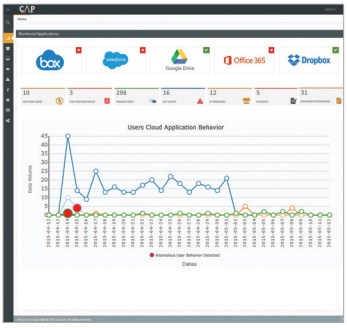
SC MAGAZINE
EMERGING PRODUCTS



Gurucul

Risk Analytics

DETAILS

Product Risk Analytics

Company Gurucul

Price $50,000 per year.

What it does Behavior-based machine learning and predictive analytics.

What we liked This is, hands-down, the most sophisticated example of behavioral analytics we have seen to date. While they are not the only player in this space, their product is well thought-out and it really works well.

OUR BOTTOM LINE

The administrator can create new data models and build or modify policies. The policy engine is about as straightforward as it gets. If you've ever created and managed policies in a security tool you'll feel right at home with this one. One feature we particularly liked was the built-in ticketing system. With this feature users can setup incidents and handle them as one would any trouble ticket on a help desk. With all of this power, we were pleased to find that, along with everything else, this makes a powerful forensic tool.

There are several products that claim to do analytics and a few that claim to do predictive analytics, but this is the first we've seen that really gets the job done in a virtual environment. The whole idea of predictive analytics is to produce actionable intelligence and then act on it. "Actionable intelligence" has become a buzz phrase since the hypesters discovered that talking about intelligence really didn't have much punch. But just because a product hypes actionable intelligence does not mean that it has the capability.

Actionable intelligence is useless unless it can accurately and reliably predict events and select the correct response. In order to get real actionable intelligence, the product needs to get serious about the math used to predict and analyze events. It needs to get serious about machine learning, a relatively new concept in practice if not in theory, and it needs to get serious about such functionality as correlation, fuzzy logic and working without signatures. It needs to be able to handle large amounts of data in a Big Data paradigm. Big Data does not, however, just mean lots of data. Big Data is defined classically as high volume, high velocity and high variability – the "three Vs." All of these capabilities are present in the Risk Analytics platform from Gurucul.

This tool is built around a suite of sophisticated machine-learning algorithms. It is intended – from the ground up – to identify zero-day activities and it is designed to provide both contextual and situational awareness. It is compatible with several third-party intelligence feeds. Everything the system does is based on understanding the identities of those entities accessing your cloud-based data. A big piece of the system's success is what Gurucul calls "peer group analytics." What that means, in simple terms, is that your system should not be dramatically different in its behavior than other systems like it.

The analysis cycle starts by normalizing input data. Then that data is correlated and its behavior analyzed. This allows predictive modeling. Data sources can be access to the platform, endpoints, network, storage or applications, among others. The actionable intelligence can take the form of fraud detection, user behavior analysis, insider threat identification and deterrence and security intelligence addressing access to your cloud-based resources.

Operationally it was interesting to see how a complex capability under the hood translated to a relatively simple set of dashboards and administrator consoles. The main cloud dashboard – completely customizable, by the way – has everything one needs to see the state of security on a cloud environment at a glance.

GURUCUL
PREDICTIVE SECURITY ANALYTICS

5959 West Century Blvd, Suite 1111
Los Angeles, CA 90045
Phone: 213.373.4878
Email: info@gurucul.com
Web: www.gurucul.com