WHITE PAPER

PROCURE-TO-PAY AND SUPPLIER PORTAL SOLUTIONS

Implications for Data Security and Access Control

Direct Commerce

directcommerce.com

direct commerce

CONTENTS

EXECUTIVE SUMMARY

Procure-to-Pay (P2P) automation solutions can provide a cost-effective approach for improving your financial supply chain, reducing paper documents, streamlining P2P processes, and deploying supplier portals to eliminate payment- and invoice-related phone calls from suppliers.

There are a variety of approaches to implementing such solutions, but certain options pose higher security risk than others. To a large extent, the security issues you'll need to manage depend on how you implement your P2P deployment.

This white paper discusses security ramifications to consider before selecting the best P2P automation approach for your business.

INTRODUCTION

Procure-to-Pay Solutions: Could Your Data Be At Risk?

With procure-to-pay automation solutions, you can easily eliminate the need to process an extensive volume of paper so you can streamline your invoicing processes, save time, improve supplier relationships, and take full advantage of supplier discounts.

And with supplier portals, your vendors can take advantage of real-time access to invoicing, payment, and purchase order data – eliminating the need for those suppliers to call your accounts payables department to check on payment status.

But unless your technology is deployed with strict security and access control in mind, you could expose highly sensitive data. Security represents one of the top priorities to selecting an approach to P2P deployment. After all, you may be handling tens of thousands of transactions per day exchanging information from thousands of suppliers.

Security, however, isn't a singular one-time deployment issue. Indeed, it is an ongoing process because the security landscape is constantly changing. Hackers and criminals continuously develop new tools to break into systems once considered "secure."

Even the largest organization are not immune to security threats, illustrating that security must be addressed on an ongoing basis when using P2P solutions and supplier portals.

For example, in 2013 alone[1]:

- Retail chain Target faced the compromise of more than 100 million customer payment cards in a data breach during the Thanksgiving shopping period.
- Adobe experienced the theft of nearly 3 million encrypted credit card records, plus login data for an unknown number of user accounts.
- A cyber-attack at JP Morgan Chase compromised the personal information of nearly 500,000 clients who held prepaid cash cards issued by the bank.

Incidents like these – faced by S&P 500 companies – show that even the largest organization are not immune to security threats, illustrating that security must be addressed on an ongoing basis when using P2P solutions and supplier portals.

DEPLOYING P2P TECHNOLOGY

Three IT Approaches

Various approaches are often considered when IT teams are called on to deploy complex P2P applications. Three of these include in-house, cloud-based, and privately hosted solutions. Each has varying implications for maintaining security and managing access control.

1) IN-HOUSE DEPLOYMENT

When technology is deployed in-house, your internal IT team takes responsibility for designing and building your P2P solution and building your supplier portals. Or your IT staff may choose to purchase and install a vendor's existing application.

With this approach, your in-house technology staff takes full responsibility for not only installing and managing the application and platform, but also

[1]Sources: http://www.networkworld.com/article/2286787/4g/135100-The-worst-data-breach-incidents-of-2013.html and http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/

constantly monitoring it for emerging security threats and quickly taking steps to mitigate those threats. These responsibilities can place a significant burden on your IT personnel – especially if they're managing dozens of other applications for your company.

In addition, an in-house deployment means that IT personnel and possibly others can log in behind your firewall and gain access to your main ERP application, such as SAP.

Implications

When deploying a P2P application in-house, your IT team will need to:

- Continuously monitor – on a daily basis – new emerging security risks, including zero-day threats that require immediate attention
- Cope with security exploits such as "heartbleed," vulnerabilities which can strike without warning and require quick security patches
- Monitor exposure to multiple vectors for intrusion
- Assure that access to your most trusted systems is restricted solely to authorized users
- Likely add personnel, which increases your overall costs and reduces the ROI of your P2P and supplier portal solution

It is important to continuously monitor – on a daily basis – new emerging security risks, including zero-day threats that require immediate attention.

ANALOGY: Consider that you're launching a new business selling customized smartphones. The in-house deployment approach resembles selling these devices from your home. You're inviting anyone in to your home, which presents significant risk of theft and potential damage.

At one time, in-house solutions were the norm, but risks such as those noted above are some the reasons why many companies have migrated away from this approach.

2) CLOUD-BASED APPLICATIONS

Given the cost and complexity of managing an in-house P2P and supplier portal solution, some companies choose to deploy these applications "in the cloud."

This approach requires hiring a cloud provider, a company which supplies you with an "instance" of a virtual machine running in their datacenter and network connectivity to that instance. You do, however, maintain control and can configure the operating system and all your software as you wish.

With cloud-based applications, it is importnat to insure that the solution is configured properly to avoid security vulnerabilities.

Although many applications are deployed on cloud platforms, it's important to note that another company owns and operates all the hardware and networking needed to host your applications. Security issues can still present risk if you leave vulnerable ports open or poorly configure the system.

Other problems that may surface include the process of resolving technology issues, including security and other matters because cloud providers may not respond quickly enough to help you resolve these issues.

Communication between you and your cloud provider may become even more complex because some issues can only be resolved by the cloud provider – and there may not be any specific service level agreement that covers response within a pre-defined timeframe.

Implications

A cloud-based P2P and suppler portal solution requires being aware of certain issues that can impact both security and application performance:

- The same physical hardware running your application may serve other companies with applications that adopt different security stances
- Your cloud provider takes responsibility for managing virtual instances
- Some applications shared on your server may be alluring targets for hackers without your knowledge. Sites on your server may include nefarious businesses, such as those that trade Bitcoins, sell online pharmaceuticals, or worse
- Your IT team still must remain current on new and emerging threats and vulnerabilities and ensure appropriate patches are quickly deployed via your cloud provider
- Lack of transparency or recourse when you depend on a cloud provider to address problems or security issues in a timely manner

Some applications shared on cloud-based servers may be alluring targets for hackers.

This second option offers benefits over the in-house approach, but you should ask who owns the cloud-based service provider's hardware and how quickly that provider can respond to emerging cloud-based security threats. Lack of rigid controls in this area can be costly.

ANALOGY: You move your new business selling customized smartphones from your home to a local mall. But what about other tenants that also occupy that mall? These tenants essentially share your infrastructure. The walls between stores may be weak. And the landlord still holds master keys to all the stores, keys which may be stolen or misused.

Finally, the third approach – a privately hosted SaaS solution – provides the most secure option and mitigates these security risks.

3) PRIVATELY HOSTED SaaS SOLUTIONS

A third approach to implementing your P2P and supplier portal solution would be to run the application on a privately hosted platform. Through this approach, you have far more control over who can access your data so you can maintain full confidentiality.

The application provider takes responsibility for not only installing and hosting the application, but also managing the platform – delivering your software as a service (SaaS).

Through this approach, security is based on "layers." This protects the infrastructure and your data against security threats. And the application provider can more easily monitor for new threats and vulnerabilities – on a daily basis – and rapidly apply patches to protect against these threats.

Implications

With a privately-hosted SaaS solution, your application provider can:

- Completely control the firewall and the operating system
- Isolate the data infrastructure
- Offer a more flexible architecture and design

- Maintain complete visibility on where data is stored
- Offer one point of contact to address any issues, including security and others
- Eliminate the risk of sharing servers with other unknown applications
- Assure that no unknown entities have “keys” to access data
- Prevent logging in “behind the firewall” where sensitive data is stored
- More efficiently manage your applications

ANALOGY: Now you move your smartphone business out of that mall and buy a free-standing building. There’s no sharing of walls between stores. You maintain all keys, essentially owning your own infrastructure with no shared tenants. You have more control over access, and can hire personnel you know to control shelving, inventory, and other aspects of your retail business.

When application providers manage both the application and the platform, you can enjoy added reassurance that extends beyond the an in-house or cloud-based approach.

When application providers manage both the application and the platform, you can enjoy added reassurance that extends beyond the an in-house or cloud-based approach.

PROTECTING SENSITIVE DATA

Secure Application Deployment

Although the SaaS approach represents a more secure way to deploy critical P2P and supplier portal applications, there are still security issues to consider. At Direct Commerce, our security is built around multiple “layers” so that different security solutions are woven together for added resiliency.

These layers include protecting infrastructure, platform, software, and management, among others. If one layer is breached other layers can protect your critical data. Direct Commerce also maintains security best practices that include regular third-party security reviews, employee background checks, and ongoing employee training.

And, of course, we constantly monitor the security environment, always on the lookout for new attack vectors so we can take quick and immediate action.

Yes, the stakes are high – especially when dealing highly sensitive invoice, payment, purchase order, and other financial data through supplier portals – but our security best practices mitigate these risks. That gives our clients the peace of mind of knowing they can take advantage of the many benefits of P2P applications and supplier portals with no concerns over access control and security issues.

A TRUSTED PARTNER

About Direct Commerce

Direct Commerce was founded in 1999 to make it easier to do business through intuitive, effective tools that automate supplier communities.

Today, Direct Commerce is a trusted partner to many Fortune 1000 customers such as Eli Lilly, The Home Depot, and Merck & Company. Our products, deployed on a privately hosted platform, offer intuitive and efficient solutions that give suppliers visibility to answer their own questions – saving clients millions of dollars while helping them achieve a purely paper-free work environment.

Our secure web-based suite of products are architected, installed and managed by an agile, experienced team of professionals that acts as a dedicated extension of your internal team. We pride ourselves on our fast and well-coordinated deployments, delivering exceptional customer service, and creating easy-to-use solutions to help you reach your full potential.

Easy-to-Use P2P Solutions

To learn more about how Direct Commerce solutions can optimize your discount management and P2P automation, visit **directcommerce.com**, email **info@directcommerce.com**, or call (415) 288-9701.

direct commerce