SunTrust Banks

Improving productivity, reducing vulnerability windows

Overview

The need

Gain visibility into a distributed IT infrastructure; reduce software patch and update cycle times; and maintain all systems at current patch levels and configuration standards.

The solution

SunTrust uses the IBM® BigFix® solution to maintain vigilance over the software running on its computers and previously undocumented IT assets on the network.

The benefit

Maintains a 98.5 percent patch and update compliance rate; decreases update and patch cycle times from 2 - 3 weeks to 2 - 3 days; reduces productivity losses and human errors through automation.

Atlanta-based SunTrust enjoys leading market positions in some of the highest growth markets in the United States and also serves clients in selected markets nationally. The company operates almost 1,800 retail branches and 2,673 ATMs in Alabama, Arkansas, Florida, Georgia, Maryland, Mississippi, North Carolina, South Carolina, Tennessee, Virginia, West Virginia, and the District of Columbia. In addition, SunTrust provides customers with a full range of technology-based banking channels, including Internet, PC and Automated Telephone Banking.

Gaining control over a highly distributed environment

SunTrust has a highly distributed environment with nearly 1,800 branch locations and no local IT resources at most of those locations. This resulted in long patch and software update cycles, a large number of manual patches and poor visibility into what assets were on the network. These issues also made it difficult to provide required compliance data to the security and risk management teams.

The solution has become part of the landscape here," says Ed Jones, senior information planning engineer, SunTrust. "It was a big change for the better when we first installed it, but has become a standard means for us to keep software at the latest version levels."

Solution components

Software

- IBM® BigFix®

Automating endpoint management

Ed Jones, senior information planning engineer at SunTrust, works at the nexus of security and systems management at SunTrust. His responsibilities include execution and oversight of the bank's patch management, software distribution, antivirus, software packaging and development, IT inventory, and workstation imaging services. Jones has been using BigFix technology since the company selected the product in 2004 to support its software patch and asset inventory programs. Since then, SunTrust has installed the solution on over 50,000 PCs, servers and mobile computers.

Software patch and update management along with asset inventory remain the main services provided by the IBM BigFix solution at SunTrust. "The solution has become part of the landscape here," says Jones. "It was a big change for the better when we first installed it, but has become a standard means for us to keep software at the latest version levels."

The BigFix solution also plays a significant role in inventorying SunTrust's IT assets and providing compliance reporting. "It gives us very detailed reports very quickly and easily," says Jones. "We can see how many computers we have, and what's running on them. We can also see if someone has installed non-standard software or a risky peripheral like a

> *"It's easy to generate reports and we know that the information is going to be complete and accurate."*
>
> —Ed Jones, Senior Information Planning Engineer, SunTrust Banks

wireless router. And we can do this on every computer that runs BigFix no matter where it resides on our network—headquarters or in any of the 1,800 bank branches."

Along with the many responsibilities Jones has, is reporting to multiple constituencies at the bank. "IT, Risk Management and Compliance groups are the main customers," says Jones. "It's easy to generate reports and we know that the information is going to be complete and accurate. BigFix is also very handy for fast-breaking custom inquiries. It's very easy to put these together and get results instantly."

Reducing the update cycle by a factor of seven

SunTrust implemented the BigFix solution across over 50,000 endpoints spread across nearly 1,800 locations. The entire roll-out process was accomplished in three months with just two people. Ongoing management of all these endpoints requires only 1.5 FTEs (full-time employees). The solution has brought both speed and visibility to the software update and patch process. "A patch or an update used to take two to three weeks to execute," says Jones. "We now average two to three days to update over 50,000 computers on our network."

Reducing the update cycle by a factor of seven is not only good in itself, but it also reduces the window of vulnerability to malware, security incidents and breakdowns that the updates and patches are designed to prevent. "Over the years, we've brought the segment of our infrastructure equipped with the endpoint management solution up to 98.5 percent compliance with the latest manufacturer recommended configurations," says Jones. "This includes both system software—mostly Microsoft Windows—and applications that run on our computers."

Jones identifies three major advantages that contribute to these time and labor savings. "The Microsoft and application software patches we get from BigFix are ready to deploy the same day we receive them," comments Jones. "We used to have to package and test updates before sending them out, which added several days to the schedule. We can install updates with virtually no need for end-user intervention. There were always people who would take a few days to execute an update on their machines, and with a user population as large as ours, an update would generate a surge of calls to the helpdesk. Finally, BigFix gives us outstanding visibility into configuration status of every machine it runs on. We know if something has been installed or not."

"We have made great strides over the last few years in moving from reacting to events to proactively staying ahead of the game. We couldn't do this without this visibility."

—Ed Jones

Achieving 98 percent patch efficiency

Why automated endpoint management? "I can 'set it and forget it'," says Jones. "We achieve over 98 percent patch efficiency, we are able to target by groups, and the system is fail-safe in that we can override human errors preventing outages. This was not true of our previous patch management vendor, PatchLink."

SunTrust also evaluated Microsoft tools at the time, but determined that the infrastructure was just too heavy and inflexible. BigFix technology was selected for its lightweight infrastructure, extensive platform coverage and patch efficiency exhibited during the Proof of Concept (POC) test.

Looking Ahead

Jones says visibility is the biggest change. “Before, we really couldn’t see what was going on in regards to Microsoft’s Security standards,” he explains. “Now we can. This has made a huge difference in how we approach our work. We have made great strides over the last few years in moving from reacting to events to proactively staying ahead of the game. We couldn’t do this without this visibility. It has really been the key to improvements we’ve made in maintaining standard system configurations, minimizing vulnerabilities and maintaining supervision over a large infrastructure spread out over 1,800 locations from Florida to Maryland.”

With such great long-term results in asset discovery, patch management, software distribution and configuration management, SunTrust looks forward to adding more capabilities of the BigFix solution. SunTrust will next look to the BigFix solution to help it achieve significant cash savings through PC power management and optimizing software licensing. These extensions are made that much easier to implement and their ROI that much greater with the technology’s single platform approach that does not require any new infrastructure to implement additional capabilities. Finally, SunTrust also plans to implement a BigFix relay in its demilitarized zone (DMZ) to extend coverage to roaming laptops while they are off the network.

Take the next step

To learn more about the IBM BigFix solution, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security/bigfix

For more information on SunTrust, visit: www.suntrust.com

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2015

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Recycle