REPORT REPRINT

# Knocking some (App)Sense into endpoint security

ADRIAN SANABRIA

4 FEB, 2016

As its only close competitor in the user environment management space moves in a different direction, AppSense sees opportunities in refocusing on its security capabilities. Far from a pivot, the security focus centers on the company's original product, released in 1999.



451 Research®

Security technologies occasionally get a bad rap. Sometimes a perfectly reasonable approach to addressing security issues is marketed beyond what it can deliver. Sometimes current technology isn't quite there yet. Sometimes the technology is there, but customers aren't ready. Whatever the cause, good ideas deserve second chances, and we often see comebacks. In the past few years, we've seen a resurgence of interest and innovation in security analytics (post-SIEM), network access control (NAC), and now the concept of application whitelisting.

AppSense is seeing this resurgence clearly outlined in the form of growing interest in its Application Manager (AM) product. AM has a history that goes back far beyond even the first big application-whitelisting push, helmed by the likes of Bit9, Solidcore (acquired by McAfee) and Lumension. It goes to show that good ideas in security don't (and shouldn't) die – they merely resurface when the market is done being distracted by the latest hot trends, and realizes they are still needed.

## THE 451 TAKE

Our research suggests enterprises with security-staffing challenges aren't looking for a product to stop all endpoint threats and attacks. Rather, they're interested in stopping enough of the attacks to gain some breathing room. Multiple layers of defense are more practical and effective than relying on a single technology or product, particularly in the case of endpoint security. This is good news for AppSense and the rising popularity of its AM product. While the company currently sees 70% of customers buying an entire suite, we anticipate the demand for the AM module alone will continue to rise. AppSense is fairly dominant in its own space of user-environment management, but it constantly runs the risk of becoming superfluous in the shadow of its primary software partners (Citrix, VMware and Microsoft). Although AppSense isn't traditionally thought of as a security vendor, access to the endpoint-security space through the AM product allows it to diversify its business without leaving its core competency behind. Additionally, AppSense has years of experience catering to the needs of both the user (performance) and the administrator (manageability). The company is well positioned to ensure security doesn't compromise the user experience or make the IT administrator out to be the 'bad guy.'

## CONTEXT

AppSense was founded in its current form in the UK, in 1999, by Charles Sharland. It began its journey in the world of virtualized desktop environments by aiming to lock down Citrix environments. Since then, the company has been through some changes, and has nearly come full circle.

After US sales began to account for more than half of the company's revenue, a global headquarters was established in Sunnyvale, California, but the UK office in Daresbury remains the EMEA headquarters. In numbers, the company counts more than 400 employees, and 3,600 enterprise customers that account for more than nine million endpoints. The leadership at AppSense has deep roots in virtualization and security, with much of the staff having a background with Citrix or HP's Information Security division.

## STRATEGY

While Citrix was clearly the key partner in the beginning, the company expanded its offerings into broader user-environment management use cases. Administrators could set and enforce policies, and users enjoyed a familiar environment wherever they logged in.

Between 2010 and 2013, AppSense saw rapid growth, as well as major changes in corporate strategy. The company's only acquisition and its only round of outside funding occurred during this period. An injection of $70m from Goldman Sachs for a 28% stake in the company prefaced the acquisition of RAPsphere in 2012. This led to rumors that it might move away from desktop products, and focus exclusively on the mobile market.

Talk of a 2013 IPO ended after some major changes in leadership, most of which remain in place today. Current CEO Scott Arnold stated then that an IPO would create distractions, and that there were other ways of raising cash if necessary. This seems especially wise from today's perspective, where security stocks are in a slump, and there are already rumors of upcoming 2016 security LBOs.

The post-2013 AppSense is a company refocused on its core user-environment management offerings, including the ability to lock down aspects of the user environment – mirroring the original product goals from 17 years ago. Also mirroring the past are the company's primary software partners: Citrix, VMware and Microsoft. Although some speculated that each of these vendor's acquisitions over the years would erode the company's market share, continued differentiation and innovation has allowed AppSense to maintain its position.

In particular, AppSense has noted a resurgence of interest in the endpoint-security market. Of the five categories we've divided endpoint-security products into, the largest, and one of the most diverse, is the post-AV prevention market. A sizable chunk of the 31 vendors in this space have recently refocused on application whitelisting. AppSense has an improved approach to preventing unauthorized app execution with its AM product, which it believes will give it an upper hand in the battle for returning peace and (mostly) freedom from malware to the endpoint.

## TECHNOLOGY

To be fair, application whitelisting was never truly a failure technically. The only failure was in the attempt to market the technology as broadly applicable, when it was better suited to niche use cases. For most administrators, the limitations of traditional application whitelisting were human ones. IT employees quickly found it was impractical to maintain static whitelists when users were attempting to download and run new applications on a daily basis.

For environments that handled highly sensitive data and didn't often change, application whitelisting was a hit, and it continues to saturate the healthcare and retail/payment markets. The perception that app whitelisting had failed to 'solve' the endpoint-malware problem stuck, however, and the stigma remains for some brands.

Undeterred, AppSense looked for a compromise – a way to block malicious executions without creating the management issue of maintaining a static whitelist. Dynamic whitelisting is the most common term representing application whitelisting's comeback, and AppSense refers to its approach as Trusted Ownership. This approach leverages file system (NTFS) ownership to block users from executing files from untrusted sources. It is quite common for malware attacks to target system privileges, which is an immediate red flag that AppSense's AM product can identify and block. In fact, any file where the owner is deemed as untrusted can be blocked from executing. AppSense also offers traditional whitelisting and blacklisting functionality after the Trusted Ownership screening process.

After considerable research into what companies are looking for in the post-AV endpoint-security market, the result was that the ability to stop 100% of malware and attacks (or close to it) isn't nearly as important as just stopping some of them. The problem for enterprises is directly related to the balance of efficacy and labor. The average security team, it seems, is primarily interested in ending the cycle of madness – the constant malware infections that threaten to indefinitely prevent other security projects from getting done.

Many products in the post-AV market aim to directly fill this need – to block as many attacks as possible while requiring as little work as possible on the part of the customer. The customer doesn't need this product to be effective 100%, 90% or even 80%. The value of a prevention product for such an embattled environment is especially apparent when 90% of the effort is spent closing the final 10% of gap.

## PRODUCTS

AppSense is well known for its DesktopNow suites, but has made several changes to its product lineup over the years. Currently, the DesktopNow Plus suite includes six products, most of which can be purchased separately. Management Center and Environment Manager give IT complete policy-based control over how a user's desktop is configured. From a security standpoint, it can be quite simple to return a desktop to a known configuration state without having to reimage the entire system. DataNow is the company's enterprise file, sync and share product. Performance Manager polices processes that threaten to abuse system resources and slow things down. AppSense Insight takes data from all applications, providing useful analytics and 'insights' into desktop usage.

The final product in this lineup, AM, could be thought of as the 'endpoint security' product, but security features are just part of its capabilities. It is AM that has the application whitelisting/blacklisting and Trusted Ownership features. Traditionally, Environment Manager was the bestselling product. But it has recently been outsold by AM, which is now the fastest growing product in the AppSense portfolio, and has inspired the company to place more emphasis on security use cases and needs that can be met by AM. As previously mentioned, this is a very mature product, with its debut occurring in 1999. AM is currently on version 8.

One of the problems that resulted in the death of app whitelisting 1.0 in the last decade was a general disdain for the user experience. This is something AppSense recognizes, and has taken special care to account for with AM. To illustrate this challenge, the company points out that many changes are not risks, but do require administrative rights. Changing the date, time or time zone, for example, is allowed; whereas other changes requiring administrative rights are locked down.

The product allows for a variety of configurations. While you can lock down application execution tightly, some organizations might prefer to allow users to run a program, but only after including a reason for running it. Policies can be applied using specific file attributes or metadata. Users more heavily locked down may have to request access to run or install an application. All these events are written to an AppSense-specific Windows log, and can be ingested by a SEIM.

The AppSense Insight product has security value also, in that it can collect and report on many details and aspects of managed systems. Insight can be used to detect anomalies that could indicate a wide variety of security issues, from unauthorized use to malicious software activity. Insight could answer many questions: Are too many exceptions being granted by the help desk? Why are they being granted? What is the customer using these exceptions for? How bad is the software-licensing situation?

## COMPETITION

AppSense's AM, when sold alone, is likely to compete with both whitelisting and privileged-account management products. Endpoint-security products with whitelisting include (but are not limited to) Avecto Defendpoint, Carbon Black Enterprise Protection (formerly Bit9), CyberArk (Viewfinity), Digital Guardian, Kaspersky Lab, Lumension, McAfee (SolidCore), Microsoft (AppLocker), Sophos, Trend Micro and Tripwire.

A key differentiator that benefits AppSense is the native integration between all the apps in the DesktopNow Plus suite of products. Another is AM's Trusted Ownership approach. The addition of privileged account management gives AppSense a respectable shot in the endpoint-security market.

## SWOT ANALYSIS

### STRENGTHS

AppSense has more to offer than just an endpoint-security offering. Its products are mature, widely deployed and proven. Trusted Ownership is a unique approach that could breathe life back into application-list management as a broad (not just niche) approach to protecting endpoints. Combined with privilege management, the AM product is highly competitive with other 'next gen' endpoint-security offerings aiming to complement traditional AV.

### WEAKNESSES

With the full DesktopNow Plus suite, AppSense puts a lot of agents on the endpoint, but it isn't likely to replace any existing endpoint-security products. Convincing customers to put an extra 3+ agents on an endpoint is a tough proposition.

### OPPORTUNITIES

Some additional prevention capabilities would provide a more solid competitive base for AM. Endpoint-security vendors are currently consolidating (particularly Digital Guardian and CyberArk), upping the ante for competition, and potentially raising the bar to entry. The acquisition or addition of exploit-prevention technology would make AM much more robust from a security standpoint.

### THREATS

As previously mentioned, the post-AV prevention space contains at least 31 vendors. The endpoint-security space as a whole contains more than 60 vendors. Being heard above the general cacophony of the startups and claims in this market will be challenging.