Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Endpoint Security through Application Streaming

Businesses are moving from a centralized core infrastructure to a decentralized one. This causes a number of issues as our businesses grow. The main issue is data flow. How do businesses maintain security when data is continually moving to the edges of our logical boundaries? Many solutions have come up to address this problem, endpoint security software, restricted rights, VPNs, strong Bell-LaPadula models, and more restrictive user policies. A solution is needed that solves the problem while allowing the user to comp...

Copyright SANS Institute
Author Retains Full Rights

AD

Endpoint Security through Application Streaming

GIAC (GISP) Gold Certification

Author: Adam Walter, adam@adamandrea.com
Advisor: Hamed Khiabani

Accepted: February 10th 2013

© 2013 SANS Institute. Author retains full rights.

Abstract

Businesses are moving from a centralized core infrastructure to a decentralized one. This causes a number of issues as our businesses grow. The main issue is data flow. How do businesses maintain security when data is continually moving to the edges of our logical boundaries? Many solutions have come up to address this problem, endpoint security software, restricted rights, VPNs, strong Bell-LaPadula models, and more restrictive user policies. A solution is needed that solves the problem while allowing the user to complete business tasks efficiently and without incident. Why not centralize again? The solution proposed in this paper works around keeping business workflows decentralized while centralizing data through application streaming.

1. A Problem

1.1. History of networks

Throughout the last 30 years technology has undergone a shift in implementation. The technology fundamentals are the same but the data itself is being used in new ways. In the 70s and 80s businesses largely had centralized databases with access terminals streaming data. This was simple, efficient and secure. A user could not pipe data from one location to another without the express permission of technical administration. Egress was limited to printers as the dumb terminals had no storage and no way to export data other than via screens and printers. However, these systems were very expensive and had a single point of failure. As well users often had to wait for processor time when the system was under high load.

As businesses progressed further into the '80s computer parts became more affordable, networks became more complex, and storage mediums became more plentiful. Businesses now had end nodes that could stand alone. These new more powerful nodes could hold and process data at an alarming rate. This was great news for business as it increased availability and distributed process time for users. These new PCs were allowing smaller businesses to compete on a larger scale and therefore were very popular.

In the '90s the Advanced Research Projects Agency Network (ARPANET) was decommissioned (Hauben, 1995). As ARPANET faded, Wide Area Networks (WAN) became a corporate standard. Advanced networks were no longer just for academia; they were an essential tool for business communication. Businesses saw data shared across multiple physical sites. Users could now transmit copies of data to each other with little effort. Sites would soon have their own copy of the data for use. While in the '70s the business technical administration controlled the flow of data in the mainframe, in the '90s the user gained increased control of where data flowed. IT departments now had to deal with multiple copies of data spread across multiple sites and mediums. In minutes data

© 2013 SANS Institute. Author retains full rights.

could be copied to hard drives, removable media, and pushed to e-mail accounts across the world.

This popularity increased as the PC became smaller and more portable. Towards the end of the '90s businesses saw mobile devices start to become commonplace. By 2004 Research In Motion (RIM™) reported reaching 2 million subscribers (Research In Motion, 2013).What used to require time at a terminal in a lab now could be done with a device held in your hand anywhere in the world.

1.2. Security

With this explosion came new problems in data integrity and confidentiality. How do businesses incorporate all the new egress points into their strategy? Technical administration has been so busy deploying and building systems that little is done in terms of securing data in an environment. In 2011 Verizon's annual report stated that "96% of attacks were not highly difficult" (The Verizon Data Breach Report, 2011).

With Information Technology (IT) departments stretched beyond their limit in deploying new infrastructure they have had to find different solutions to meet security requirements. To make things simpler the security industry has identified ways to handle risk in an easy to digest fashion. Below this paper will discuss three of these methods for handling risk in regards to mobile platform security; acceptance, mitigation, and avoidance.

1.2.1. Acceptance

This is obviously not preferable but is common throughout networks especially in the Small and Medium Business (SMB) market where it is a common belief that they are not a target. These SMBs are severely restricted by budgeting and personnel so they have seemingly little choice. Adherence to International Organization for Standardization (ISO) principles guidelines is important (ISO, 2013). However, the Verizon Data Breach Report reports even larger companies have been seen to "accept the risk" without with much more thought, even though they may have resources dedicated to defining appropriate risk levels and tiered strategies to back them up (The Verizon Data Breach Report, 2011).

© 2013 SANS Institute, Author retains full rights.

The good news is that accepting the risk is kept in check by compliance audits and controls. To handle audits, companies today have a variety of seasoned personnel that can help them understand what acceptable risk is, and what it is not. Once a business has an understanding of what the risk is they can make an educated decision whether to accept it or handle it in another fashion.

1.2.2. Mitigation

Mitigation has always been a tricky subject. What is mitigation? Who determines whether a threat is adequately mitigated? If the business has the resources to afford a third party vendor or have an in-house security team then they can adequately supervise mitigation. However, many businesses are at the mercy of audit requirements and they don't respond to mitigating controls until they are under pressure. This can lead to band aids and lots of follow-up work while the overworked technical staff scrambles to obtain compliance.

To complicate matters, businesses have added complexity to their best practices by adding mobile infrastructure. How do they maintain policies regarding data confidentiality and integrity on devices that can be anywhere? Some companies simply deny mobile devices on their network (see Section 1.2.3 Avoidance on page 5). Others attempt to secure the data in device sandboxes, or restrict sensitive data to physical locations. However, with the number of egress points that mobile platforms provide, mitigation is difficult. We needed an efficient way to detect and manage all these egress points.

It used to be that a business could only detect a threat to their environment through hard work and a good understanding of the attacker's tools, or hiring a pricey third party. Now businesses have robust appliances that can scan a network at the push of a button. These appliances provide IT staff a breakdown of risks on their network and often a method for mitigating threats. This has been a big boon to the IT security field as it reduces the need for costly additional third party audits.

© 2013 SANS Institute. Author retains full rights.

Finally, compliance guidelines have been updated regularly to help with the mitigation efforts. With the arrival of the mobile platform businesses now see security controls being created to adjust for these new egress points.

Nicholas J. Percoco (2012) said:

> The challenges are broad and many but some of the top issues revolve around management/control over the device, the integrity of the payment applications, and the security of the payment process.

This was in response to a new set of PCI best practices regarding mobile device payments. As a business move through a PCI audit they must respond to mobile device controls. This clarifies to the IT professional what needs to be done. Security controls also inform departments of vulnerabilities they may have missed.

Sometimes mitigation and acceptance are just too expensive or restrictive to business practices. This brings us the final option discussed in this paper.

1.2.3. Avoidance

Sometimes businesses make the hard decision to cut off problems at the head. A common problem is mass storage devices. Eventually you have to decide how much that service is worth. Often the question answers itself and the device is unceremoniously disconnected from business ecosystems. Sometimes businesses take a more complex route and create different zones for nodes on a network, this is called segmentation. Segmentation is becoming a key factor in avoidance. However, this often requires scrutiny by a third party as technical staff members can have a misunderstanding of what segmentation strategies will adequately satisfy a risk.

A major problem with avoidance is that it causes extra work for IT staff members. Either you have to do without a tool, re-architect a solution (usually on short notice and no budget), or deal with multiple firewalls through your network. Avoidance ends up being no fun for IT departments in the end, there are complications as the business ends

© 2013 SANS Institute. Author retains full rights.

up tip toeing around the risk going forward. Every time a new business line comes in a strategy needs to be created to avoid the risk.

1.2.4. Remarks

When dealing with security things are getting messy in our decentralized world. Two major factors are budget and time. The SMB is not the only market struggling with these issues. Enterprises are also struggling with mobile users on a larger scale. So how do businesses keep up with end nodes, compliance, reliability, and security when there are a wide variety of items running different operating systems in disparate locations?

One option is to hire resources to manage the complex workload. Businesses are exploding when it comes to personnel to keep up with this diverse market (Bureau of Labor Statistics, 2012). But what if businesses decided to simplify? What if instead of heading down the road of diversification businesses brought it all back to their origins? Egress reduction has always been a goal, but this has moved further and further away from our grasp.

A great example of a mess that has been introduced is mobile phones. As smart phones hit the market, avoiding this risk became more difficult as productivity gained through these devices became justifiable. However, businesses couldn't just give people smart phone access to business systems, the financial and security implications were too great. They couldn't let sensitive information spread around like that. There was a great need to control the data flow or deny the request. They had to guarantee that they had control of sensitive items.

Enter the Blackberry. The need for a functional phone that could be controlled by the business was seen and met. This device was integrated into the workforce and was completely managed by infrastructure. It was great, everyone was happy and risk was avoided. Then something horrible happened to the IT world. The smart phone started trending. Suddenly it was not good enough that the phone be used for business purposes, as younger generations started getting smart phones, the desire for entertainment on our phones rose. Platforms like iPhone and Android appeared as contenders. As of 2012 it

© 2013 SANS Institute. Author retains full rights.

was reported that they weren't just contenders for the mobile market, they were the dominating force (Gartner, 2012).

IT departments could not manage these devices centrally and easily. Normally IT would stick to their guns and enforce a no non-managed devices policy, but it was too late and the workforce was addicted. Then pressure started, and exceptions were made. So what used to be risk avoidance became risk acceptance. Many businesses still handle mitigation by creating user policies and signing wavers to transfer risk. In the end risk avoidance put businesses in a messy world.

How does technical administration end up handling this issue? Ask them about the mobile workforce and you will get a lecture on security and standard practice. If you ask them about the use of personal devices on the network, you will get a variety of opinions. However you look at it, mobile workforces are a real issue in the IT workplace as every week a shiny new device is introduced to the world.

The marketing folk are very interested in selling you technology but they know IT is burned out on mobile platforms. So they have ripped off the "mobile workforce" sticker and slapped a new one on. Bring Your Own Device (BYOD) is currently filling the heads of executives with hopes and dreams while striking terror into the seasoned administrator's soul.

Businesses are living in a world where BYOD is a reality. That is unless you work for a company with exceedingly high profit margins that can afford to buy mobile devices for all its employees. In many cases BYOD is done against the IT administrators recommendations, in others it is with their blessing. There are many concerns with BYOD in the infrastructure, security is the foremost, but also you have application compatibility, supportability, and consistency to worry about.

When you talk to security administrators about BYOD the major issues boil down to two problems; OS stability and endpoint security. Most administrators they want stability and control. However, what if businesses took the OS and endpoint security out of the equation and avoided the risk? Well while we are at it, I want an easy button and a unicorn. As lofty a goal as this is, it may be possible to do exactly that in enterprises. At

© 2013 SANS Institute, Author retains full rights.

least that is the direction technology is pushing. Whatever side of the fence you are on, the following proposes a solution to fit business needs.

2. A Solution

2.1. A lesson from the Mainframe World

As the IT field matures, businesses are learning to look at successful technology practices and apply them where applicable. One mature technology that has been successful in securing data as well as delivering it is the mainframe.

There is a bad stigma in the IT world that the mainframe is dying. However, "…more than 95 percent of the top Fortune 1000 companies use IMS to process more than 50 billion transactions a day and manage 15 million gigabytes of critical business data" (IBM™, 2005). Also, at Syracuse University students can work to achieve a minor in Global Enterprise Technology. Individuals are encouraged to understand the computing needs of enterprises to supplement their major. This suggests that there is a draw for our future professionals to have an understanding of mainframes in the modern business world.

So let us take some time to look at the mainframe security model. As you will see with the following, mainframes enjoy a feature many modern technologies do not. Data is centralized under one ecosystem.

Computer Associates published a very interesting compliance whitepaper on the need for increased security on the mainframe. The paper outlines the need for policy based controls:

© 2013 SANS Institute. Author retains full rights.

According to Harbeck (2012):

> In other words, a security administrator should not have to understand the underlying technical details of a system in order to setup a permission that responds to a simple requirement in all cases. Therefore, it is essential to externalize security outside of applications, so that it can be enforced centrally based on a set of security policies defined for the complete IT environment. These security policies are generally based on a set of user roles defined for the entire user population.

In the paper it outlines the guidelines for using policy based controls based on the Control Objectives for Information and Related Technology (COBIT) framework. This policy based framework in a mainframe is simple. Administration of diverse egress points becomes simplified. The business gets to control where data flows through policy on one system. Since this is a single system, auditing of policies becomes greatly simplified. An administrator now has a single pane of glass to review and generate reports in order to attain compliance.

However, there are multiple costs associated; personnel, migration, and maintenance. IBM™ has worked hard to make their Z series platform affordable. In the end though, there still is a lot of stigma against moving to a mainframe platform for data management.

2.2. Centralizing the Distributed Network

Now that we have taken this detour what do we take away? Centralization is handy. Businesses love to have all our data in one place. It speeds up transactions, simplifies security, and aids in compliance. However, businesses are not going away from a distributed network anytime soon. Our businesses need availability on the road, they need to use the products that employees are trained on, and they need to always be aware of continuity.

In a security survey 61% of the businesses had a BYOD policy (Johnson, 2012). One of the great things about BYOD is that it has management thinking properly about security. There seems to be a misconception that "I own it so it is safe". With BYOD

© 2013 SANS Institute, Author retains full rights.

businesses are putting the fear into the checkbook holders. Now it is a matter of "We don't know where those devices have been!" So businesses are pushing cash into network segmentation, increased monitoring, and security.

With this attention to security there has been a technology that has matured very well and there are several competitors vying for attention. Application virtualization, in particular application streaming, has come a long way. Citrix is the frontrunner here. Forget the pains of metaframe, it is a different world out there now.

What is application streaming? To answer this we need to move to a high level understanding of the technology as each vendor implements the technology differently. Application virtualization takes software and encapsulates it to fool the client OS into believing it is running in the local runtime. The client has an application experience similar to a local one. However, data never truly leaves the host servers.

So what is making this possible? Thanks to ecosystems like XenApp and App-V you can serve up applications without the data ever leaving the datacenter. These are not the only ones in the marketplace though; VMware is developing their own solution so keep an eye on them. It has been reported that several other competing cloud based solutions out there trying to get a foothold (Enterprise iOS, 2012). Each vendor has a different implementation but they all have a similar end goal. Take an application, and deliver it to any client while keeping it in a central memory space. This effectively turns any endpoint into a simple terminal.

There has been an interesting turn of events here. However, as businesses work on pushing more and more into a mobile workforce they keep asking the same question over and over... Will it work with Windows, what about OSX, iOS or Android? What happens when the stream is broken? What kinds of security protocols are used and is my device compatible? Each of these questions is handled by the vendors in a different way. What will fill a company's needs is unique, so the variety of vendors is a great thing.

Right now you can use virtual application services to publish an application to pretty much any OS out there. Since the application is residing on a core host the client does not need the resources to manage the full application. This means businesses can

© 2013 SANS Institute, Author retains full rights.

now run an entire office suite on a thin client or a smart phone. No more worries about endpoint delivery when every application has a tunnel to a sandbox with no interactivity with the end device other than what you permit. Security is broken down to a single sandbox. Just like the mainframe. Administrators control the policies on data flow and segmentation. Professionals now know exactly where data is at all times, and get to say where it goes. This makes compliance a dream. Your auditors can be handed one log for sensitive data to show that it has been safeguarded.

This truly is a game changer; this will change the way administrators around the globe view accessibility and security. There are tradeoffs, but for the moment, the horizon looks pretty bright and clear. A new day is approaching where it doesn't matter what the endpoint device is or where it comes from. You are bringing functionality and security to every device on your network, whether it is a thin client, phone, tablet, laptop, or PC. It will simplify administration and delivery. It will make management happy by allowing shiny thing syndrome to run rampant. Yes there is a learning curve but one that technical staff are more than happy to deal with.

© 2013 SANS Institute. Author retains full rights.

3. Conclusion

3.1.1. Prepare

As with any security measures it is a matter of seeing the horizon and being prepared for what is coming. With application virtualization you are moving towards an environment that is much easier to grasp. The security problems don't go away but by simplifying your environment you can make mitigation something much more attainable. Businesses can't all be implementing the best technology as soon as it is available. However, businesses can start preparing their environment and budget for future security controls. By forecasting they can be ready for the environment that will make their business a success.

In the end, there are no magic bullets to fix all our security issues. However, businesses can move in the right direction. With application virtualization and the centralization of the data they are doing exactly that. It is now necessary for network administrators to begin preparing their environments for the execution of this goal. Businesses should be looking at application virtualization just as they do with IPv6. They know it is coming so they plan architecture developments with that in mind. Preparing your network for application virtualization is a matter of steady transition.

3.1.2. Segment

Consider a minimum of three security zones; internal, DMZ, and Secure. You should do more but when virtualizing applications you will want to make sure that they are segmented off from everything they should not have access to. This is paramount to good security practices. Therefore, when a company has the resources to move to virtualization platforms there will be a home for the data.

3.1.3. Standardize

Standardization is something IT firms have been fighting for years so it is nothing new. If you are not imaging in the enterprise yet, start. Imaging forces standardization of builds, software, and hardware. This will ease the transition to a

© 2013 SANS Institute, Author retains full rights.

virtual PC later. Once your users are used to the idea of every PC being the same they will embrace the idea of application virtualization even more.

Part of the standardization procedure should be identifying your base software suite for your business. This is very important to application virtualization in that you will be pushing out standard applications to everyone. If the users are trained up on the software they will be using virtually, the learning curve will be very small. You might even find that your Database Administrators and developers love the virtualized applications because they can reside in the security zone for their work rather than fight the firewalls for access to data.

© 2013 SANS Institute, Author retains full rights.

3.1.4. Virtualize

Virtualization is everywhere. Whether you are considering a cloud based solution or internal virtualization, it cannot be avoided. For businesses that are moving to the cloud, the application virtualization battle has already begun. However other businesses decide that they need all their applications in house. For them there are some impressive solutions available. Either way, you probably already have started virtualizing your environment and are looking for ways to improve it. Understand that while application virtualization technologies play well cross platform, your life will be made easier if you make the decision ahead of time to choose a virtualization platform that supports the virtual application technology you want.

3.1.5. Final Thoughts

Whatever the strategy is, plan for it. The problems with diverse networks are just that, diverse. Businesses need to take a look at what is going to work for them. They need to understand their history, find what has worked, and make it better. Also, the company needs to be innovative with solutions that will fit the business model. With application virtualization there is an excellent solution. It will not fit all business models but it will simplify many issues. Centralizing data reduces threats, eases administration, and

simplifies the network. With these potential benefits a business should be doing a proof of concept to see if this strategy will fit into their business model.

© 2013 SANS Institute. Author retains full rights.

4. References

Bureau of Labor Statistics (February, 2012). Employment Projections:2010-2020 Summary. Retrieved from http://bls.gov/news.release/ecopro.nr0.htm

Enterprise iOS (2013). Comparison of MDM Providers. Retrieved from http://www.enterpriseios.com/wiki/Comparison_MDM_Providers

Gartner (August, 2012). Market Share Analysis: Mobile Devices, worldwide 2Q12. Retrieved from http://www.gartner.com/resId=2117915

International Organization for Standardization (January, 2013). ISO 31000 - Risk management. Retrieved from http://www.iso.org/iso/home/standards/iso31000.htm

Harbeck, R. (February, 2007). Regulatory Compliance and the IBM™ Mainframe: Key Requirements. Retrieved from http://www.ca.com/us/~/media/files/whitepapers/mainframe_compliance_whitepaper.aspx

Hauben, M. (October, 1995). Behind the Net - The untold history of the ARPANET. Retrieved from http://www.dei.isep.ipp.pt/~acc/docs/arpa.html

IBM™ (January, 2004). Information Management System. Retrieved from http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/ibmims/

Johnson, K. (March, 2012). SANS Mobility/BYOD Security Survey. Retrieved from http://www.sans.org/reading_room/analysts_program/mobility-sec-survey.pdf

© 2013 SANS Institute, Author retains full rights.

Percoco N.J. (September, 2012). PCI Security Standards Council Issues Guidance for Mobile Payment Industry. Retrieved from http://www.eweek.com/c/a/Security/PCI-Security-Standards-Council-Issues-Guidance-for-Mobile-Payment-Industry-672073/

Research in Motion (January, 2013). RIM™ History. Retrieved from http://www.blackberry.com/select/get_the_facts/pdfs/rim/rim_history.pdf

Syracuse University (January, 2013). Minor in Global Enterprise Technology. Retrieved from http://ischool.syr.edu/future/undergrad/minorGET.aspx

Verizon Business (April, 2012). 2012 Data Breach investigations Report http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

© 2013 SANS Institute. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**