



BUSINESS LINES:

## Operations

### Instant Access

Deploying a single sign-on solution streamlines Glenmede's operations and eliminates a mushrooming security risk.

>>> By Anne Rawland Gabriel

**T**HE RELENTLESS addition of passwords to business applications is causing a major productivity fallout at many organizations and may be putting securities firms at significant — and underestimated — risk.

“When we ask a room full of IT professionals how long it takes them to remove all authorized access for a single terminated employee, we see the most consensus around the ‘weeks, months or more’ time frame,” asserts Mark Diodati, identity and privacy strategies analyst for research and advisory firm Burton Group. “Even in small organizations it’s problematic.”

Indeed, managing multiple tiers of data access across employees, contractors and partners — both on-site and at remote locations — has spawned a new IT security category known as “identity and access management.” Commonly referred to as securing the front door to enterprise data, this mushrooming category will grow to \$5.1 billion by 2010 according to IDC’s most recent research.

The Glenmede Trust Company, a wealth manager for ultrahigh-net-worth individuals, began logging unacceptable levels of productivity and security overhead resulting from password management early in 2005. At the time, password-protected applications regularly accessed by the firm’s 250 employees approached 30. “As we scaled up our

client offerings, we needed more tools and more protection layers,” says Nicholas Voutsakis, the firm’s CTO. “But some tools were negatively impacted because people couldn’t remember yet another password, and we experienced a steady flow of help desk calls for password resets.”

Due to his firm’s emphasis on client service, Voutsakis says, finding a user-friendly solution was critical. “Fortunately the technology was mature enough by late 2005,” he says. “Then it was simply a matter of prioritizing it into our project portfolio.”

authentication. “Irrespective of specific regulatory requirements, if your peers are using strong authentication strategies, ignoring the trend means you’re dead in the water if you’re ever in court,” points out Burton Group’s Diodati.

Glenmede used its authentication project as an opportunity to review security strategies enterprisewide, as well as for our clients who access their data via the Web, explains Glenmede’s Voutsakis. “Although regulatory requirements framed our solution search, they weren’t the primary driver. We were also analyzing security enhancements to our



>>> *“If your peers are using strong authentication strategies, ignoring the trend means you’re dead in the water if you’re ever in court.”*

—MARK DIODATI, Burton Group

Coincidentally, new banking regulations stipulated implementing two-factor authentication by the end of 2006. There are three universally recognized authentication factor categories: something you know — a password, PIN or similar code; something you have — a security token/badge, credit card or mobile phone; and something you are — a fingerprint, retinal scan or other biometric. Using two or more factors is considered strong

remote log-in capabilities via an SSL [secure socket layer] VPN by Cisco. So hardening our front door was part of a larger implementation. This, in turn, was part of an even broader strategy to integrate and secure a range of enterprise technologies while making them all easier to use.”

#### Single Sign-On to the Rescue

Headquartered in Philadelphia and spread across four U.S. states, Glenmede has a typ-



ical LAN/WAN of primarily Dell and Cisco hardware running Microsoft Windows Server 2003 with applications delivered by Citrix. To satisfy all of its security and integration objectives, Glenmede narrowed the authentication field to three vendors of a new breed of single sign-on (SSO) solutions: Citrix, EMC's RSA and Imprivata.

As the name implies, SSO technology allows users to log on once for multiple application access, while allowing IT to completely block a terminated user with a single click. According to Voutsakis, Imprivata's SSO solution, an all-in-one appliance called OneSign, integrated well with the wealth manager's existing applications, including its building access cards. Further, OneSign was plug-and-play: Set-up and configuration were measured in hours, rather than days, with negligible administrative overhead, he adds.

Glenmede began the OneSign implementation in mid-2006, first testing the appliance in conjunction with building access card proximity readers. Soon afterwards, however, Imprivata introduced fingerprint authentication. "But some people's fingerprint scans failed," Voutsakis says. "After Imprivata introduced improvements, scanning failures were reduced to only five people. We simply gave those individuals proximity readers, which put everyone on the SSO system."

In addition to achieving productivity goals, the SSO implementation received a thumbs-up during Glenmede's most recent third-party security assessment and also is enabling new initiatives. "For example, we're developing a pandemic plan to allow all employees to work from home during a crisis, which we couldn't do effectively before having our remote security in place," Voutsakis states.

On the back end, Glenmede will begin using the solution's detailed activity logs to monitor which applications are used most

often and which are underutilized or are even expendable, Voutsakis says. This information will impact future buying decisions and improve application ROI, he points out.

Under the hood, Imprivata's appliance transparently performs complex security chores without generating mountains of data to back up. "One unit is designed to handle 40,000 to 50,000 users and generate a database of less than 80 gigabytes," claims Imprivata CTO David Ting. "Also, the database is encrypted and is literally impossible to steal."



*"[Single sign-on] was part of a broader strategy to integrate and secure a range of enterprise technologies while making them all easier to use."*  
—NICK VOUTSAKIS, Glenmede Trust Company

Some SSO solutions also improve security by enabling the integration of IT and building access systems. Known as physical/logical convergence, the rapidly emerging trend provides contextual enterprise security for the first time. "Let's say an employee is badged into your Boston location," hypothesizes Burton Group's Diodati. "Then the system detects an access attempt from a Rhode Island coffee shop. Automatically, the remote attempt is blocked and an alarm sounds." Not surprisingly, contextual security has the added benefit of encouraging users to report missing badges immediately, Diodati observes.

**Tips, Tricks and Sage Advice**

For those taking the plunge into SSO, Diodati offers several tips. "First, pur-

chase a solution that maximizes compatibility with existing IT infrastructure and building access systems," he says. "Then it's critical to develop deployment best practices, both technical and operational, before you implement."

"For example, most systems can randomize passwords," Diodati continues. "But randomizing may not be the default setting. Also, it's a given that users will forget their access token or won't get a clean biometric scan. So what happens when users can't get in? How secure is your work-around? And how often does a situation occur before

additional remediation is required?"

Diodati also stresses rigorous testing prior to deployment. "Test your SSO with each application, not just some," he says. "Then conduct a significant pilot project before you roll out to everyone."

According to Imprivata's Ting, his company's goal is to provide an enterprise-class solution in a consumer-oriented box. "A lot of security systems are very complex and come with ongoing service costs," he says. "Ours is purpose-built, like a washing machine. You don't have to know how it works and you can wash all you want for the same cost."

Next up for Imprivata is enhancing OneSign's disaster recovery (DR) features. "Currently the appliances are deployed in pairs and they fail over automatically," says Ting. "We'll introduce distributed capability in the fall, allowing for connection to a distant hot site. Regardless, if network access to the user is cut, the client software continues to log activity and then uploads information when the network is restored." <<<

wallstreetandtech.com

**BEST PRACTICES** around password and identity management in financial services are emerging:

wallstreetandtech.com/showArticle.jhtml?articleID=193400879