

Rothschild Bank AG Zurich

Keeping Banking Infrastructure Secure

Industry: Private Banking Investments

Tripwire Solution: Tripwire Enterprise



Members of the British and French Rothschild families set up Rothschild Bank AG in Zurich in 1968. Since then, it has grown into an international private banking group with offices in major cities around the world, serving a varied international clientele. The same proud banking heritage, innovative financial skills and highly personalized services that distinguish Rothschild's activities throughout the world form the basis of the Zurich Bank's ability to help clients achieve their goals.

"Tripwire Enterprise's ability to oversee and monitor the infrastructure is what helps us manage risk and ensure our bank's security."

—Jan Brunschwig
Vice President, IT Security
Rothschild Bank AG Zurich

Challenges

A global financial institution, Rothschild Bank AG has numerous branch offices with IT managed centrally from Zurich. To manage risk and to detect intrusion, it is necessary for the bank's IT organization to have the ability to monitor change across the entire infrastructure and to be able to react quickly to any unauthorized change that could compromise security. Because the datacenter operates and integrates with multiple operating systems (including Windows, Linux and Solaris), it required a configuration audit and control tool that could easily work with all environments and configurations.

Tripwire Enterprise: The Bank's IT Security Guard

Even though Rothschild Bank AG Zurich has a large presence in private investment circles, it operates very much like a small company, with personal, hands-on management. Its IT department is no exception. However, in the ever-complicated and 24-hour world of network-based communications and transactions, they didn't have the manpower to monitor logs 24/7 for change activity. They needed a solution to collect data across all tools and logs and alert them quickly to questionable change events. They also needed a tool to correlate and feed information back to them if a change seemed to be an intrusion—or not. This functionality is particularly important for servers accessible by the Internet. Jan Brunschwig, IT Security officer for Rothschild Bank AG Zurich, and his team chose Tripwire Enterprise for its ability to monitor changes across the entire, heterogeneous infrastructure and alert them to any change that could be a possible intrusion.

Rothschild Bank AG Zurich has long been a Tripwire user, integrating it for over five years now into its IT operations. While Tripwire software had served as an intrusion detector, or "security guard", for the bank, the IT organization's needs have grown, as have the capabilities of Tripwire solutions. The bank recently took advantage of Tripwire Professional Services to implement Tripwire Enterprise's new configuration audit and control for directory servers, with rules specifically for Active Directory.

CASE study

As an example of the need for strict Active Directory monitoring, there was a recent situation where the IT staff added a new application. Jan Brunschwig wanted to be able to monitor all activity across the domains while this application was uploaded in order to ensure no unauthorized person gained access to the application. Without Tripwire, this vital information would have been invisible to him.

"With Tripwire I can monitor applications and be sure that no one accesses systems and administrative files without my awareness," says Brunschwig. "This ability to oversee and monitor the infrastructure is what helps us manage risk and ensure our bank's security."

In order to meet SOX-like regulations that are quickly becoming mandatory throughout Europe, Rothschild Bank AG Zurich plans to use Tripwire's ability to make all change visible as a vehicle for reaching regulatory compliance. Visibility is also the first step in the IT organization's continuous improvement process; it will be using Tripwire to take the next step—accountability—in establishing stringent policies for its change processes.

Tripwire Enterprise configuration audit and control solutions detect, analyze and report changes across millions of elements (e.g. files, directories, registry settings, directory server objects, and configuration files) in the entire IT infrastructure. Tripwire Enterprise detects all changes, analyzes them to reconcile the authorized from unauthorized, and reports on change activity. It operates independently of any administration tools used to manage and make changes, providing an unbiased accounting to IT management.

About Tripwire

Tripwire, Inc. is the recognized leader of configuration audit and control solutions, serving nearly 6,000 customers. As the first in the industry to combine configuration assessment with configuration change auditing, Tripwire helps IT organizations automate compliance across the data center, reducing risk and increasing operational efficiency. Tripwire ensures the organization achieves continuous operational, regulatory and security compliance, helping IT achieve and maintain a known, trusted and compliant system state. Tripwire is headquartered in Portland, Oregon, with offices worldwide.

"Tripwire has long been ahead of the pack, supporting multiple platforms. It's the only solution we considered."

— Jan Brunschwig



www.tripwire.com

US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182
326 SW Broadway, 3rd Floor Portland, OR 97205 USA

©2007 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other trademarks and company names are property of their respective owners. All rights reserved.

CSRTH3