

At the Toro Company, Identity Brings Security and Compliance with Respect for Employees

Security tends to focus on lockdowns and restricting access. But that approach doesn't provide awareness of the actual activity within enterprise systems and can create perceptions of mistrust between the company and its employees. The Toro Company is using identity based techniques to meet regulatory requirements for control while easing the feeling of user mistrust that many security approaches create.

The Toro Company began life 90 years ago as a tractor engine manufacturer. In its long history it developed the first automated golf course maintenance equipment, the first power mower for home use, and the first snow thrower. Today it is an NYSE listed Fortune 500 company that manufactures and markets professional and home landscape equipment under the Toro, Lawn Boy, eXmark, Irritrol, Lawn Genie and Pope brands with \$1.5 billion annual sales.

As a heartland company that has built its reputation on customer care and service, Toro's culture is one of employee empowerment. Today's computer security and



© 2003 The Toro Company. All Rights Reserved.

regulatory compliance requirements can challenge that culture. Mike Drazan, Toro's VP of Corporate Information Services, said "You have to understand our culture. We trust our employees, they are the most valued component of our business. We have a high degree of loyalty and we have a lot of employees with a lot of years of service. I have an individual in my systems group who has 39 years of service. That's the kind of company we are. We have people who've been here a long time and the value in that is they know our business, they know our customers and they love Toro. When you start driving in security and saying we're going to be looking over your shoulder on what you are getting access to and how you're doing it, that doesn't send a valuing message to an employee. In today's world we need better oversight and better control, but we want to do it and stay within our culture."

Serendipity

Serendipity intervened roughly two years ago in the form of Prodigen's CEO Ken Searl who Drazan knew from a previous business relationship. "When he started thinking about security he called me. At the time for me it was a hot button because I'd been in the market looking and wasn't seeing what I wanted. We shared a very similar belief in what was missing in the market." That belief was that rather than focus on restricting user capabilities, IT security should be based on knowing what the company's business processes required users to do and then monitoring for use that is outside the norm.

To accomplish this, Searl's company had developed what he calls the Contouring Engine and after their discussions Drazan agreed to beta test it at Toro. "I wanted to try it in my environment," said Drazan. "So we sat down with some of his team and some of mine and wrestled through 'what did you actually build and how does it work?' He had some good technical peo-



© 2003 The Toro Company. All Rights Reserved

ple that built a good product and it fit the way we wanted to manage security."

The appeal of the Contouring Engine approach to Drazan was twofold. It would let him detect improper access to company data, and it also paved the way for the coming compliance auditing requirements. "We started talking to consulting firms about Sarbanes-Oxley and their anticipation of what was going to come down," said Drazan of his outlook two years ago. "It was clear it all came down to controls. The regulations and the auditing that was going to take place was going to be looking at controls. When I look at most businesses, and [back then] our own, I couldn't look the board in the face and say we know that only the people that should, have access to our information. What I [do] know is [that] I'm dishing out passwords. I don't really know if it is the right people with the right profile doing the right things all the time. I know how many passwords are out there and I know what they have access to, but I can't tell how they are used."

Knowing Your Business

The concept of Prodigen's Contouring Engine isn't too hard to understand. It

works by gathering transaction data from application logging streams. That data is then sorted by identity (user name), filtered and processed. A profile of anticipated activity is built, and the Contouring Engine then creates security alerts if an identity engages in unexpected behavior in the system.

That simple premise, however, isn't necessarily easy to implement in a large company. Along with assuring that the monitoring system has proper security and tamper resistance, there is the issue of developing the initial profiles of how users actually use a company's systems. The Contouring Engine has tools that aid the initial development of these use profiles. "We gather the activity of a user for some period of time in a specific application at the transaction, or in Toro's case at the record, level in one of the apps," said Searl. "Once you establish that, then we monitor their daily activity against that profile. So if anybody would steal their identity, or steal their password and get their identity, we would know almost instantaneously."

Toro began its implementation with the company's SAP applications, which Drazan judged would give the best

returns while learning about the approach. "When we first worked with Prodigen we spent twenty to thirty days to define how we wanted to connect to SAP and then educating our security team on setting up the profiles," said Drazan. "That went fairly smoothly. After that we spent [about] three months wrestling through that first comparison of the profile versus the alerts that were coming out [to determine] whether it was concurrent transactions, unknown users, repeated security denials or someone working outside their work hours. It took a long time for us to shake out some of those things, longer than we had anticipated frankly."

In the process, however, Drazan found that they learned a lot about how the company was really using their systems. "As an example of that," said Drazan, "we had a plant where at the receiving dock somebody would sign on in the morning and then everybody doing inventory receipts would use that screen. Well, we didn't know that. We thought everybody that was doing work on the system was signing in themselves and scanning the information. So we got thousands of alerts, because [the terminal] never signed off. It took us some time to sort some of that stuff out, and then both change employee behavior and make sure the system was filtering alerts that were worth something to us. Three months might be a little long for some companies, [but] I'd say it's at least thirty to forty-five days."

The Rollout Was an Education

"You are learning in the process what you really want to track based on the real behaviors of people," said Drazan. "You find out what's really going on and that it was done for a very clear reason – because that was the most effective way for our plants to do business. So it wasn't

as simple as just going out and saying you can't do this. We could have done that but I don't think that was the way to value our employees. [The behavior] certainly evolved for a reason, so we needed to spend the time [to understand it.]"

They found that proceeding by groups was the best rollout strategy. "We took an approach of taking it department by department and started putting people on," said Drazan, "because that allowed us to build the profiles in a manageable way and then educate the functional area that we were working with to learn what we were doing."

Asked how far along the rollout is today, Drazan responded, "We [were most] interested in our core business data: our financial data, our order data, our inventory data, our engineering and product development data, which are in our core applications. Those core applications are done and we are [now] looking at some of the other peripheral systems like our warranty system. Right now [approximately 9 months into the process] we're up over 3500 employees and we're probably at about 60% of the transaction volume. We're targeting [the remainder] over the rest of this fiscal year which ends in November."

Asked how the system would respond to growth and new applications, Drazan said, "We try to do things planfully. If we put a new application on [the Contouring Engine] there is the time we have to spend to evaluate the application, figure out where we get the information and connect to it, and test that. We then figure out what departments we're rolling into and if there is any implication in the profiles. We've gotten to the point where that's relatively simple. Most applications we can get connected and functioning within thirty to forty five days depending on the application and how big an audience you are affecting. Then you walk into that group and work through it."

Evaluating the Results

Installing the contouring engine was part of three pronged approach at Toro. First, Drazan worked to create access control and improve administration and management of who had access to what in Toro's systems. He also began an identity management project to delegate and distribute password administration. "The goal behind that," said Drazan, "was to move the responsibility and the control of who is assigning passwords and giving access to components of our information systems closer to the people who knew. The manager that runs an organization is the best person to know who reporting to him should have access to applications. Giving [the managers] the ability to assign passwords and give them out shifts the responsibility, which all of a sudden drives more of an awareness in our business of security. And it gives [managers] the ability to give the right people access and takes that off the shoulders of an IS person who really doesn't do anything more than administer a password."

As to the Contouring Engine, Drazan said, "It works. The pressure of today's world both from an external access and a government regulation standpoint, is to have more control and more oversight, which was in direct conflict to our culture of empowering employees, trusting employees, and also an incremental cost in buying and accessing new tools. So what I was looking for was a way to improve security in our business without disrupting our culture while protecting our employees. What the contouring engine has done is given us a way to put profiles in place, drive security into the organization at a higher level of awareness and then allow us through the monitoring to actually address exceptions in a valuing way."

"If we find [activity] that's different [from the profile] we go to the supervisor asking questions about what we see," said Drazan. "Rather than running out saying



‘you did something wrong’ or ‘this person’s doing something they shouldn’t be doing’ it allows us to go and ask the person ‘did you lose your password,’ or ‘did somebody else maybe get your password and can we change it?’ Or [we can discover] that we in fact do not understand that person’s job. That’s a lot different than accusing somebody of doing something they shouldn’t be doing. That’s an important thing for us. It gives us proactively the ability to understand who’s doing what and how they’re doing it without making people believe that we’re looking over their shoulder all the time because we’re not.”

The Bottom Line

The combination of identity management and the Contouring Engine have let Toro approach security from the desired direction. “For Toro our culture tends to be more empowering,” said Drazan. “Our belief is that that we value employee loyalty, we value the fact that we have people who’ve been here a long time, who know our customers, who know our business, so we give them the ability to manage their piece of our business, and get closer

to our customers. They don’t need anybody looking over their shoulders, and most people view security as someone looking over their shoulder – it’s that Big Brother syndrome. We don’t want to drive that in our business, that’s not our culture and it’s not what we want to push into the business. Yet government regulations and some of the ethics issues, and in fact the behavior in the market around systems, says we have to be tighter with security.”

Total ROI or cost in such complex deployments can be difficult to assess, but Drazan is certain this approach has kept his total costs down. “My security costs have gone up about 5%,” said Drazan, “and most of my peers are telling me theirs are up over 10%. At a time when government regulations are much tighter than they have ever been and control requirements are up, virus protection and perimeter control demands are up, there are some very real security risks that increased that we had to address which drove some of that[total] increase. [And] most companies aren’t [yet] doing the monitoring that I’m doing.” ■