

Case Studies - Recent Key Provider Wins



Provides software solutions for public sector over the past 40 years

Needs: Require FIPS secured connectivity from customer sites to AWS gov cloud workloads
Pains: Deployment and support challenges effecting profitability:

- Sales friction addressing IT reqs
- Long lead times to deploy VPNs
- Support issues due to network changes at customer sites

Outcomes: Highly secure, scalable, simple solution to:

- Quickly overcome IT pushback
- Deploy new sites 95% faster
- 50% cost savings by removing legacy site-to-site VPN offers
- Improved Support as solution deploys without F/W config issues
- CJIS and FIPS compliance

Major pains, perfect timing to evaluate and solve, clear ROI



Provides a digital health enablement platform to drive efficiencies/ outcomes

Needs: Scalable, secure and reliable connectivity from customer sites to AWS cloud
Pains: Legacy ZTNA solution was failing and problematic:

- TrustGrid reliability issues
- Sales challenges due to vendor reqs to be named in customer contracts
- Need better remote administration and push to run workloads in Cloud

Outcomes: Highly secure, scalable, simple solution to:

- Deliver quick, scalable solution using COTS product vs. DIY
- Designed secure connectivity directly into the application, meet HITRUST
- Enable better connectivity and manageability to 1800 customers

Build (OZ) vs Buy eval, fast ROI uncovered after experiencing pains from legacy vendor decision



Offers a cloud-native RMS delivering a fast, reliable, secure experience

Needs: Deploy new SaaS offers in the Cloud and access agency's private networks/ data
Pains: Simplify their move from purely On-Prem to SaaS offer:

- Roadblocks, customers lack IT depth
- Difficulty supporting VPNs
- FIPS requirements and decision to build NaaS into their Cloud

Outcomes: Simplified, secure and complaint offer to:

- Drive revenue and minimize customer technical involvement
- Meet FIPS/ CJIS requirements and leverage a flexible yet simple model
- Upsell/ convert customers to SaaS
- Eliminate future operational and support issues

Build (OZ) vs Buy eval and needed direct NF support to deliver On-Premise



Delivers an identity automation platform for disconnected apps.

Needs: Deliver PAM to customer's private apps by embedding secure connectivity
Pains: Moving from public to private app access behind f/w:

- Newer revenue model and offers requiring secure connectivity
- Difficulty transmitting shared token to Cerby Cloud for administration
- Complex, bi-directional workflow

Outcomes: Secure, scalable solution integrated with customer apps:

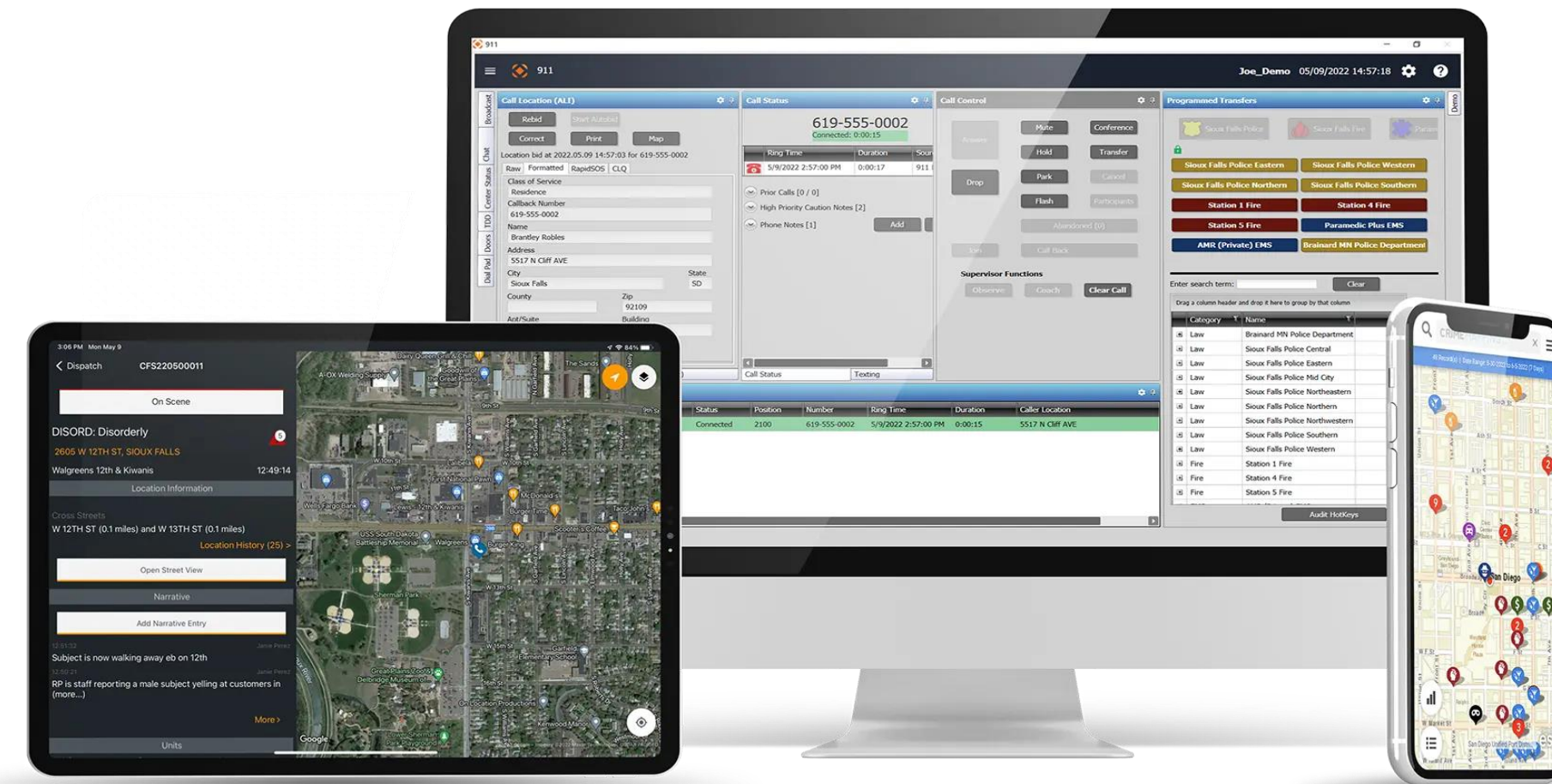
- Drive new solution revenue
- Accelerated time to market vs DIY approach
- Alignment on business model to move fast and enable growth

Building new offer to deliver PAM to private apps and required mTLS

CentralSquare Technologies – Customer Overview

Background

- Provide software solutions for Public Safety (ex. Police Dispatch)
- Competitor of Mark43
- Rudford engaged them via LinkedIn request
- VP of Cloud connected quickly



Win Details

- \$510k booked for 14 month agreement
- Adding \$40,417 MRR
- Less than 30 days from first meeting to signed contract
- Highly repeatable use case
- Great story and reference

Discovery of Pains

- First customer call on Oct 7
- ~8000 customers, CJIS & FIPS required
- Big contract with AWS
- Require/ deploy an AWS S2S VPN at customer sites
 - Long lead times - deployment takes 6-8 wks
 - Customer network challenges - firewall, IPs
 - Support issues - Costly to deploy/ manage
- Major revenue blockers/ sales friction

NF Team – Rudford, Nic, Hersh

“Part of the desired result is to be able to implement customers much faster than they can get done today so we can unlock ARR sooner. Replacement of VPNs as a means of securely connecting our customer sites to our cloud in an encrypted fashion. Also simplifying deployments, ongoing network configurations and reducing potential for issues caused by changes in customer network configurations. NetFoundry's platform being zero trust also improves our overall security posture and CJIS compliance” - Kirk Cameron, CTO

Process and Path To Solutions

- Day 2 - Engaged wider team quickly, deep dive, defined POV
- Day 3 – NDA signed, started PoC, demo of working solution
- Next 2 weeks – completed PoV, tech eval, business model/ pricing aligned
- Week 3 – Proven VPN replacement, Finalized contract redlines, pricing model
- Week 4 – Contracts signed

CentralSquare – Solution Diagram

Benefits and Outcomes

- Speed up rev rec and deals signed
 - Simplified outbound only connectivity solution
- Cut deployment times to 2 days
 - Removed IT involvement and approvals
- Streamlined business model to save \$
 - Per customer site pricing model
- Removed support issues related to IP address or Firewall changes
 - Identities, no inbound ports
- Enhanced compliance offer
 - Zero Trust offer meeting FIPS & CJIS standards

