical security, security zone architecture, data separation, encryption in transit, data encryption at rest, assessments and audits, and business continuity.

Cherwell Information Security Management System (ISMS) Solution

The Cherwell ISMS solution runs on top of and is seamlessly integrated with the Cherwell's software platform and is available from the Cherwell mergeable application (mApp) exchange. It governs IT risk assessments and enables the effective preparation and response to IT security audits insuring that effective policies and procedures are defined and followed minimizing the risk of information security breaches and ensuring business continuity. The solution can help guide and track a variety of security-related compliance efforts such as FedRAMP:2014, ISO 27001:2013, and ISO 9001:2015. In fact, Cherwell uses the ISMS solution to facilitate our annual ISO 27001:2013 certification.



The ISMS solution also includes security incident management capabilities for managing security events and incidents. ISMS security incidents are specific to security breaches, and differ from the Cherwell Service Management incidents as they follow the NIST guidelines for security incident handling and allow strict privacy throughout the process to recovery.

Like the other topics covered in this short document, there are more details on the Cherwell ISMS solution available separately.