

Case Study: CSAC Protects County Interests with Identity-Based Access Controls

Jeff Williams
California State Association of Counties

September 12, 2006



Introduction to CSAC



- Nonprofit, nonpartisan advocate for California's 58 counties
- Represent before lawmakers, agencies and federal government
- Counties range from 1,200 to 10 million people
- Serving counties for 112 years—since 1894

Multiple constituencies, unique challenges



- Serve multiple groups
- 296 county supervisors
- 62 board members
- All demanding, high expectations for CSAC service and integrity

State Government – security status

- State government entities are the 2nd most often targeted (behind financial services)
- 13% of all breaches – internal and external – involve state governments
- State government networks often have “ghost” servers that haven’t been used in years but still contain sensitive data
- Open and easily accessible information is often part of our mission – this brings risk

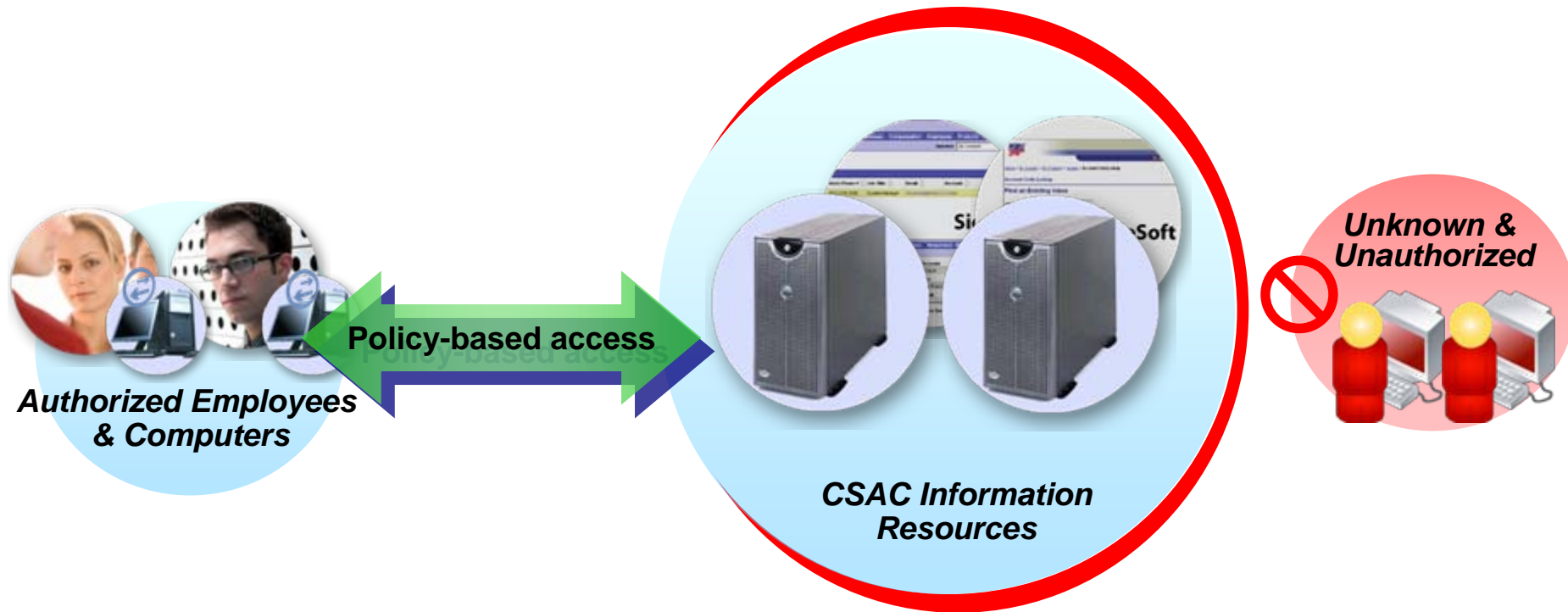


CSAC's issues:

Small organization, big risks

- Protect servers/applications from unknown users
- Grant appropriate access to specified users/machines
- Reporting and auditing capabilities for state compliance initiatives
- IT must be responsive with limited staff, budgets
- Integrity and credibility of CSAC at risk if systems breached
- Risk to counties' agenda and fiscal well-being

Goal for CSAC: Right Users In, Wrong Users Out



Solution considerations

- Firewalls —limited

- Identity blind
- No machine authentication
- Limited auditing
- Complex configuration

- Chose

- Identity management and network access control appliance and software

Selected solution: Identity Management and Network Access Control



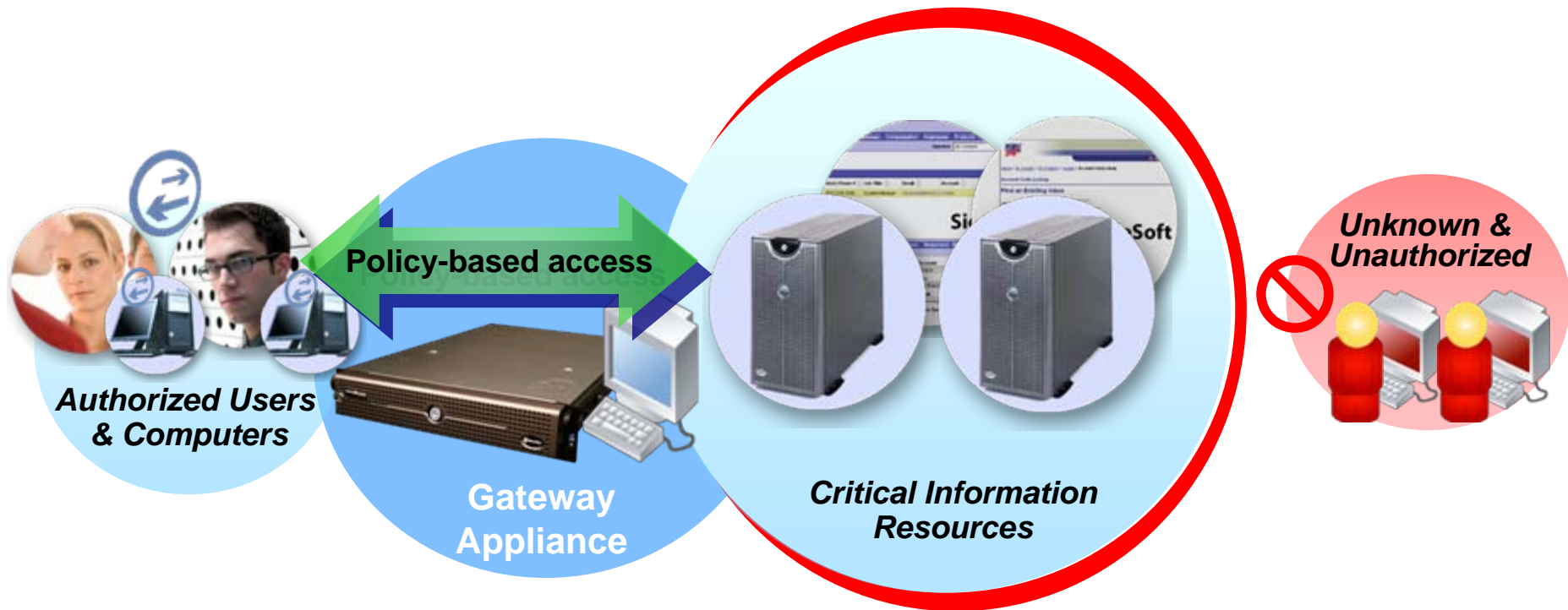
User & Computer Identity



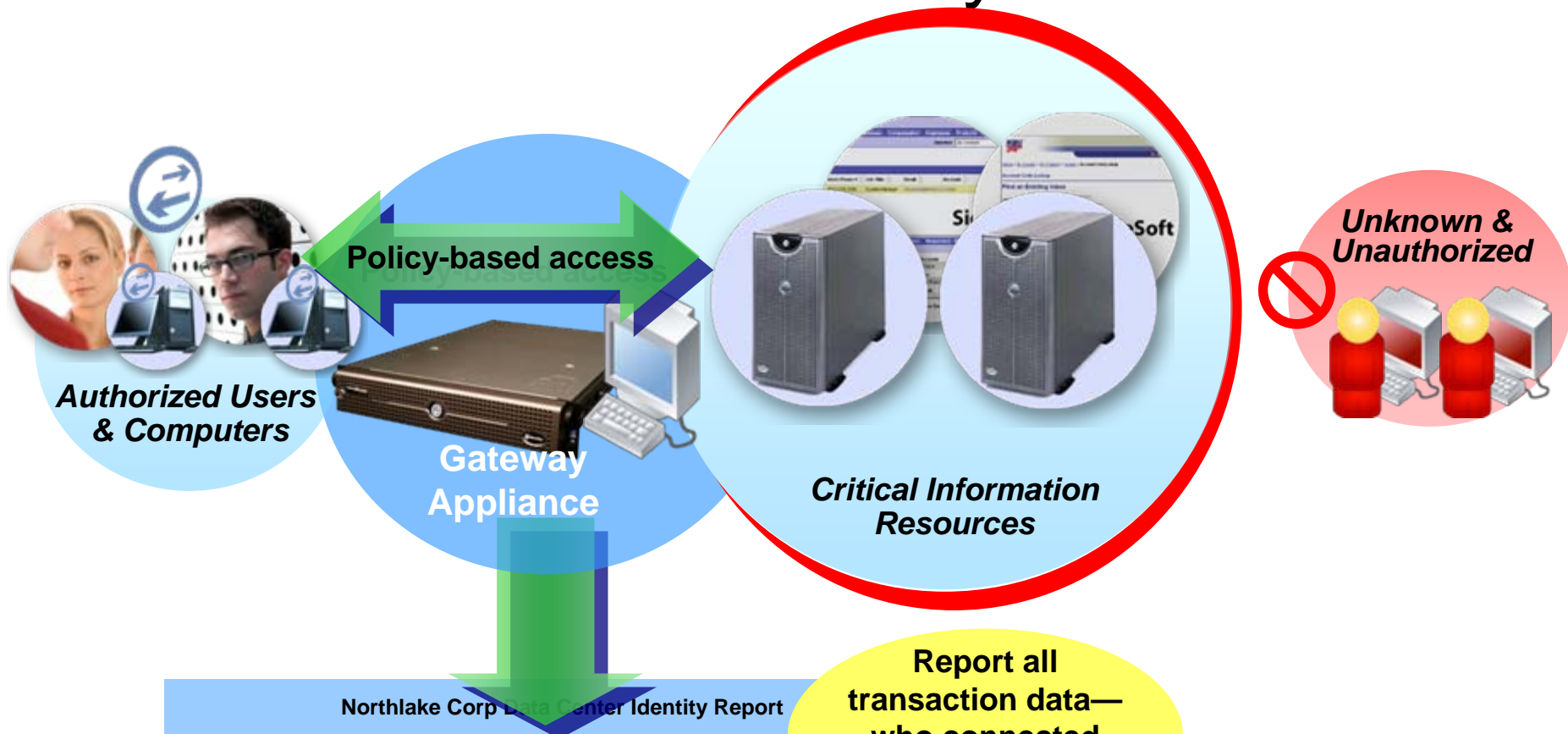
TNT's Identity

- Simple, straightforward implementation
- Met CSAC's priority access control objectives
- Established unalterable user and computer identity into network traffic
- Grant or deny access to specific information resources based on identities
- Simple tool to configure, set policies and report all activity

Solution delivers user- & computer-based access control



Simple, clear reporting & policy verification—total visibility



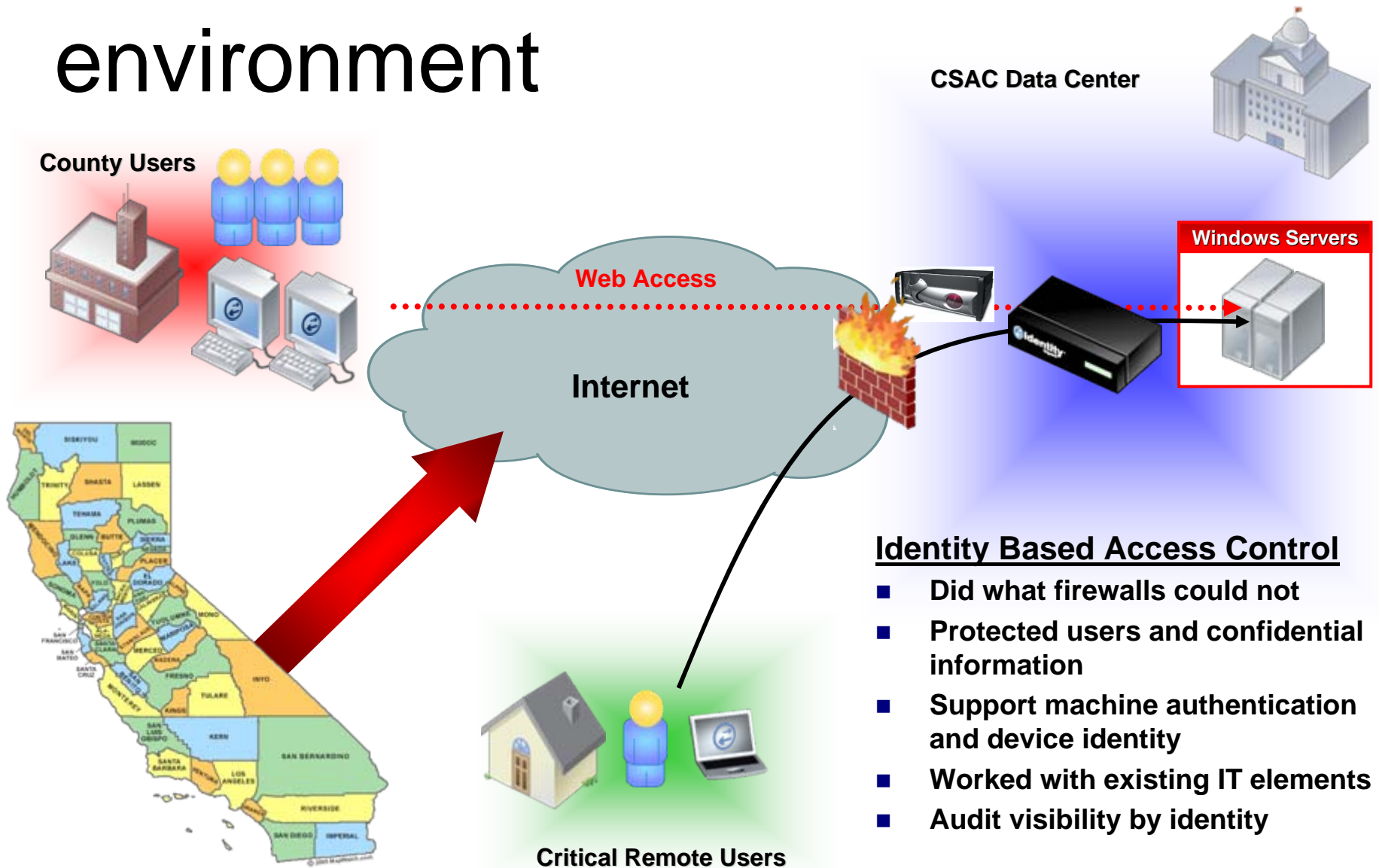
Northlake Corp Data Center Identity Report

From 10/3/05 11:23 AM to 10/14/05 11:23 AM
 Trusted Network: Northlake Data Center Mode: Audit
 Workstation Any Destination: Any Application: Any
 Connection Status: Any Identity Status: Any

Report all transaction data—who connected with what, from where, when

User	Access Level	Workstation	Server	Application	Time of Connection Attempt	Connection Approved	Policy
Sarah Brown	Level One	Sarah Brown Work PC	Finance Server	Oracle Data Base	10:45:14 AM	No	Yes
Mark Littlefield	Level Two	Mark Littlefield Work PC	CRM Server	Seibel	10:46:48 AM	Yes	No
Lisa Sosebee	Level Three	Lisa Sosebee Work Laptop	ERP Server	Peoplesoft	10:47:36 AM	Yes	No

How solution fits in CSAC's environment





Results

- Identity enabled infrastructure provided full view of user and endpoint behavior
- Led to rapid, straightforward and effective access control policy decision
- Protected the critical state information records from data breaches
- Ensured confidentiality of communication within state government and counties
- Provided full audit to address regulations