

## A Case Study from Mirage Networks®



### INTRODUCTION

When contractors are a part of your business, how do you keep the network safe from threats on their unmanaged laptops, cell phones and other devices?

This is exactly the challenge Kern Schools Federal Credit Union® (KSFCU) was facing. The answer? Mirage NAC™.

### THE CHALLENGE

KSFCU is in the top ten percent of the largest credit unions in the United States, with a network size to match. For a financial institution, contractors like auditors and regulators accessing network resources are a fact of business. So are federal and state regulations, like the privacy provisions in the Graham-Leach-Bliley Act (GLBA). An assault upon the network's security could have far-ranging effects beyond downtime and lost productivity: it could force the organization out of compliance with federal law.

With these requirements, KSFCU realized that it faced the very real potential for a destructive worm breaking out from a contractor's unmanaged laptop and taking down KSFCU's network. KSFCU searched for a network security solution that would stop worms and other threats from wreaking havoc, and that would increase user productivity and satisfaction without increasing the burden on IT.

### THE REQUIREMENTS

Given KSFCU's need to control day-zero threats coming from uncontrolled contractor devices, key requirements for this solution included that it:

- » be effective without relying on either agents or signatures, and be infrastructure-, OS- and device-agnostic;
- » enable policy compliance checks of devices upon entry, to further decrease the likelihood of infected devices accessing the network;
- » continually check devices for threats once network access is granted; and
- » offer targeted quarantining and mitigation options that don't interrupt the traffic of uninfected, policy-compliant devices.

continued »

## » executive summary

### Industry:

- » Financial Services

### Business Challenges:

- » Ensure security while enabling contractors to access the network
- » Maintain a positive user experience without increasing IT drain
- » Invest in a solution that can scale from branch offices to corporate campus

### Security Solution:

- » Deploy Mirage NAC at corporate campus
- » Staged deployment in remote, branch offices

### Business Value:

- » Helps meet federal and state regulations around data safety
- » Leverages other infrastructure and security investments
- » Redirects IT resources from Help Desk calls to other critical functions

## THE MIRAGE NETWORKS SOLUTION

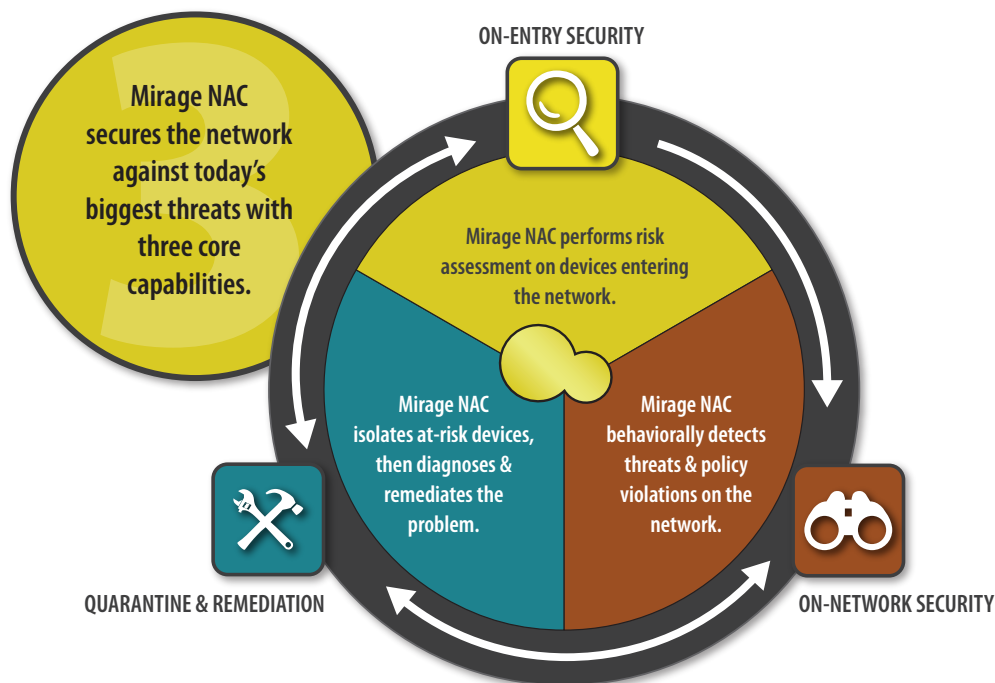
KSFCU diligently reviewed the market, removing from its short list solutions that required too costly and hard-to-manage implementation and deployment. The company then chose the Mirage NAC solution, which enabled KSFCU to easily and cost-effectively keep infected devices off its network. This unique, full-cycle approach spans the three core elements of a complete NAC solution:

- » On-entry security: risk assessment for all guest IP devices
  - Checks new and unmanaged devices
  - Scans for prohibited services and devices
- » On-network security: policy enforcement and threat mitigation
  - Behaviorally detects day-zero and other threats on all devices and all OSs
  - Identifies devices breaking protected segments' security policies
- » Infrastructure-independent quarantine and remediation
  - Isolates offending endpoints without cross-infection
  - Fixes threats and vulnerabilities, and can automatically rescan and readmit

KSFCU utilizes the Mirage NAC solution to test all contractor devices when they request access to the network. If a device fails the policy checks, it is quarantined and removed from the network to enable remediation. Once the device passes the checks and is admitted to the network, the threat mitigation capabilities of Mirage NAC begin, continually monitoring all network traffic from all network-attached endpoints, regardless of OS or device type. It identifies and quarantines devices whose behavior indicates they may be infected or out of policy, and offers vulnerability scanning and threat mitigation functionality that decreases the users' demand on IT while speeding their return to productivity.

*"Mirage's approach has alleviated my concern about the many unmanaged contractor machines that come onto my network, potentially spreading malware. In combining the on-entry and on-demand deep scans with agent-free and signatureless threat detection and mitigation, Mirage is enabling my team to focus on mission-critical business rather than unproductive emergency fire drills. And my users are happy because we've minimized the pain associated with threat mitigation, and they can get back to work quickly. All in all, it comes as close to ideal as you can in this environment."*

*- Chris Hanson, IT project manager,  
Kern Schools Federal Credit Union*



Mirage Networks  
6801 North Capital of Texas Highway  
Building 2, Suite 200  
Austin TX 78731

phone: 866.869.6767  
fax: 512.874.7806  
email: [info@miragenetworks.com](mailto:info@miragenetworks.com)  
web: <http://www.miragenetworks.com>

©2006 Mirage Networks, Inc. All rights reserved. Mirage Networks, the Mirage logo, Mirage NAC, NAC-in-the-Box, and "You can't control people. Control what's on your network." are trademarks or registered trademarks of Mirage Networks. All other names and products may be trademarks of their respective companies.