JANUARY 2020

Securing Your Business from Fraud & Theft

zenoti

www.zenoti.com

Table of Contents

IT'S A TOPIC NO ONE LIKES TO TALK ABOUT.

$148

The average cost per lost or stolen record in a data breach is $148.

But take a moment and really think about it: what would happen to your business if security was breached?

Think of everything that would be exposed, like your customers' payment information, their contact information, and their personal records. Massive companies like Marriott, Uber, and Capital One have made the news for mismanaging customer data. Even with their budgets and resources, these major companies struggle with the fallout and have to fight hard to win back their customers' trust.

For mid-sized or small businesses, a data breach could be even more disastrous — it might mean the end of your business altogether.

This document identifies security risks posed to your salon, spa, or medical spa, along with an explanation of Zenoti's built-in safeguards that help you prevent these types of fraud and theft.

Fraud based on software access levels

Your customer, employee and financial data are confidential and represent competitive information. You don't want your front desk staff to have the same software access as your leadership team, but this can be difficult to manage.

Zenoti's security mechanisms give you the ability to assign access to different components of your software based on job role, location, and machine. Zenoti also allows you to restrict certain people from being able to export data or download reports, which helps to keep sensitive customer data secure.

30%

30 percent of companies have over 1,000 sensitive folders open to everyone.

Limit data and functional access based on roles

Each employee is given a unique login, role, and granular level permissions. Roles and permissions give employees access to capabilities and data associated with their job, and restricts access to other data and capabilities in the software.

You can customize permission settings based on roles. For example, create a role for your directors with high levels of access to the system. Create a separate role for your inventory manager that allows access to only the inventory features and reports.

58%

58 percent of data breach victims are small businesses.

Limit access based on center or location

Limit access to the system's capabilities and data by center or zone. For example, grant your receptionist the ability to book appointments only for her single center. Allow a zonal manager access to the system for multiple centers.

Limit access based on machine

Managers often need to access Zenoti outside of their physical location to book appointments, review customer profiles, or review reports. Your receptionists, however, only require access from specific workstations within your center. You control exactly which computers can be used to access Zenoti.

Restrict export of data

Zenoti restricts the ability to export data based on permissions. While your receptionist can access customer profiles when booking appointments (which is important to be able to personalize each interaction), they cannot export a customer list or related data into a spreadsheet. These settings restrict access to non-essential information, which prevents staff from viewing or exporting sensitive data.

"

Ensuring the integrity of your data and systems is of paramount importance in today's software environment. Choose a provider that knows your business and the high-risk areas and ensures your business is protected from threats inside and outside of your organization.

—

Sudheer Koneru
CEO, Zenoti

59%

59% of employees steal proprietary corporate data when they quit or are fired.

Fraud from customers and staff

Although most of your customers and staff are honest, there's a chance your business will, at some point, have to address a problem with fraud or theft. The best way to mitigate fraud from customers or staff is to prevent it with the right software features. Here are some of the ways Zenoti keeps your business safe from malicious users.

Review complete audit trails of deleted appointments

One common example of appointment fraud that we've seen is when a staff member deletes an appointment from the appointment book after the services were performed and then pockets the money.

Zenoti is effective at mitigating this type of theft because it produces a trail that shows when appointments are entered, changed, or deleted. The software then alerts you (via email and text message) of all deleted appointments. Alert settings can be sent to individual or multiple recipients (e.g. managers, admin staff at corporate office).

Because Zenoti is a cloud solution, all appointment cancellations or deletions are stored and monitored remotely, so you can get the most recent information at any time, from anywhere.

Ensure appointments are always booked

Customers who self-book online and through mobile not only save your staff time, but also ensure your appointments are visible in real time in the appointment book. You'll have a record of any modifications made by staff to these appointments.

Trace inventory shrinkage to specific products

Another common form of fraud is inventory shrinkage. Zenoti inventory control allows you to conduct frequent audits that are quick and error-free. Service and retail sales, along with audit information are used to report projected vs. actual expense on inventory. This helps you understand your real cost on shrinkage. You can also drill down to trace shrinkage by category or specific products.

Accounting fraud

Accounting fraud can make you lose out on profits or run into cash flow problems. Whether it's the result of fraud or human error, financial discrepancies are harmful to your business, your culture, and your customers.

100

Billing schemes are ranked as the second most common type of fraud for organizations with fewer than 100 employees.

Get alerts on pricing overrides

You can choose to receive daily alerts when pricing overrides are made during billing. This helps you compare adjustments between centers and ensures identification of price or discount abuse in a timely fashion.

Complete audit trail on deleted invoices

This alert is triggered when an invoice is deleted. As with most alerts, you can set a minimum number that triggers the alert. For example, you may want to be alerted after at least three invoices were deleted.

Alert on guest outstanding report

Alerts are used to notify you when a guest's outstanding balance is too high. This ensures you know when to follow up with guests to collect payments, but also helps you identify any theft issues with your staff (i.e. accepting payments from a customer, but pocketing a portion of the payment and marking the guest's balance as outstanding).

No changes on customer payments

You can lock customer payments so that changes cannot be made after a bill has been printed. For example, if a customer pays for a service and receives her bill, the front desk cannot change the mode of payment later. This prevents staff from redeeming packages or membership credits and pocketing the money. Each bill must be "closed," or it is otherwise reported by the system and you'll be alerted.

In the event there is a genuine need to modify a bill after printing, the front desk is required to recreate the bill and abandon the old bill. It's easy for your team to perform these actions when necessary, but each of these actions is recorded in an audit trail in case you need to investigate.

Fraudulent membership, package, and gift card redemptions

Memberships, packages and gift cards are prepaid tools that are often exploited by guests and staff. Zenoti offers a unique system that ensures only the rightful owner of a membership, package or gift card can redeem value from these items.

Unique PIN code to verify each guest

When the customer attempts to redeem a membership, package or gift card, Zenoti sends a unique PIN to the customer's cell phone. The system requires that PIN to complete the redemption. This method is successfully used in banking for security.

Automated text message on redemption

Automatically (and optionally) send text messages to your guests when memberships, packages or gift cards are redeemed against their account.

Customer visibility to balances

Zenoti offers your customers direct visibility to their membership, package, gift card and loyalty point balances. Balances can be printed on every bill. Customers can also access their own profile information, which includes a history of redemptions and balances via your website and a mobile app.

Automated tracking of partially paid packages redemption

Zenoti supports partial payments on packages and limits redemption on that package up to the value paid. For example, if a customer has paid only $200 of a $1000 package that offers 10 massages, the software allows that customer to redeem up to two massages. The partial package report provides complete insight into partially paid packages including sale date and available balance. This helps you to proactively follow-up with customers who need to make additional payments.

60%

In 60% of cases, attackers are able to compromise an organization within minutes.

Zenoti enables you to effectively manage and protect your business. Risks from fraud and theft to your business are mitigated with a richly layered system, that enables you define how your valuable data is used and alerts you to potential issues that could compromise your operation.

Contact Zenoti for more information.

About Zenoti
Zenoti is the most advanced cloud-based, business software for spas, salons, and medi-spas. Trusted by 5000+ spas and salons across the world.

www.zenoti.com

zenoti

000003