KINAXIS®

YOUR GUIDE TO SUPPLY CHAIN DATA SECURITY

Table of contents

MAKING DATA SECURITY A PRIORITY

Your supply chain is only as strong as its weakest link.

of all data breaches originate from within the supply chain

The old adage is true. Your supply chain is only as strong as its weakest link. Unfortunately, that also holds true when it comes to the security of data within your supply chain. An estimated 80% of all data breaches originate from within the supply chain.[1] And the impact of one of those breaches is monumental.

Target Corporation, one of the largest retailers in the United States, suffered a massive data breach in late 2013 after a cyber intruder stole information on more than 40 million credit and debit card accounts through malware installed on Target's point-of-sale system. The attack also compromised the personal information of up to 70 million customers, including names, mailing addresses, phone numbers and email addresses. The cost to the company was more than $88 million.[2]

Cyberattacks like these are the number one threat to many organizations and their supply chains.[3] But shoring up security within your digital walls isn't enough. For Target, the data breach came through one of its vendors.[4]

"Companies in almost every industry are more reliant than ever upon their vendors, and particularly those in their supply chain. The demand for constant online communication creates enormous opportunities for hackers to exploit weak vendor security practices as a point of entry into their ultimate target," said Steve Bridges, senior vice president at JLT Specialty, an insurance broker specializing in cyber insurance.[5]

While cyberattacks aimed at stealing data remain the most visible risk, attacks designed to deny or disrupt service are also gaining in popularity. These types of cyberattacks jeopardize production and delivery schedules, causing delays and negatively affecting customers. Nodes along the entire supply chain can feel the impact.

Whenever, wherever or whoever accesses your supply chain information, it's vital to make your data safe, secure and only accessible by those who should have access. Data security in your supply chain is a team effort. The good news is, there are ways to protect your supply chain data. It all starts with proactivity. Don't wait for an attack to happen. Take steps today to ensure your data stays safe.

USER ACCESS

Does every end user need full visibility into all areas? Probably not.

- ☑ You should encrypt all passwords and the system should only store them using secure means like a one-way hash based on a PBKDF2 (password-based key derivation).
- ☑ Sign-in information should be transmitted securely using HTTPS/TLS encryption.
- ☑ Users should connect with their appropriate data instances through non-persistent session cookies and you should encrypt all transmitted data using transport layer security (TLS).

Restricting access

One of the primary ways to ensure data security in your supply chain is recognizing and restricting who has access. Does every end user need full visibility into all areas? The answer is probably not. Access to your most sensitive information should be on a need-to-know basis. Choose which employees can see and interact with specific information by customizing their read and write data access. For those with larger user bases, the most efficient way of limiting user access may be through a hierarchical, role-based user/group model to control viewing and editing privileges. Always ensure you work with vendors who support SAML/Single Sign On.

By controlling the user experience, you can limit what a user can see or do in your data system, ensuring they only have access to select data. Don't forget, this type of restricted access extends beyond your walls. You need to hold suppliers, customers and third-party service providers with access to your data systems to the same restrictions and accountability as your own team.

Password policies

Implementing strong password and encryption policies is critical to keeping your supply chain data safe. By creating security protocols involving company ID, user ID and passwords to authenticate user identity, you can minimize the risk of unauthorized access to sensitive supply chain data. Make sure your data systems avoid unwanted visitors by implementing parameters to help make your system more secure, including:

- ☐ User lockouts after a specified number of sign-in attempts
- ☐ Automatic password expiry (force a password change after a specified number of days)
- ☐ Minimum password length
- ☐ Minimum password complexity
- ☐ Password re-use exclusions

Monitoring sign-in activities

Since unwanted cyber visitors rarely check in at reception, it's critical you take the necessary steps to monitor for their presence. You should track and review information about sign-in activity on all your systems, watching for unusual activity or non-authorized access. It becomes especially important if external users, like customers or suppliers, can access any of your data storage systems.

The sign-in activities of users can potentially alert you to possible sign-in attempts by unauthorized users. For example, you can look for multiple failed sign-in attempts or sign-ins by users you know are away and unable to access the system.

It's critical your team, both internal and external, know the risks of a breach.

Security training

You're only as secure as your weakest link. That statement bears repeating. When it comes to data security, user education is key. It's critical your team, both internal and external, know the risks of a breach. You should properly educate everyone in your organization on how to spot malicious attacks, including phishing attempts. This minimizes the risk of unauthorized third parties attempting to steal account information or sensitive data. As the techniques and technologies of cyber criminals change frequently, regular security training is a must. Yearly sessions aren't enough to keep your company safe. Quarterly, or even monthly, are the best way to continually remind users of the ongoing threat of cyberattacks.

Internal fraud protection

While no one likes to think of their own employees as willing partners to cyber espionage, it can and does happen. That's why you should have the following policies and procedures in place to protect against internal fraud:

- Ensure employees sign and adhere to a code of conduct, including a non-disclosure agreement to protect the confidentiality of information and data
- Restrict access to the hosting environment, (both physical and network), to only those who require it
- Deny staff from third-party service providers access to user passwords
- Conduct regular monitoring of system logs
- Perform internal security reviews on a regular basis

Physical security

Whether you've outsourced your data center requirements or kept them in-house, physical security and environmental controls are just as important as firewalls and malware detection. Here are some security protocols you (or the location where you house your data) should have in place:

- Monitor your facility access via video surveillance and on-site personnel
- Include at least one biometric screening as part of your security protocol
- Limit access to your data center to authorized personnel based on job function
- Review physical security access permissions quarterly to prevent unwanted visitors who could potentially gain access to any on-site data servers or enter your network through a connected device

Whether you've outsourced your data center requirements or kept them in-house, physical security and environmental controls are just as important as firewalls and malware detection.

Your data center facility, whether on-site or off premises, should be monitored by a command center 24 hours a day, seven days a week. Critical conditions should result in the generation of an automated alert, triggering immediate human engagement.

Physical security also extends beyond just restricting access through the front door. It includes the safety of the equipment storing your data. Utilize backup generators, fire detection and suppression systems, air conditioning systems, environmental monitoring and alert notification systems to prevent hardware malfunction or destruction. Have a solid backup plan in case an issue does arise.

MONITORING AND AUDITING

Knowing what's usual and what isn't is the foundation your supply chain data security stands on.

The best way to understand and detect potential security issues within your supply chain data is through accurate monitoring and auditing. Knowing what's usual and what isn't is the foundation your supply chain data security stands on. Comprehensive monitoring involves complete data change tracking in all supply chain systems, including user names and timestamps, for future reference.

Monitoring should also encompass key security controls of your supply chain data systems and the corresponding performance of routine security audits. Your audits should include logging of the following types of changes:

- System configuration changes
- User changes
- Group changes
- Permission changes
- Resource dependency changes
- Profile variable changes

Make sure you also regularly review server access, network access, firewall traffic, intrusion detection, system backup, FTP data traffic, system utilization and all other application logs.

If the systems allow, setting up automated alerts for specific events can make your supply chain data security monitoring faster and easier. You'll know sooner when something out of the ordinary occurs, so you can act faster to get the situation under control.

SYSTEM INFRASTRUCTURE

Security should be top of mind when developing your supply chain infrastructure.

Protect your supply chain data with a layered defense methodology that has all traffic traverse multiple firewalls, intrusion detection and prevention technology and gateway servers. Security should be top of mind when developing your supply chain infrastructure. Be sure to house your data in a safe and secure environment. That could be on a unique and dedicated environment or a shared database that uses specific customer metadata and encryption keys to protect your company's private information.

When it comes to accessing your network, your internet service provider's hosting centers need to be highly reliable, scalable and have high-performance connectivity to the internet.

If you use a web client to access any of your supply chain data, ensure communication between the web client and your data server is through a combination of web service (SOAP/REST) and HTML over a secure HTTPS connection.

DATA SECURITY AND CONFIDENTIALITY

Define data classifications and set security parameters ensuring you handle each type accordingly. Not everyone needs access to every type of data, especially when it comes to financial information. Anyone requiring access to your data should sign a non-disclosure agreement. Spell out confidentiality obligations regarding your data or that of your customers and suppliers.

All data transfer services should use encryption, preferably the SFTP (SSH) protocol, with data transferred directly to your data server, never touching down outside the firewall architecture. A secure implementation protects and ensures the integrity of your company's data.

A secure implementation protects and ensures the integrity of your company's data.

Network devices, server hardware, services, performance counters and most application processes should be monitored using dedicated monitoring software. As should service accessibility and general responsiveness.

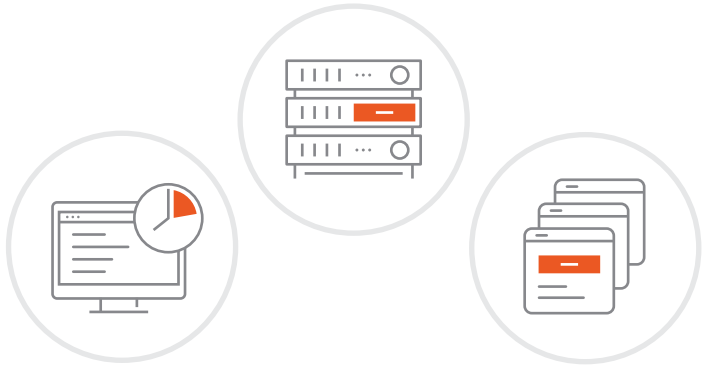
Manage remote systems using VPN technology. Approve access to the data hosting facilities at the director level and limit it to designated personnel only. Don't forget to perform any remote admin activities over a secure VPN access from secure machines.

INCIDENT REPORTING

If you find yourself the victim of a data security breach, it's important to have a solid plan in place.

If the unthinkable does happen and you find yourself the victim of a data security breach, it's important to have a solid plan in place. Develop an escalation chain, usually beginning with a service analyst and moving upward to IT directors and beyond.

Enabling third-party security incident and event management for continuous log review and threat detection can help spot network vulnerabilities before they're breached. Schedule automated scanning for regular intervals. Service operation manuals and corporate policy documentation should be readily available.



Server outages

Track data server outages and regularly review the reports generated by your tracking system.

You should also have clear escalation plans in case of data server outages because they can be just as detrimental to your supply chain as a data breach. In the event of an outage, alter the appropriate personnel and move the issue up the chain of command to the director level or higher, if appropriate.

Data backup

Leverage backup technology to ensure you can quickly recover and restore data in the event of a data server outage, or worse, a hacker attack that wipes your network. A good rule of thumb is to back up your data at least once every 24 hours, retaining that copy for at least 30 days. Performing monthly backups, and keeping them for at least a year, is another good safeguard.

Set minimum recovery times and recovery point objectives that align with the business classification of data protection and ensure your service provider can meet or exceed them. It's best to have a data recovery point every 24 hours and the ability to get your data back up and running in the same timeframe. Your production site recovery methodology should include geographically diverse alternate data centers. That way, in case of an emergency – hacker related or not – you'll have a data copy that's still relatively up to date.

A good rule of thumb is to back up your data at least once every 24 hours, retaining that copy for at least 30 days.

Remote replicate (disk to disk) all encrypted production backup files across your alternate sites. It will help re-image your virtual machines with production information, restoring production service faster. Review and test your recovery plan on an annual basis to make sure things run smoothly.

Reviewing system utilization and application logs routinely may help catch and reverse errors. Quarterly service health check reports should include:

- Service level agreement performance
- Response time performance
- Average weekly user load
- Data integrity
- Top accessed resources
- Number of reports generated (user initiated/alert initiated)

PROACTIVE PREVENTION

In the cyber world, things change quickly, so you need to as well.

Proactivity is your best line of data defense. Restrict access to only those who need it. Monitor and track all activity. Have a solid action plan in place. And don't forget that in the cyber world, things change quickly, so you need to as well.

Stay abreast of current threats and trends, and make sure everyone involved in your supply chain, from users to suppliers to customers, adopts the same approach.

While your supply chain and its associated data may only be as strong as its weakest link, putting strict security measures in place makes all the difference. Don't fall victim to a cyberattack, data breach or intrusion.

Protect your data as if it's your most valuable asset, because in the end, it may just be.

SECURITY CHECKLIST

Looking for a cheat sheet to make sure your supply chain data is as safe and secure as possible? Our handy data security checklist will answer a few vital questions about your data. It provides a starting point for the conversation about how your company handles data security.

- ☑ **Is data restricted to only those who need access to it?**
- ☑ **Are corporate password policies secure enough? Are they enforced?**
- ☑ **Is sign-in activity monitored?**
- ☑ **Does your staff receive regular security training?**
- ☑ **Where does your hardware reside and who has access?**
- ☑ **How is physical access granted and revoked?**
- ☑ **Are user actions tracked and audited?**
- ☑ **Do you have a comprehensive incident response plan?**
- ☑ **How is data backed up?**
- ☑ **Do you routinely evaluate your security policies and procedures?**

Kinaxis provides data security peace of mind

Keeping customer data safe is a top priority for Kinaxis®. That's why we use the most advanced technology for internet security. Whenever or wherever you access your supply chain information, all communication is encrypted. Your data is safe, secure and only available to those you want to see it.

We have security personnel onsite 24 hours a day, seven days a week, visitor screening and keyless security with biometrics to prevent unauthorized access to any of our hardware, including data servers and corporate machines.

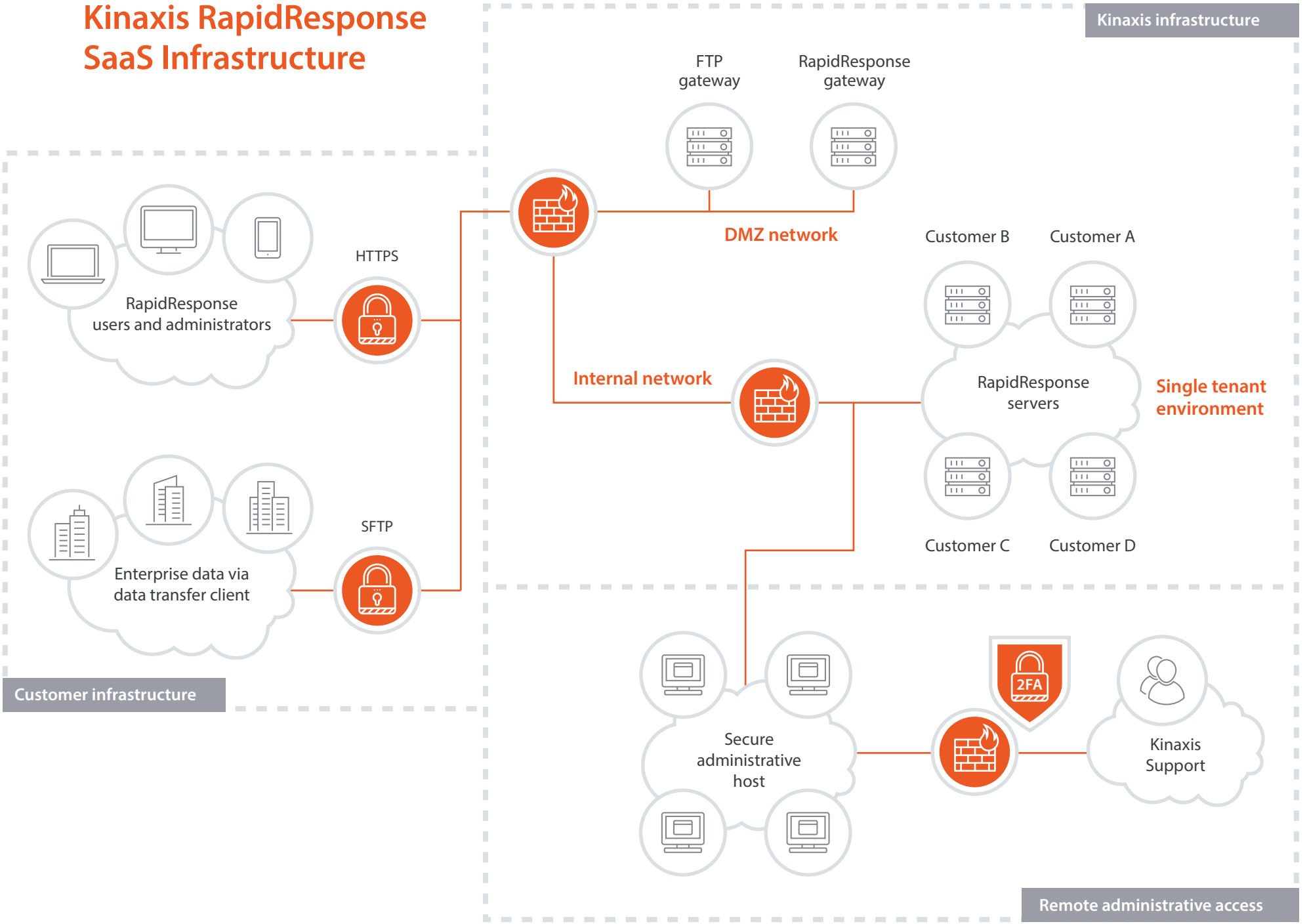
Included with our revolutionary supply chain management software, Kinaxis RapidResponse®, is a complete suite of security features with fully automated intrusion prevention and detection and data transmission encryption. Remote admin access is firewall controlled.

Our formal data security practices and policies have strict management oversight to ensure controlled access to customer data. Our data centers have complete N+1 infrastructure and data recovery options within a site at the transaction level.

We provide nightly off-site data replication so you can rest assured your data will be available when you need it. Our disaster recovery time objective is less than 24 hours, which minimizes unexpected downtime due to operating or physical server failures.

Our customers are our number one priority and that means keeping your data safe, secure and available so you can focus on managing your supply chain and what matters most to your business. If you're looking to learn more about the data security features of RapidResponse, or Kinaxis' security policies, check out our security brochure.

Kinaxis RapidResponse SaaS Infrastructure



About Kinaxis

Offering the industry's only concurrent planning solution, Kinaxis helps organizations around the world revolutionize supply chain planning. Kinaxis RapidResponse, our cloud-based supply chain management software, connects your data, processes and people into a single harmonious environment. With a consolidated view of the entire supply chain, you can plan expected performance, monitor progress and respond to disconnects when reality hits. RapidResponse lets you know sooner and act faster, leading to reduced decision latency, and improved operational and financial performance. We can prove it. From implementation to expansion, we help our customers with every step of their supply chain journey.

RESOURCES

1. Mello, John P. Jr., Target Fiasco Shines Light on Supply Chain Attacks, TechNewsWorld, February 3, 2014.
2. Ahead of the Curve: Understanding Emerging Risks, Marsh & McLennan Companies, September 2014.
3. Ahead of the Curve: Understanding Emerging Risks.
4. Martyn, Paul, Risky Business: Cybersecurity And Supply Chain Management, Forbes, June 23, 2015.
5. Martyn, Paul, Risky Business: Cybersecurity And Supply Chain Management.