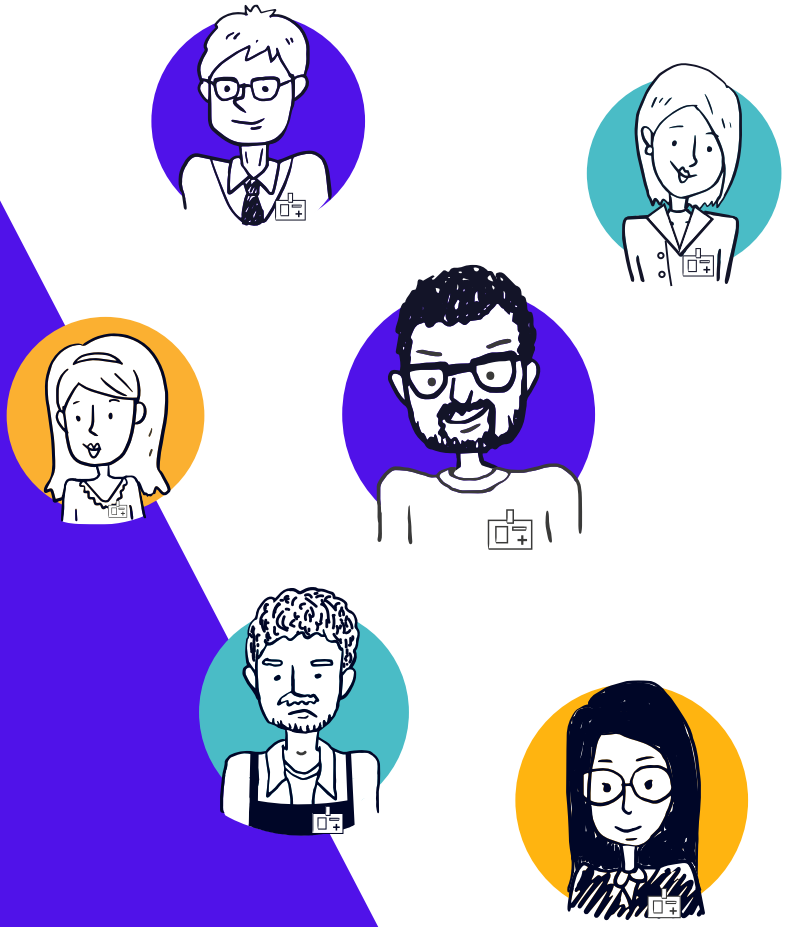
Sycurio.

Faces of healthcare fraud.

Who's infecting your patients' data... and what's the cure?

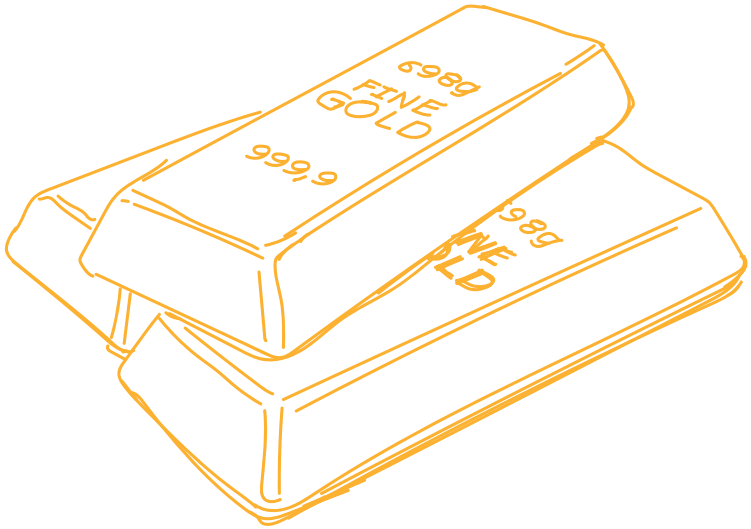


Personal information today is pure gold to fraudsters. Demographic details alone are highly valuable, and more sensitive information, such as payment card numbers, user IDs and passwords, are worth a great deal on the black market. But, what many people don't realize is that healthcare and medical information is perhaps the most valuable of all.

Today, complete medical records currently sell for as much as **$1,000** on the Dark Web. It is no surprise that healthcare call and contact centers are prime targets for fraudsters, who are persistently – and ingeniously – looking for new ways to get their hands on your patients' data.

Breaches in the healthcare industry are reported at a rate of more than one per day in the U.S. alone and there has been a 25% increase in healthcare data breaches year over year. Further, in our **State of Healthcare and Payment Experience and Security survey**, we found that two-thirds of consumers (66%) report they would leave a healthcare provider if their payment or personal information was compromised in a data breach due to the provider's lack of security measures—a signal of the high stakes the industry faces today.

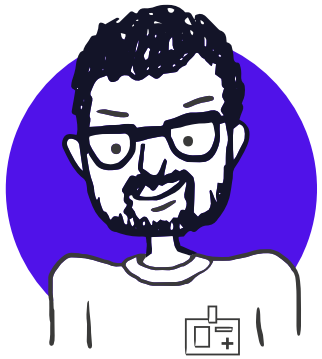
You may think you have sufficient processes in place to protect your contact center and comply with regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and a wide variety of state laws designed for protecting personally identifiable information (PII), but are you confident that you have the right systems, controls and people in place to stay ahead of the fraudsters? And have you given enough thought to insider threats?



Hackers and cybercriminals outside your organization aren't the only ones eyeing sensitive data. Insider threats – which could involve patient service representatives (PSRs) and agents, third parties and other contact center employees – account for 58 percent of healthcare data breaches.

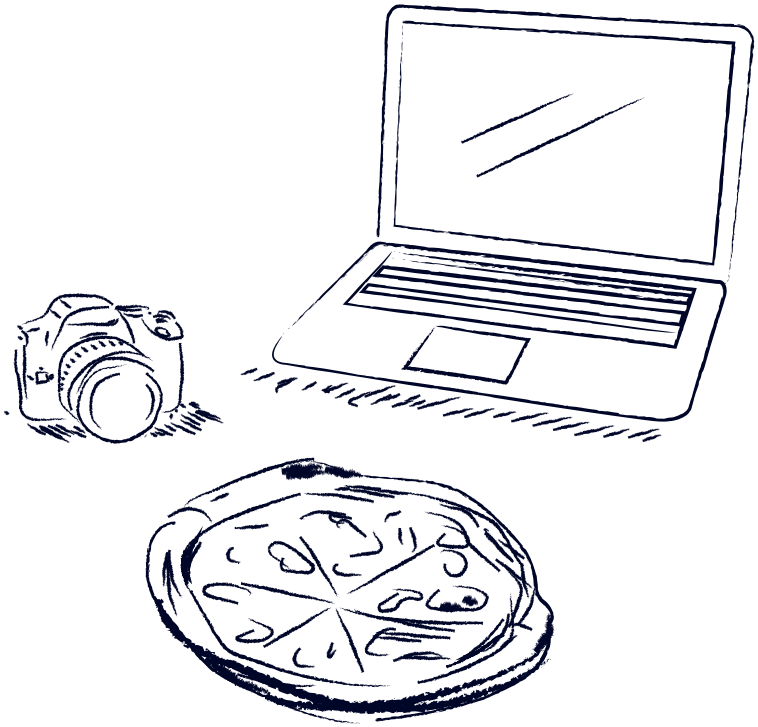
While most patient service agents are diligent, customer-focused and trustworthy, if they are handling sensitive data, they could still pose a risk. Anyone working in your organization may be subject to bribery, threats or trickery. Even honest and well-intentioned employees can fall victim to fraudsters' targeted attacks and nefarious schemes. And if you have temporary staff, your employees are working remotely or use contractors to maintain your facility or IT systems, your security risks are even higher.

Meet Six People Putting Your Contact Center Data at Risk...



Opportunistic Oscar.

The tempted temp



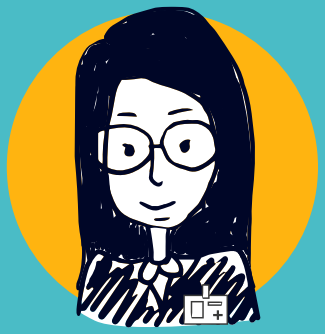
Oscar is one of the many temporary agents assigned to a healthcare provider's billing department. He's a nice guy, but he doesn't overthink things. He's surprised that patients are providing him not only with payment card numbers, but also CVV codes, addresses and more over the phone, as they pay their medical bills. He decides to write down a few patients' credit card numbers.

One afternoon, Oscar treats a group of his contact center colleagues to a delivery of pizzas courtesy of one of the card numbers he's taken. He knows that the credit card company will ultimately pick up the bill if the cardholder disputes the fraudulent charge, so he doesn't feel too guilty. Also, he isn't very worried about getting caught as he's only employed by the contact center for a few weeks while he looks for a full-time job. Oscar's scheme works so well that he uses a different card to buy a camera online the next day, and another to buy a new laptop the day after that.

Unfortunate Ursula.

The credulous clicker

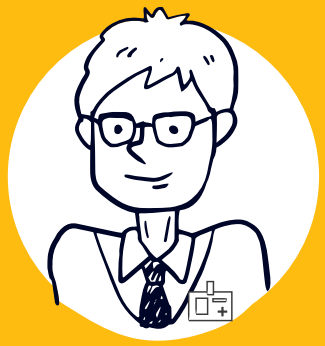
Meanwhile, Ursula, a diligent patient service representative, is busy responding to patient emails, answering questions and facilitating prescription renewal requests. Ursula comes across an email from a patient sharing the results of a recent X-Ray in an attachment, which she opens. Unfortunately, entirely without her knowledge, this installs a malicious worm that spreads throughout not only the contact center's IT network, but the entire healthcare system's network, too. The worm steals patients' data and transmits it to fraudsters operating from the outside.



Disgruntled Daisy.

The vengeful victim

Daisy recently earned her nursing degree and started a new position in the very hospital where she had been working part-time as a patient service representative. However, nursing school left her severely in debt. A few weeks into her new job, Daisy requests time off for her annual family vacation. However, her supervisor denies her request due to a staffing shortage. Feeling unfairly treated and desperate to pay off her student loans, Daisy decides to pay one of her former contact center colleagues $500 to share some patient files with her – some of which contain payment card information. She starts selling this information on the Dark Web, netting a $1,000 profit in the first week alone.
Daisy doesn't go on her vacation, but she does appreciate making swift progress on paying off her debt.



Scheming Steve.

The hidden hacker

Steve is part of an outsourced IT support team and is regularly sent to fix technical problems in a hospital's contact center. Although Steve is an "IT guy" by day, he is a hacker by night – and lists a wide range of compromised PII for sale on the Dark Web. While upgrading the security software on an agent's computer, Steve discreetly introduces a Remote Access Trojan (RAT) into the machine. This little piece of software allows the device to be accessed remotely. From his home computer, Steve can now hack into the contact center's network and access patient accounts, along with all the sensitive data he can find. Should he choose to do so, he could wreak havoc.

Conniving Carl.

The contract cleaner

Carl works part-time cleaning the building that houses the contact center. He has unrestricted access to every floor, every room and every office. Carl is a skilled computer operator and knows how to capture customer information. While cleaning in the contact center one night, he slips tiny USB sticks, which contain keylogging software and a Wi-Fi transmitter, into several computers. Over the next week, the keyloggers capture detailed information of all patient transactions, including their payment card details and social security numbers. The transmitter sends these to the computer of Carl's associate, who is based elsewhere in the building. Carl returns the following week to remove and collect the USBs, which have gone completely unnoticed.

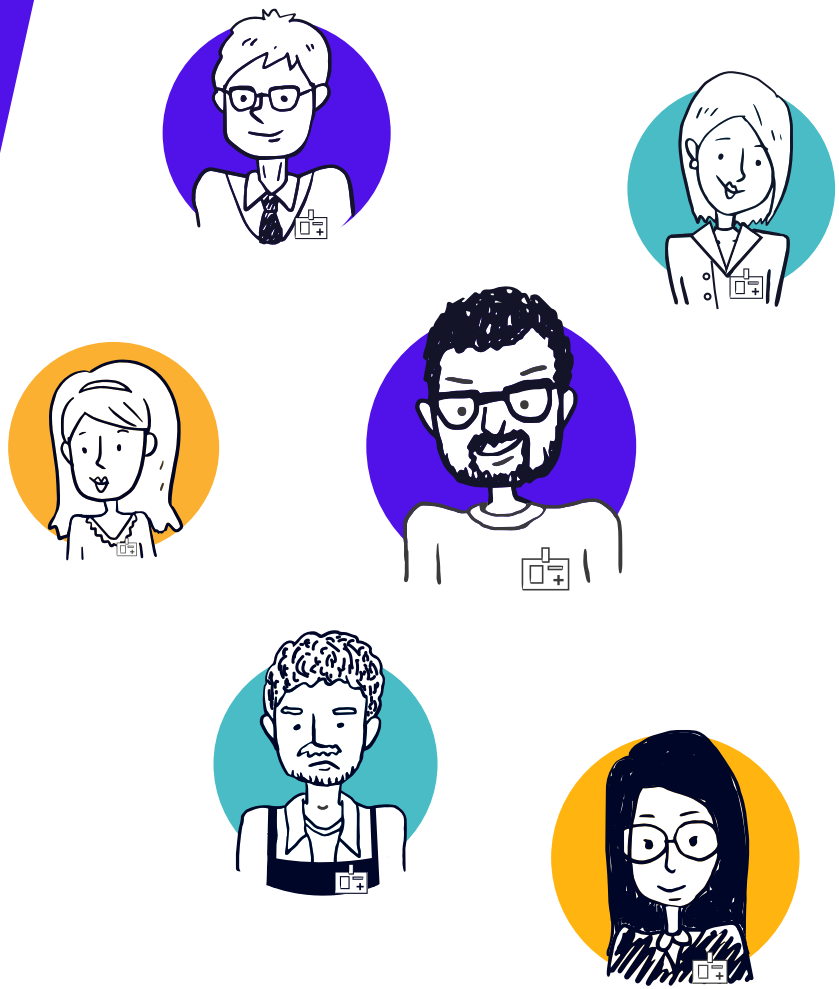
Curious Cate.

The star-struck care rep

Cate is a care rep in a major pharmacy chain's contact center. One afternoon, she overhears a colleague talking about a call from a celebrity, inquiring about a new prescription. Out of sheer curiosity, Cate looks up this celebrity's account information in the pharmacy's system, and is excited to discover his home address, phone number and even billing information. Her curiosity gets the better of her and she looks up her neighbors' and friends' information and peruses their medical history. Cate wonders if the tabloids would be interested in purchasing the information she discovered on the celebrity...

Any one of these six people can bring disaster to your call and contact center. All can compromise your patient data. A data breach could result in your organization paying thousands of dollars in compensation to each affected patient. It could mean crippling fines. Above all, however, it could lead to a ruined reputation that undermines your brand and your organization.

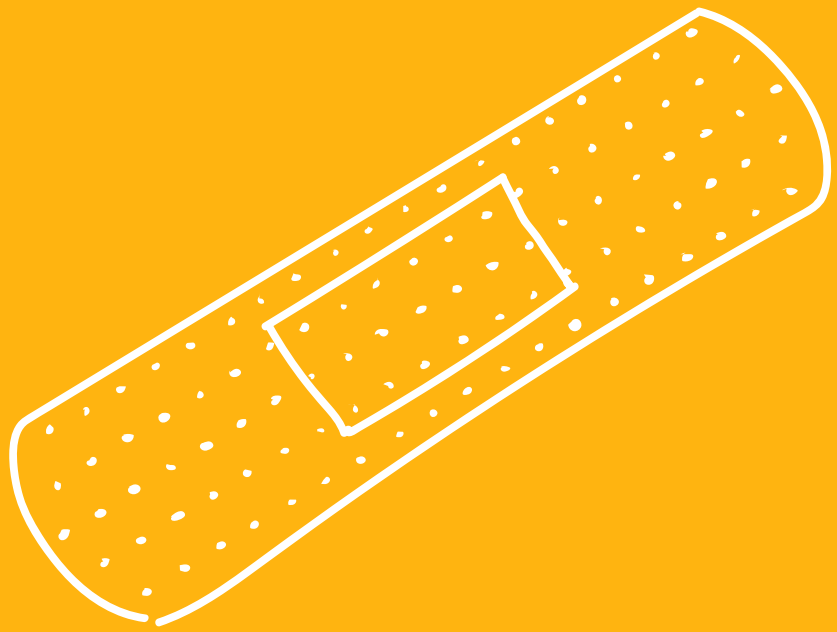
Over access to patient data, coupled with the curious human nature, is surely a recipe for risk. All it takes is one curious employee to “break the glass” and expose sensitive data, violate compliance regulations and put your company in the spotlight for the wrong reasons. And while an agent may not necessarily steal data for fraudulent use, the simple act of accessing patient data without a legitimate reason to do so is a clear violation of HIPAA.



Don’t compromise data security with a quick fix.

At the heart of the problem is your patients’ data security. If you hold sensitive information in your contact center, you can never be 100 percent sure it is safe. In fact, our global survey of over 500 contact center workers found that 72 percent of agents who collect payment card data over the phone are still required to ask customers to read card numbers out loud, which raises the danger levels to red. What’s more, some of the measures that are supposed to help protect sensitive data are making matters worse by lulling contact center managers into a false sense of security.

Fortunately, there are several ways to strengthen data security and protect patient information.

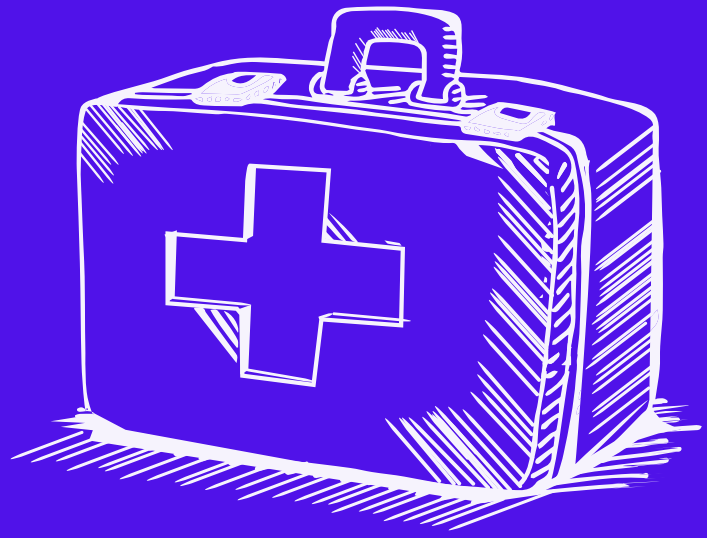


So, what's the answer?

People are fallible, and no organization will ever be able to predict and prevent every potential breach. There are, however, steps you can take to reduce risk and keep patient data safe – starting with your contact center.

1 Implement an incident management policy

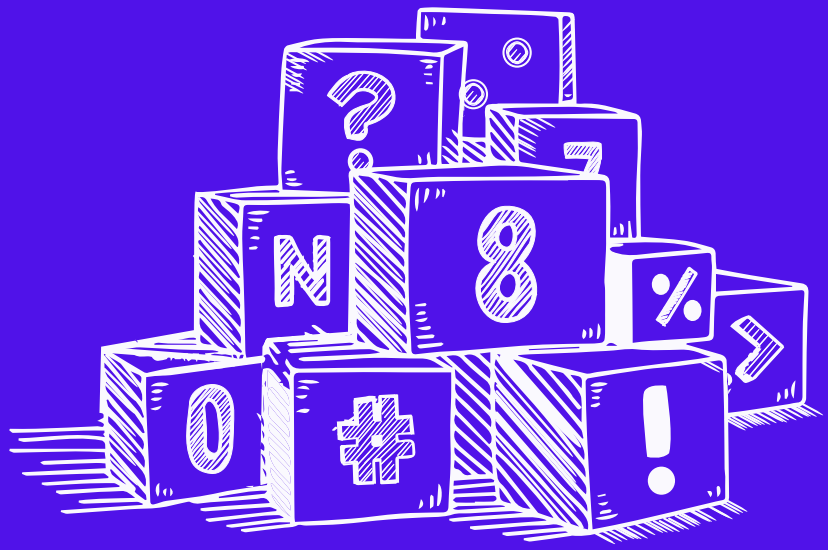
Prepare for a worst-case scenario and have a documented Incident Response Plan (IRP) that is reviewed and tested at least annually.



2

Use tokenization to replace sensitive data

Tokenization replaces data with a meaningless equivalent while it passes through your hands. Even if a breach is successful, the available data will be zero value to the cybercriminal.



3

Enforce the principle of Least privilege – don’t give people more access than they need

The principle of Least Privilege gives employees the minimum level of access necessary for them to do their job. So, if an agent doesn’t need to view customer payment card data when a phone transaction occurs, it should not be exposed to them.

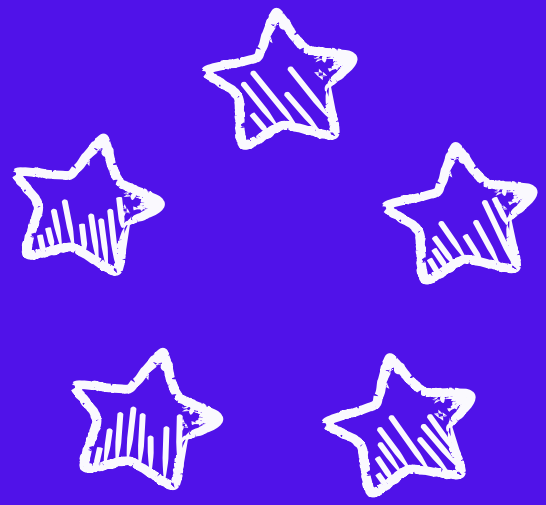
4

Remove customer data from your contact center

When sensitive data is exposed to agents and handled and stored in your IT systems, it's just waiting to be compromised. Your objective should be to keep as little of it as possible in your contact center environment. Because most healthcare organizations' networks are "flat" (non-segmented), it is too easy for cybercriminals to move from one network to the next – the contact center is an ideal point of entry.

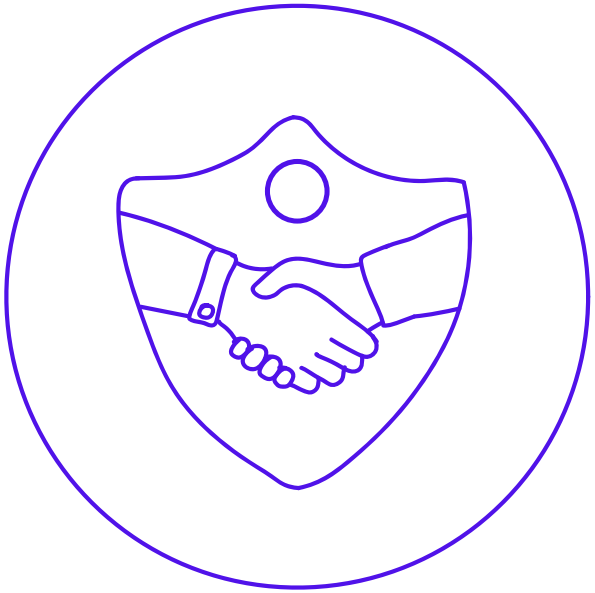
For example, with **Sycurio.Voice,** patient data is securely and directly routed to the payment provider. Your patients type the payment card data into their telephone keypads themselves so the patient service representatives in your contact center do not hear or see the sensitive information. **Dual-Tone Multi-Frequency (DTMF)** masking technology conceals the tones made by the telephone keypad so they are not captured on call recording systems or deciphered by malicious fraudsters.

And what's more, your agents can stay on the line and talk with the caller throughout the entire process, helping them complete the payment process if necessary, ensuring a smooth customer journey.



The bottom line.

Set your agents free to do their jobs without fear or threat, ensure patient trust and safeguard your organization's reputation by investing in technology that reduces risk and descopes your contact center from regulations like PCI DSS.



Make a start and talk to Sycurio about **Securing patients' payment card data – and complying with the PCI DSS**:

nasales@sycurio.com

+1 888-267-5723

sycurio.com

Sycurio.

Sycurio is your contact center data security and compliance expert.

We work closely with enterprises around the world, including healthcare organizations and insurers, to remove sensitive data from IT and business networks – protecting your customers and your company's reputation from fraudsters like those profiled in this guide. Our award-winning, patented data capture method enables organizations to securely capture personal information, including payment card data, bank account details and social security numbers, over the phone using Dual-Tone Multi-Frequency (DTMF) masking technology. Unlike interactive voice response (IVR) systems, agents remain in full voice communication with the caller as they enter their information into the telephone keypad, ensuring a positive customer experience.

In addition to reducing risk and deterring fraud, Sycurio's solutions help simplify compliance with regulations like the Payment Card Industry Data Security Standard (PCI DSS) so you can focus on business as usual.