Workgroup Fortress

Shared Secure Content
for workgroups of online and offline users

Fortressware | PROTECTS YOUR DISTRIBUTED TEAMS' WORK ENVIRONMENTS

Today increasing amounts of work are performed without regard to geographical or organizational boundaries. The drive to tap into additional sources of expertise and reduce costs is relentless. High-tech enterprises based in the U.S.A. and India manage development teams around the world. Financial services firms in Europe run back office operations from locations in Asia. Regardless of industry or location, the common denominator is a need to share information.

But with sharing comes potential loss of sensitive information. When the risk is judged to be high, either information is not shared at all or its flow is constrained severely. The result: work may not be done where it is most efficiently executed, leading to less competitive solutions, higher costs, and lower profits.

Workgroup Fortress is designed specifically to provide security in such dynamically distributed collaborative environments. It does so through several patent-pending technologies that enables it to work with any application or type of file and still provide robust security. Costly training and re-tooling expenses are eliminated because there is no need to change existing tools and procedures. Rather than be distracted by concerns about the cost and effectiveness of protecting their information assets, firms using Workgroup Fortress plan rationally based on the best allocation of resources.

Differentiators

Secure Collaboration

Only solution designed specifically for a workgroup of online, offline, and mobile users to share any type of proprietary information securely.

Rapid Deployment

Agile solution for creating secure projects on the fly, for any size workgroup, without specialized knowledge or IT support.

Minimal Impact

Unobtrusive solution that does not impact productivity; existing tools and business processes are unaffected.

Flexible Use

Adaptive solution that simultaneously supports multiple sensitive or non-sensitive projects, keeping their content and audit trails separate.

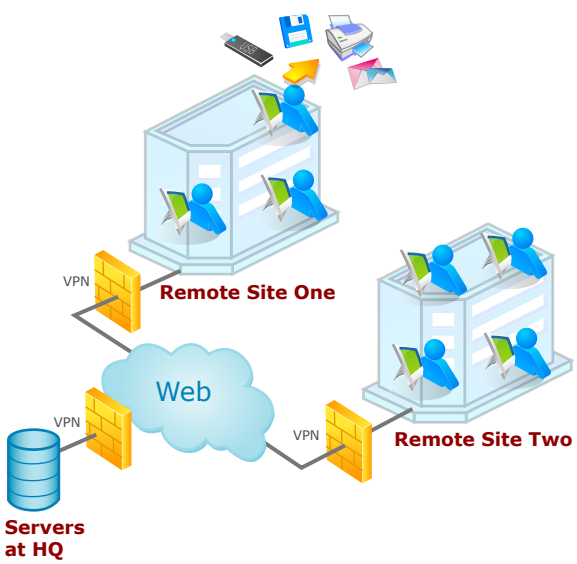
Integrates with Rational Software

Ready for IBM Rational software

Secured Partner Aladdin Aladdin.com

Confidential leaks abound

Businesses require their employees, partners, and service providers to maintain always-connected, always-on operations. A multitude of documents, e-mails and other electronic communications with private, confidential, or otherwise sensitive information circulate throughout organizations every day. As a result, the opportunities and means for information to leak have multiplied. A file saved to a flash drive or remote server, a document emailed or printed–all are easy and ubiquitous avenues for leaking information. And, whether inadvertent or malicious, a leak today can have substantial financial, legal, and privacy implications.



Recent headlines

- U.K. agency loses sensitive data on 25m people
  - Security Focus
- DuPont scientist admits downloading, stealing $400m worth of trade secrets
  - Computerworld
- Mortgage company's spreadsheets containing customer information leaked from home computer
  - USA Today

The challenge of today's security solutions

Until now, the focus has been on external security, i.e., keeping the bad guys out. But not all malicious threats originate from the outside. The insider threat has grown as organizations have broken down barriers to the flow of information, especially to distributed workgroups that include partners, service providers, and mobile employees. And not all internal threats are malicious. A threat can arise when personnel fail to follow procedures for keeping sensitive information secure. Clearly, external security solutions must be augmented by an additional protective layer that is focused on meeting the internal security challenge.

Existing measures are insufficient. They tend to focus on discovering information after it has leaked. Furthermore, they often result in lost productivity and higher IT costs. Limiting or cutting off access to the Internet, for example, can adversely impact the quality of work products. Requiring the IT department to classify documents in order to establish varying access rights, or write and maintain complex access rules, diverts resources from other priorities. With such limitations, it is no surprise that many enterprises continue to face loss of their information assets.

A different approach

In the world of distributed work, a balance must be struck between productivity and protection. Recognition of this requirement underlies the principles behind Workgroup Fortress:

- The point where information is created and used is the most logical point at which to protect it. Otherwise, information assets may begin to seep out, multiplying the effort required to locate and resolve problems at a later time or place.
- Security should be non-intrusive, requiring no changes to the work processes or tools used by an organization.

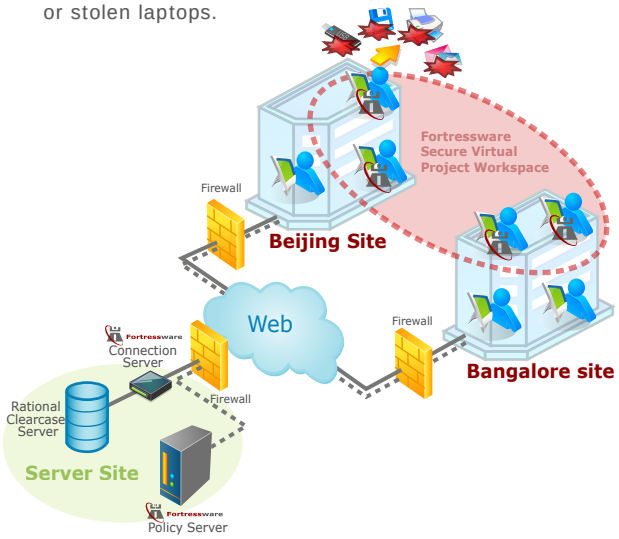
When information assets are non-intrusively protected from the beginning, managers have all the flexibility and options to manage their distribution in controlled ways.

The Workgroup Fortress solution

Workgroup Fortress offers the only internal security software solution that can be deployed quickly with minimal overhead, and is transparent to use. Now it is possible to implement the right solution for meeting the expanding internal security requirements of project teams, departments, and other enterprise workgroups.

Unlike traditional security solutions requiring the involvement of the IT organization, the technology behind Workgroup Fortress enables a project manager to create and distribute an access policy quickly via a secure "capsule" to define a virtual project workspace. Each workspace maintains a secure, yet flexible dynamic boundary that expands and contracts with changes to the project. Content cannot be moved or copied outside this area in any unauthorized manner.

With on-the-fly encryption and decryption at the time and place of file creation, Workgroup Fortress secures proprietary information independent of the file format or the application accessing the information inside the workspace. Encryption is also one of several measures that protects the mobile workforce against information breaches due to lost or stolen laptops.



Thus, a software development team located physically in Bangalore and Beijing and collaborating within a Workgroup Fortress secured virtual project workspace is able to communicate and share all project files and data effectively. However, team members are unable to engage in actions that would compromise sensitive information, such as printing or copying to remote or local devices. Further, because Workgroup Fortress is application agnostic, team members continue to use the same tools without modification; for example IBM's Rational Clearcase for version control.

The solution's audit log gives management real time visibility and control into a distributed team's activities. In addition, auditing features reinforce best practices and methodologies for complying with internal and external requirements, including Sarbanes-Oxley, HIPAA, and Gramm, Leach, Bliley.

Workgroup Fortress includes Fortress, the client software; Forward, the command center for rapid creation, administration, management and replication of access policy; and server software for network security and centralized control over the virtual workspace.

Fortress - security software for the client

Fortress, the client software, enforces your information security policies. Working both online and offline, Fortress provides access only to authorized users. Fortress works in the background so that a user does not even realize that he/she is within the Fortress secure environment. Fortress only makes itself visible when the user attempts to contravene a defined policy that could result in an internal leak.

Fortress features

- Generate a non-intrusive secure project environment from the Fortress capsule
- Encrypt and decrypt on the fly
- Enforce access policies
- Propagate the access policies in real-time for efficient and flexible policy administration and management
- Control offline environment with expiration dates on files from the Fortress capsule

Forward - the command center

Forward enables the rapid creation, administration, management and replication of access policies via the Fortress capsule.

Forward features

- Set policies for a project's team members
- Select team members
- Create Fortress capsule with metadata on the project
- Include the team's working files optionally within the Fortress capsule

Server

- Validate remote users
- Update policy dynamically
- Monitor and log all activities of team members
- Assure secure access to network resources

About Fortressware

Fortressware is a venture-backed company founded in 2004. The currently shipping product is Workgroup Fortress version 3.2.

The idea for Fortressware came from the founders' experience in starting off-shore development centers when they worked for a public global enterprise. They researched the risks of a geographically distributed development environment as well as looked at all the security solutions that were available in the market.

They did not find any that satisfactorily met their needs for protection against internal leaks while maintaining the project teams' productivity. They then decided to build a company to provide such solutions for globally distributed enterprises.

For more information, visit www.fortressw.com.

Contact Information

Address:
2672 Bayshore Parkway, Suite 608
Mountain View, CA 94043

Phone:
+1-650-472-3886

E-mail:
Info@fortressw.com

Fortressware