Three Key Areas of Cloud Security for Manufacturers

by Rob Janssens

Senior Manager of Process and Compliance, QAD

A QAD Leadership White Paper for the Global Manufacturing Industry

CONTENTS

THREE KEY AREAS OF CLOUD SECURITY FOR MANUFACTURERS

USING THE CLOUD TO ADDRESS INFORMATION SECURITY

2017 proved, to the consternation of countless organizations around the world[1], including manufacturers[2.3.4], that hackers had become more sophisticated. The depth and breadth of impact from information security breaches on operations, on the supply chain, on financial results and on brand was unprecedented.

Thus far in 2018, there is nothing on the horizon that suggests that the menacing information security threat environment will soon grow safer. Every company is under pressure, therefore, to develop a responsible information security strategy, execute on the strategy diligently and adapt the strategy as needed. Companies cannot resolve all their information security threats. Successful companies, in terms of preventing information security breaches:

1. Accept the evolving nature of the threat environment
2. Make an appropriate level of commitment to develop people and processes to effectively defend, remediate and mitigate information security risk
3. Work with partners that take security seriously.

Many manufacturers find that running applications in clouds offer a safer and lower cost alternative to trying to use in-house resources to keep up with the ever changing threat environment. Not all cloud providers, however, offer the same level of expertise and capabilities in terms of information security. Manufacturers should choose their cloud providers wisely in terms of information security and there is a long list of criteria to consider when making such decisions. Within that long list of criteria, however, there are a few information security areas of particular importance to manufacturers. This paper addresses the following questions regarding information security in the manufacturing sector:

- Why is cloud a compelling choice for companies to consider given the current threat environment?
- What are some of the key criteria for choosing a cloud provider from an information security perspective?
- What are three critical areas of cloud information security for manufacturers?

CLOUD NOW A SAFER HAVEN FOR MANUFACTURERS

The cloud is two decades old. Cloud providers have had a long time to improve security tools, practices and processes. Cloud providers, aware of buyers' security concerns, have invested heavily in security.

In addition, cloud providers are in the business of serving many clients – a compromised cloud can infect many or all customers. Therefore, security is central to the success or failure of a cloud provider. Cloud providers, arguably, are the most motivated of businesses to try to keep a step ahead of hackers and, if they fall a step behind, are motivated to excel at minimizing the damage.

Given the ever-evolving sophistication of hackers, security-conscious cloud providers now offer

a safer environment at a lower cost than most on-premise environments. Cloud providers with a deep commitment to security have the scale to make investing in security expertise, programs, processes and tools pay off for all concerned.

Some cloud providers can help manufacturers in areas of specific concern, such as intellectual property (IP) theft.[5] For example, cloud providers that span the stack in terms of security – infrastructure, application platform and application – like some cloud ERP providers, may successfully prevent SQL injection attacks which are a common technique for IP theft and compromising critical data.

CRITERIA FOR CLOUD SECURITY CONSIDERATION

Here is a partial criteria list that manufacturers can use when considering cloud ERP providers from an information security perspective:

- **Responsible Patching:** Cloud providers should apply patches on a timely basis to reduce the likelihood of breach. Many breaches take place simply because security patches from software providers were not applied on a timely basis.
- **Penetration/Intrusion Testing:** It does not make sense to wait until an attack happens to find out if defenses are strong enough. Cloud providers should operate a program to test defenses on a regular basis.
- **Incident Response:** Even with diligence, manufactures should assume that sooner or later there will be a breach. The sooner a dedicated team with dedicated processes detects the breach and initiates remediation, the lower the costs and impact.
- **Application Familiarity:** A cloud security and management team deeply familiar with the applications a manufacturer uses often provides superior security than, for example, a managed service provider without the application familiarity. Cloud providers that understand the interdependencies between infrastructures, platform, app and configurations settings from a security and management perspective usually does a better job.
- **Certifications:** A cloud/application practice that maintains all appropriate security certifications, and can share the applicable certifications, is underscoring its ongoing commitment to ongoing security and compliance.
- **Teamwork:** Look for a cloud ERP team that will work with the manufacturer's security professionals to ensure that the manufacturer's self-directed policies and compliance requirements are understood and met by the cloud ERP provider.

There are naturally other security needs unique to manufacturers. For example, trends like the Internet-of-Things (IoT), value chain collaboration and information sharing like blockchain and cloud-based supplier relationship management will continue to raise the stakes on information security in manufacturing.

THREE KEY AREAS OF INFORMATION SECURITY FOR MANUFACTURERS

Some companies feel overwhelmed by the many complexities of information security. While indeed information security is a complex subject, there are three areas that manufacturers, along with their cloud providers, should concentrate on first. Those three areas are list below. Some of QAD's relevant practices are discussed, as applicable, to provide illustrations of best practices.

THREE KEY AREAS OF CLOUD SECURITY FOR MANUFACTURERS

1. Access Control

Access control provides a user who has a valid identity and who has authorized rights and/or privileges, to access and perform functions using information systems, applications, programs, or files. The challenge today is that there are so many devices, computers, data sources and apps, it is difficult to develop a comprehensive approach to access control.

QAD offers a comprehensive access control strategy whereby QAD and customers' users only have access to the network and network services that they have been specifically authorized to use, all based on least privileged principles. Access is controlled by secure log-on procedures and restricted in accordance with access control policies.

Provisioning user access (e.g., employees, contractors, customers, business partners and/or supplier relationships) to cloud infrastructure, platform, applications and network components is authorized by the customer's management prior to granting access. Access may be restricted per established policies and procedures. This also applies to timely de-provisioning (revocation or modification) of user access. Quarterly user access review is performed, including weekly review of move/add changes.

2. Vulnerability Management

Cloud providers should use vulnerability assessment tools and best practices that accommodate virtualization technologies, which are fundamental technologies for clouds. Such tools are capable of scanning physical *and* virtual environments.

Furthermore, policies and procedures should be established regarding vulnerability testing, along with supporting processes and technical measures. QAD uses such tools and techniques for timely detection of vulnerabilities within QAD Cloud applications, infrastructure network and system components. This includes, for example, network vulnerability assessments and penetration tests to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities is also used.

Dashboard and metrics supporting the vulnerability management efforts provide ongoing insight. Cloud providers should also continuously look to increase automation in this context to reduce the possibility of tampering or human error. Formal change management processes, in combination with SDLC (systems development life cycle) practices are used for all patches and configuration changes, further contributing to the reduction in vulnerability.

3. Governance and Risk Management Baseline Requirements

Cloud providers should establish baseline security requirements for physical and/or virtual applications, related infrastructure and network components. Those requirements should align with applicable legal, statutory and regulatory compliance obligations.

Deviations from standard baseline configurations must be properly authorized and should follow change management policies and procedures prior to deployment, provisioning or use. Compliance with security baseline requirements should be reassessed regularly.

In addition, cloud providers should establish a formal risk assessment process used in conjunction with any changes to related information systems and to determine the likelihood and impact of all identified risks. Both qualitative and quantitative methods should be used. All risk categories should be considered, for example, audit results, threat and vulnerability analysis, and regulatory compliance. This helps ensure risks are mitigated and that acceptance

levels based on risk criteria are established and documented in accordance with reasonable resolution time frames and stakeholder approval.

For example, QAD Cloud made sure to implement and maintain a comprehensive security management system certified to meet internationally recognized data security standards like ISO 27001 and CSA STAR. This is a most effective way of reducing cloud computing risk. Meeting standards is not a one-time occurrence and may require meeting standards as they change. For example, QAD has established high maturity standards recognized by CSA STAR Level 2 Certification, attesting to its security controls and processes.

SUMMARY: USE CLOUD PROVIDERS THAT MAKE INFORMATION SECURITY A TOP PRIORITY

One option open to manufacturers to reduce the cost and impact of the scary information security threat environment is to deploy key applications, like ERP, with cloud providers that excel at information and show a deep ongoing commitment. But how do you choose?

While there is a long criteria list for manufacturers to build and consider, a list that uniquely reflects company-specific security needs on a variety of fronts, there are 3 key areas to focus on when looking at cloud providers.

Does your cloud provider address access control holistically – across all users, all kind of devices, all networks, all systems and applicable applications? Does your cloud provider run a comprehensive vulnerability management practice that includes the change control, analytics-based insights and an adaptive risk-based model to stay on top of new vulnerabilities as they emerge? Does your cloud provider identify standards tied to industry and regulatory requirements? Is there an ongoing risk assessment process for new and updated systems? Is there a commitment to continually meet standards as they evolve?

Cloud has come a long way in terms of information security. Different cloud providers, however, have progressed at different rates in terms of cybersecurity. Manufacturers need to ensure that cloud providers supply a breadth of capabilities and commitments for information security. Manufacturers need to ensure that their cloud providers perform particularly well in the most critical areas of information security like access control, threat management, risk management processes and certifications.

Your Strategic Assessment: To find out how you can obtain an assessment that clarifies where you stand today on cloud security, contact a client advisor at QAD. With a full decade live in production, QAD Cloud ERP has an excellent track record of availability, performance, security and rapid, successful implementations.

Sources

[1] 2017's biggest hacks, leaks, and data breaches — so far, ZDNet, September 20, 2017

[2]Honda Halts Car Production After WannaCry Infection, by Maritza Santillan, Tripwire: The State of Security, June 21, 2017

[3]LG Shut down due to Wannacry attack on its systems, by Ayobamidele Francis Mo bee, Digital Space Radio, August 23, 2017

[4]Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk by Danny Palmer, ZDNet, August 16, 2017

[5]Security trends in the manufacturing industry: Intellectual property and operating information are the crown jewels, IBM X-Force® Research, 2017

QAD Inc.
100 Innovation Place
Santa Barbara, CA
93108 USA
Tel: + 1 805 566 6100
www.qad.com