REPORT REPRINT

London calling - CensorNet rocks its CASB with two-factor authentication

GARRETT BEKKER, ADRIAN SANABRIA

27 MAY 2016

With the addition of context-based, granular access controls, the company now boasts one of the broader collections of SaaS security offerings and a flexible architecture that can help enterprises connect the dots across their SaaS, Web and email applications under a single umbrella.

451 Research®

 |

Combining the capabilities of traditional web and email security gateways with cloud application control (CAC, which some refer to as cloud application security brokering, or CASB), London-based CensorNet has a unique take on security for SaaS- and Web-based applications. After adding SaaS app discovery, analysis and control to address the 'shadow IT' problem and launching its CensorNet Unified Security Service (USS) in the past year, its most notable move was the acquisition of Denmark-based multi-factor authentication (MFA) platform provider SMS PASSCODE in February to provide the ability to control who is accessing applications, from where and what they are allowed to do – all based on context.

THE 451 TAKE

As we see it, the current market for securing SaaS- and web-based applications is siloed, with too many players offering just a single piece of the puzzle. While the current status quo might suffice for short-term tactical needs, over the long haul we anticipate convergence of the current tangle of point products as an inevitable stepping-stone to more widespread adoption. In that spirit, we like the approach CensorNet is adopting, and with the addition of MFA and context-based, granular access controls, the company now boasts one of the broader collections of security offerings and a flexible architecture that can help enterprises connect the dots between what is happening across their SaaS applications, web apps and emails under a single umbrella. The challenge will be to somehow stand out in one of the most heavily funded and high-profile security segments.

CONTEXT

CensorNet was founded in 2007. CEO Ed Macnair joined the company after a management buyout in 2014. Prior to CensorNet, Macnair founded and served as CEO of SaaS single-sign-on (SSO) vendor SaaSID, which was acquired by hosting firm Intermedia in 2013 for an undisclosed sum. Prior to SaaSID, Macnair served as CEO of Marshal Software following a management buyout of email management, web security and firewall assets from NetIQ in 2005 – which the latter had obtained in 2002 when it paid $23m in cash for Marshal.

CensorNet had previously been technology-driven, and focused little attention on sales and marketing. In early 2015, the company had about 12 fulltime employees and claimed over 400 enterprise customers, although in the past year it has been hiring aggressively to build out the team, including developers for mobile apps and sales and marketing personnel, increasing its headcount to nearly 50. With the purchase of SMS PASSCODE, CensorNet will have nearly 4,000 customers and 100 total employees spread across its headquarters in London and offices in the US, Denmark, Sweden, Norway, Finland, The Netherlands, Germany, Austria, South Africa and – soon – Australia. 451 Research estimates that SMS PASSCODE added roughly $10-15m in revenue, bringing total sales to $15-20m. About 60% of CensorNet's customer base has historically been in the education vertical.

PRODUCTS

The company initially provided web content filtering technology, which essentially blocks users from visiting malicious, suspicious or inappropriate websites based on reputation lists of known-bad or suspicious URLs. One of CensorNet's key differentiators is its architecture. Traditionally, web security products were network-based proxy devices that were installed at the network edge to provide secure access to web content.

However, network-based devices are of limited use for remote and mobile users, and thus cloud-based web proxies have become increasingly common as an alternative. Web proxies have their own challenges, however. They typically work only with HTTP traffic, examine traffic in just one direction (outbound), can present performance bottlenecks and introduce latency when they are hosted in datacenters – i.e., no longer close to end users – and traffic must be routed through a central location. In addition to latency, Web proxies can block the true location of a mobile user – websites will only see the IP address of the proxy – nullifying the effectiveness of location-based services and websites and apps that are dependent on IP-based location data.

CensorNet has instead developed a hybrid architecture that combines an on-premises appliance, multi-tenant SaaS version and low-footprint agent that can be installed on a laptop or tablet. Users behind the corporate firewall are routed via the appliance, while for mobile or remote users, the agent performs a simple lookup against a cloud database to restrict access to both traditional websites as well as cloud applications.

The company claims that the agent adds no latency and doesn't require any browser configuration, and since the user can maintain a direct connection to the web service, location-based services still function normally. It allows granular access to various parts of a SaaS app without breaking functionality, as proxies sometimes do. CensorNet's goal is to be able to see everything that goes in and out – and also work with a broad range of protocols beyond just HTTP – by using the agents to detect activity occurring outside of the web browser and feeding that activity to a threat detection and behavioral analytics platform.

For web filtering, the company offers most of the standard features, including a database of URLs and heuristics, and also has a team of analysts employing third party services to analyze web pages in multiple languages on demand and block zero-day threats and web-based malware. Malware scanning is done through multiple third parties, including Bitdefender. CensorNet also recently added email security, a multi-tenant cloud-based service that relies on eight different scanning engines for detecting spam, malware, phishing and other e-mail based threats.

In addition, the company has introduced CAC capabilities to perform discovery, analysis and control of SaaS apps to help businesses get a handle on shadow IT and what SaaS apps their employees are using, as well as restrict usage of certain potentially risky features such as file uploads, file sharing, data export, etc. CensorNet can also perform desktop monitoring, and record all user activity as a video that can be used for privileged user monitoring and incident response, or to support legal actions.

What SMS PASSCODE brings to the table is mobile-based strong authentication, which, despite its name, is really an MFA platform that can also do voice callbacks, encrypted email and hard and soft tokens on mobile phones in addition to SMS-based authentication. SMS has a password reset offering that CensorNet plans to market more aggressively this year. The SMS PASSCODE platform was traditionally deployed on-premises, but has been gradually evolving into a cloud-based architecture. One notable differentiator is that the technology does not require a seed on each device, which is arguably more secure.

Rather than providing binary yes/no decisions, as most SaaS SSO specialists currently do, the combination of CensorNet's CAC with SMS PASSCODE's risk-based authentication allows for highly granular access control of the specific features of SaaS apps by user, role, device, current network or location. For example, a user can be granted 'view only' access to an application that includes sensitive data when they are using a tablet in an airport, but can download or print the same information when at their desktop and connected to the corporate network.

STRATEGY

In our view, the CAC market as currently constituted addresses only a small portion of the overall SaaS and web security challenge. Combining identity- and location-based authentication with the granular access controls of a CAC vendor is a logical move, and not surprisingly many of the leading CAC firms have partnered with SaaS identity management specialists like Okta, OneLogin, Ping Identity and Centrify. These features have been combined into what CensorNet now calls its Unified Security Service, and a large part of the value proposition for USS is addressing web and email security, SaaS SSO and CAC/CASB in a single offering. In addition to more granular, contextual access control, bringing email security into the mix has some interesting implications for threat prevention. Most threats have multiple vectors, and if administrators can see something downloaded via a SaaS app and subsequently sent out through email, there is value in being able to visualize and correlate the different channels and uncover potential relationships.

There are some cost synergies to be had, as well. Like a twice-daily trip to Starbucks, the $4-per-user/per-month pricing strategy of most SaaS security services might seem cheap at first, but can add up quickly, especially as more and more single-function products are layered on. Combining multiple functionalities into a single offering makes financial sense, particularly for small to midmarket customers.

CensorNet's primary go-to-market strategy is to white-label its offerings for MSPs, particularly those that might prefer to host the technology on their own datacenter infrastructure and push their own brand rather than, say, Zscaler or Cisco's ScanSafe. The company has APIs to provision into MSPs' existing billing systems. The initial strategy is to talk to not only large MSPs like Verizon and Vodafone, but also tier two MSPs such as j2 Global. In addition, SMS PASSCODE has some key partnerships with Cisco, Juniper and Citrix.

COMPETITION

At a high level, CensorNet is aiming to provide a single offering that bridges the gap between SaaS-based web content security vendors, email security firms and cloud application control providers. The former group includes Websense (acquired by Raytheon in 2015 for $1.3bn and now known as Forcepoint), zScaler and ScanSafe (purchased by Cisco in 2009 for $183m in cash), while the latter includes Adallom (bought by Microsoft last year for an estimated $250m), Bitglass, Elastica (acquired by Blue Coat in 2015 for $280m), Netskope, Imperva Skyfence and Skyhigh Networks.

In the short term, expect additional competition to emerge from incumbents both in CensorNet's midmarket segment (the likes of Sophos and Barracuda, for example) and upmarket. An acquisition by IBM or Akamai could shift the space considerably, and both have already made moves in this direction: IBM with its Cloud Security Enforcer offering, and Akamai with its purchase of secure web gateway firm Bloxx and investment in CAC specialist FireLayers. Akamai made its announcements within two weeks of each other last fall.

Authentication is among the most fragmented and competitive sectors in a generally fragmented overall security market. With the addition of SMS PASSCODE, CensorNet should also now be considered potentially competitive with a very long list of fairly fungible MFA vendors that 451 Research estimates at well over 100 strong. Notable names in this category include legacy authentication giants like EMC's RSA Security, Entrust Datacard, Gemalto's SafeNet, Symantec and VASCO, as well as more recent entrants such as Duo Security, SecureAuth, Yubico, Keypasco, Swivel Secure, TeleSign and others.

SWOT ANALYSIS

STRENGTHS

With the addition of context-based, granular access controls, CensorNet now has one of the broader collections of security offerings and a flexible architecture that can help enterprises connect the dots across their SaaS, Web and email applications under a single umbrella.

WEAKNESSES

The company lacks the name recognition of some of the higher-flying – and heavily funded – CAC providers. While USS is one of the broader SaaS security platforms out there, there is room to add other features such as data-loss prevention, encryption or tokenization for data sovereignty or compliance use cases.

OPPORTUNITIES

Although we've barely scratched the surface, security remains the number one barrier to cloud adoption. Accordingly, the SaaS security market has the potential to become a major piece of the overall security picture as cloud computing becomes more mainstream.

THREATS

SaaS security is in the early stages, and while startups have driven the early action, we think it's just a matter of time before industry heavyweights like IBM, Intel's McAfee, Symantec, Cisco, and Palo Alto Networks get serious about the opportunity.