Grupo Gentera Takes Microcredit to the Streets Securely with Forcepoint's Help

Gentera serves Mexico's underbanked and unbanked with microfinance loans delivered by an innovative, ultra-mobile workforce.

This microfinance bank provides banking, credit, and insurance services to individuals and groups working together to build businesses. Gentera sends its sales representatives out onto Mexico's streets to serve customers without ever entering a bank branch—relying on Forcepoint security solutions to protect customer data and privacy on the backend.

CUSTOMER PROFILE:
Grupo Gentera is the leading microfinance bank in Latin America.

INDUSTRY:
Financial Services

HQ COUNTRY:
Mexico

PRODUCTS:
- Forcepoint Web Security
- Forcepoint Email Security
- Forcepoint Cloud Access Security Broker (CASB)
- Forcepoint Data Loss Protection (DLP)
- Forcepoint Insider Threat (IT)

Grupo Gentera is the biggest microfinance bank in Latin America, serving 2.5 million customers in Mexico, Guatemala, and Peru. Gentera provides banking, credit, and insurance services to individuals and "solidarity groups" of five to 50 members working together to build businesses. The bank operates more than 350 service offices in Mexico and other countries but in recent years has spearheaded an initiative to bring its microfinance services out of the bank branch and closer to the people who need them.

Representatives of Gentera carrying smartphones are now a familiar sight on the streets of Mexico City, Ecatepec, Guadalajara, and other cities and towns throughout Mexico. These reps are a mobile powerhouse which can quickly vet and approve a prospective customer for microfinance services, completing the process of making a loan or setting up a bank account without ever walking into a physical bank branch. It's a marvel of the Digital Age but it wouldn't be possible without some heavy lifting by Gentera's cybersecurity team and Forcepoint.

Securing a 15,000-strong mobile sales force in the streets

Creating a mobile, street-level sales force without putting the bank's data and network at risk required building out a unified, centrally manageable security platform, said Gentera Information Security Manager Carlos Chan. The bank needed to be able to defend a vast, moving security perimeter and backend data repositories with maximum protection and minimal friction—and it all had to work together seamlessly, while complying with laws like Mexico's Federal Law on Protection of Personal Data Held by Individuals (LFPDPPP) and regulations by oversight agencies like the National Banking and Securities Commission (CNBV). "We have more than 15,000 employees in the streets. Some of those people are still using pen and paper to sign up customers, but about 80 percent of them have mobile phones with an Android application for collecting all the customer information we need to start accounts and make loans," Chan said.

"Our employees in the streets might have their mobile device or papers stolen. That means people's data might wind up in the wrong hands. We needed incident response capabilities and forensics after the fact to close all the gaps that put our street operations at risk."

Gentera safeguards the data generated by its mobile workforce at its bank branches with Forcepoint Data Loss Prevention (DLP) and Forcepoint Cloud Access Security Broker (CASB). At Gentera headquarters, the cybersecurity team also utilizes Forcepoint Web Security and Forcepoint Email Security to protect against external threats like malware and phishing, as well as Forcepoint Insider Threat (IT) to provide forensics in the event of a data loss incident or data breach attempt.

A dozen data loss threats stopped in their tracks

"What we have created with this security framework is a layered approach to securing data, protecting our customers, and complying with all the relevant rules and regulations," Chan said.

"We started out with Web Security and Email Security because they're good products. When we developed our street microcredit program, we knew we needed to closely manage access to our IT resources and our operations in the cloud like Office 365. We also had to protect against data loss, like a device being compromised or lost or an employee sending customer data collected for us to one of our competitors."

Forcepoint CASB is the tip of the spear for Gentera when it comes to making sure only the right people are able to access the bank's cloud apps and services. Chan highlighted the ease of integrating CASB within the Gentera security framework, calling it "a natural fit with our infrastructure."

Challenges

Secure the data generated by an ultra-mobile sales force operating with smartphones in the streets.

Maintain rapid, effective incident response at all times.

Comply with governmental and industry rules and regulations..

Approach

Utilize Forcepoint CASB for access management, DLP to safeguard data, IT for incident analysis and forensics.

"We've stopped a dozen incidents thanks to DLP and CASB. This is great for us in terms of our regulatory responsibilities because part of our organization operates as a governmental institution and another part is a private sector business. The incidents that we prevented occurred in both the secure information area where we do governmental things and in the data privacy area where we operate as a private business," Chan said.

> "We've stopped a dozen incidents thanks to DLP and CASB. This is great for us in terms of our regulatory responsibilities."
>
> **CARLOS CHAN,** GENTERA INFORMATION SECURITY MANAGER

Forcepoint Insider Threat provides a complete picture for incident investigators

Gentera added Forcepoint Insider Threat as the final piece of the puzzle most recently. IT gives visibility into potential insider threats with a complete view of privileged users who interact with intellectual property and sensitive systems. After an incident, it is invaluable for determining how it occurred with archives of user actions kept through metadata, keystrokes, forensics, and video.

"Insider Threat is the latest Forcepoint product that we've implemented. We use it as a tool for investigating how incidents happen after the fact and we also see it as a big part of our future roadmap for preventing incidents and being even more proactive about countering data exfiltration threats," Chan said.

"The great thing about IT's forensics capabilities is that it helps us learn about data loss risks that might be unintentional. We can see the context for how something occurred and we have the capability to learn exactly what happened and what actions were performed in each moment, basically reconstructing the incident from beginning to end."

Forcepoint's modern cybersecurity tools help Gentera analyze user and system behavior to more quickly detect anomalous activity that might lead to a data loss incident. The bank is able to use these tools to safeguard against such incidents without shutting down a user's access while analysts manually sift through hundreds of alerts. The result: An integrated security solution that keeps sensitive personal and financial data protected on the backend of its mobile workforce's operations— without slowing down the salespeople and other representatives delivering Gentera microfinancing to help customers take their businesses to the next level.

Results

More than a dozen data loss incidents prevented with CASB, DLP.

Data generated by street-level sales force secured with minimal friction from cybersecurity.

Forcepoint IT gives a complete picture of how incidents occur and how to prevent them in the future.