Call Centers and the Insider Threat

Call centers have unique features that make them a particularly high insider threat risk to the enterprise. Over the course of 15+ years of insider threat investigations, we've noticed certain patterns that CISOs need to watch carefully. Here's why you need to pay special attention to the insider threat in your call center.

Call Center Employees Have Access to Sensitive Customer Data

Call center employees have direct access to sensitive customer information. Every day, your employees handle hundreds of customers' credit card information, passwords, bank info, health care information or even social security numbers.

Call Center Employees are Entry-Level and Low-Income

Low-level employees are especially risky insiders for two main reasons. The first is that they don't tend to have a lot of employer loyalty or look at their jobs as a long-term career. Second, employees who are struggling financially are much more likely to be tempted by offers from outside agents or by the money they could get selling or using customer information themselves. This results in employees that need money and may be comfortable with hurting their employer.

Call Centers Have a High Turnover Rate

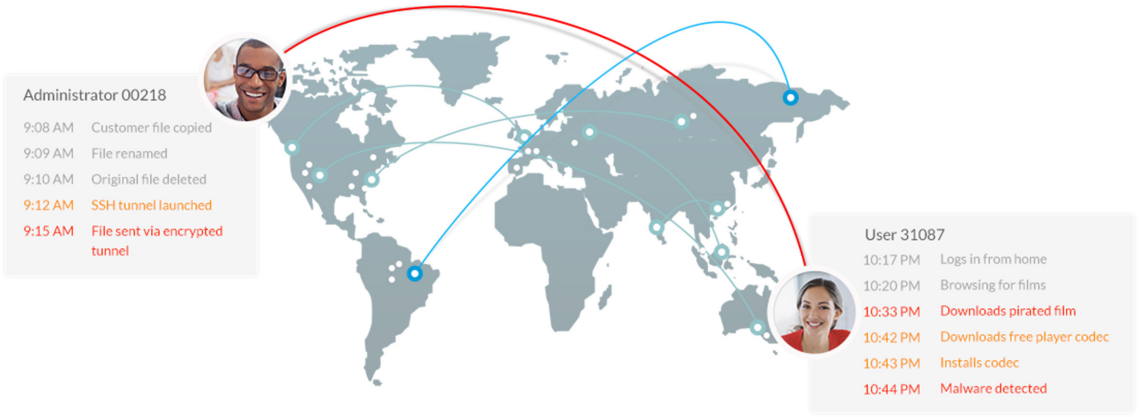
The likeliest time for an employee to steal data is when they're leaving a company. Call centers have a high turnover rate – the average US call center turnover rate hovers at aroud 33%, with a quit rate of 60% of the total turnover. In other countries, this number is even higher: average call center turnover in India, for example, is 55%. These high rates mean that you are constantly exposing yourself to the risk that a departing employee might decide to take along some sensitive customer data when they go. Plus, a high turnover rate means a greater number of employees passing through your door in a year, which means exposing your data to more people. Since it only takes one errant employee to cause a huge breach, this exposes you to considerably more insider threat danger.

Monitor Changes in Behavior BEFORE Data Theft Occurs

Most of your call center employees will be accessing the same kinds of applications and information within your organization's customer databases. How would you know if an employee started deviating from that normal behavior? With Dtex, you can baseline "normal" employee activity within a department and alert you when someone does something out of the ordinary. With this kind of visibility, you can see when an employee starts disengaging from the business or starts doing things they shouldn't, before they make a costly mistake to your business.

Trust but Verify with Dtex

You need to accept the reality of the risks within your enterprise, but the answer isn't to treat every employee like a future criminal. The nature of your business means that tight restrictions will likely hinder productivity, frustrate employees, and ultimately, upset customers. Instead, focus on getting true visibility into employee activity so you can target the real risks within your enterprise. Dtex provides analytical models based on 15 years of experience that pinpoint risky patterns of behavior. The result is endpoint visibility that gives you all the information you need without producing overwhelming alerts and false positives.



Take a Test Drive

With the tiny footprint and minimal network traffic, it is easy to test Dtex in your production environment with little risk of negatively impacting end users. We invite you to contact us for a trial period for up to 500 users to see the results Dtex provides risk free.

Some of our global customers SANYO WILLIAMS MARTINI RACING vodafone ASTON MARTIN T··Mobile· MIZUHO