FireLayers answers a burning question: how to address the multi-layered CAC market?

Analyst: Adrian Sanabria

18 Jul, 2014

FireLayers joined the popular cloud app control (CAC) market earlier this year with a focus on compliance and governance, in addition to security. First and foremost, the CAC market is all about adding visibility to an area where most enterprises have thus far been blind: activity within SaaS applications. Rather than stopping there, this market realizes that, once aware of what users are doing, there will be issues that can't be unseen – enterprises will need some way of dealing with the results. That's where the 'control' piece comes in.

The 451 Take

In an already crowded market, it is important to differentiate and have strengths that are clear to potential customers and acquirers (we're assuming an acquisition exit would be considered by most in the CAC market at this point). FireLayers has chosen to focus on application control, and how it impacts compliance and governance. The company feels that this is the core of what this market is all about, and we agree, having chosen to include 'control' as the focal word in the name we've given this market. While we still think that nearly all CAC competitors will eventually be competing with comparable feature sets, we think the crucial defining stage of the market is occurring now, and vendors that choose to focus on the wrong elements will find themselves trailing the leaders a year or two down the road.

Context

FireLayers was founded in early 2013 by Yair Grindlinger and Doron Elgressy, an experienced leadership team sharing a common past. Both worked together at Security-7, which was founded by Elgressy and acquired by CA in 1999. Grindlinger and Elgressy cofounded IT support services business SupportSpace in 2006. Before SupportSpace, Grindlinger served as the CEO of PortAuthority Technologies. Both also have experience in the investment space.

Many Israeli security startups have found it effective to establish R&D offices in Israel and a sales and marketing headquarters in the United States. FireLayers emulates this trend with a headquarters in Redwood City, California, and offices in Herzliya, Israel. A notable exception from the model is that technology and product leadership is located at its headquarters, with R&D occurring in both locations. The company currently employs 15 full-time employees with a few full-time consultants, and is actively hiring. The company is primarily funded by YL Ventures (headed by its initialed namesake, Yoav Leitersdorf). YL Ventures also backs several other security startups covered by 451 Research, including Hexadite, Seculert and 6Scan.

Products

FireLayers sorts its product's capabilities into proactive and reactive security controls. These controls are implemented through policies defined within the application's intuitive UI, which reminds us of Checkpoint's SmartDashboard. Identifying automated or human intrusions is a reactive control example. Fine-grained access control over what users can do in SaaS applications is proactive, as is the ability to mitigate technical vulnerabilities (which reminds us of the 'virtual patching' concept). FireLayers was also the first CAC vendor to introduce the concept of adding controls that the SaaS application didn't already have or support. An important feature is the ability to add a two-factor authentication (2FA) requirement for particular functions. Allow us to demonstrate the possibilities in a highly fictional example:

Potential customer: 'Here are the security and regulatory requirements we need your app to meet before we can use it.'

SaaS vendor: 'Well, our app doesn't support all your requirements at the moment, but in collaboration with FireLayers, we can support all your requirements in a few weeks *and* give you detailed user monitoring and analysis.'

Potential customer: *shocked silence*.

Perhaps that's not exactly how the conversation would unfold, but the importance of an ability to add features to existing SaaS applications cannot be overstated. Not only do many SaaS apps lack the features necessary for enterprises to be compliant in the cloud, SaaS vendors following the Jason Fried/David Hansson school of product design might decide they don't want to add those features. Policies are the heart of this product, leaving us with the impression that we're closer to 'cloud NAC' than 'cloud firewall' as an analogy for how this product works.

FireLayers organizes its product's capabilities into three categories, like most others in this market, but the functionality is divided a bit differently. FireLayers ANALYZE includes the reporting and analytics portions of the product – the company does not currently have a 'shadow IT discovery' tool like some of its competitors. ANALYZE helps customers understand the risk, compliance, and security gaps related to application use and user behavior. By analyzing behavior, FireLayers attempts to discover and alert on anomalies that could represent attempted or successful breaches. In the ANALYZE tool, the customer can drill down into each specific event, down to the application field level. As is the current trend with CAC vendors, FireLayers assigns risk ratings to different cloud vendors, although it is based on application usage analysis, not the results of service-provider questionnaires, SLAs or hosting details. Detecting and preventing out-of-band attacks is also a rising trend in the CAC market, and is one unique to the reverse proxy architecture. Although this architecture also has its own drawbacks (namely the possibility of breaking when third-party SaaS apps change), because forward proxy architectures don't capture the authentication attempt at the SaaS provider, they will miss out-of-band attacks (i.e., attacks that don't come from corporate-owned devices).

The FireLayers RESPOND tool within the product is a unique approach in the CAC market. RESPOND is really a research center to help customers understand where the risks are and how to develop more effective policies. The company places a lot of emphasis on its FireLayers Response Center, which is responsible for gathering research for RESPOND and interfacing with customers on technical requests. Third-party research, information from known breaches, known vulnerabilities and industry best practices (e.g., Cloud Security Alliance material) also feed into this research. The result is predefined rule sets that can be applied in policies deployed by the CONTROL tool.

FireLayers CONTROL is where the in-line manipulation of application traffic is implemented. This, like the other tools, is entirely SaaS-based, and allows the customer to modify how traffic is handled in the FireLayers reverse proxy. In addition to implementing policies and controls, auditing and alerts can also be managed here. With log review and continuous monitoring being pervasive requirements across regulated industries, the ability to audit user actions regardless of whether the SaaS vendor supports client-accessible logging is essential for many organizations. Rule sets within

policies are assembled in a simple graphical manner, choosing rule elements from lists. Building rule sets goes a bit like this:

- Select who the rule should apply to (e.g., accounting, helpdesk, Web applications, payroll admins, etc.).
- Choose how it should apply, or in what context (e.g., not from mobile devices, only during business hours, only from within the United States).
- Choose what apps it should apply to (e.g., Gmail, all CRM apps, file-sharing apps).
- Select the functions within the app(s) the rule will apply to (e.g., download data, upload, reset password).
- Choose an action to apply: allow, block, request approval for access, terminate session (forcing re-authentication) 2FA, give user a visual warning (achieved by inserting JavaScript).
- Choose whether to audit, mask data, encrypt data, alert on rule execution or track rule execution.

There are predefined rule sets, but customers can create custom rule sets or request made-to-order policies and rule sets from FireLayers. When choosing the SaaS apps to apply a rule to, customers can choose to go vertical (based on a single app, like Office 365), go horizontal (a rule based on password reset will affect that function across all apps being controlled) or apply globally across the entire system. Rule-creation can also be approached from an IDS/IPS perspective, and can be based on detection of malware, suspected data leaks or anomalies. Another use of the 'action' function within rule-building serves to educate users as to why they might have been blocked or are otherwise not allowed to use a feature, rather than leaving them thinking that the application has suddenly broken.

Predefined packages for salesforce.com, Microsoft Office 365, ServiceNow and NetSuite are available, although FireLayers has an open API customers can develop for, and additional support can be added on request. Policy structure is based on the XACML 3.0 standard, an achievement the company believes to be a commercial first. As with other CAC vendors that support the reverse proxy architecture, the company says that any app that supports SAML can be supported. In addition, the company also supports OpenID, OAuth and proprietary authentication mechanisms, given the opportunity and time to build custom support. Maximizing flexibility for different use cases and customer requirements, a forward proxy model is also available, and the platform can be run from a customer's private cloud, as well. In addition to the SAML approach, FireLayers also supports integration with cloud SSO providers like OneLogin, Okta and Ping Identity, or a centralized approach like cloud-based DaaS or a SAML gateway.

Competition

The CAC market revolves around adding features and functionality to SaaS applications, generally with the intent to achieve security and compliance goals that the applications fail to achieve on their own. Beyond this general shared goal, some vendors in this market have chosen to specialize, while others aim to offer a more generalized or rounded product. FireLayers intends to keep its focus on compliance, governance and application control. While all CAC vendors include application control functionality as a feature, FireLayers chooses to place the majority of its focus on solving the shortcomings of existing SaaS applications for its customers.

CAC competitors focusing on threat detection and prevention include Elastica, Adallom and Skyfence. Competitors trying to offer something for everyone include Skyhigh Networks and Netskope. CipherCloud and PerspecSys have evolved their products from cloud-encryption gateways to CAC functionality, and still maintain an encryption-heavy focus. Bitglass has a data protection focus. Cinaya, CloudLock, LogMeIn, Zscaler, Intermedia and Gemalto also have products that compete in this space. For more details on many of these vendors, see our Sector IQ report Cloud application control: a crop of startups ripe for harvesting.

SWOT Analysis

Strengths

As one of the smaller startups in the CAC market, we think it wise of FireLayers to focus on the core application control feature, rather than the more marketable shadow IT problem. A focus on compliance and governance is also more likely to net early profits than targeting the wider general market.

Weaknesses

As with others that have chosen the reverse proxy architecture, there is a chance that the product can break in some ways if not updated in anticipation of third-party SaaS changes.

Opportunities

We believe early customer wins that agree to share their stories, especially large ones with persuasive use cases, will be key in accelerating the growth of this market.

Threats

Interest from enterprises and investors alike justifies the market's quick growth. More than 16 vendors now compete, with widely differing products and approaches. With most employing monthly subscription models, competition is fierce, with stories of large customers already changing allegiance.