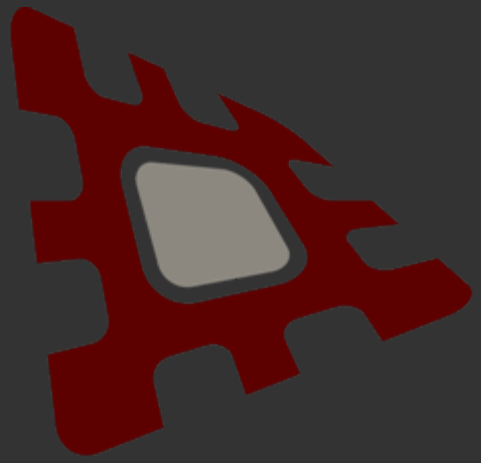


WHITENOISE
SYSTEMS

www.whitenoisesystems.com

Company

- Formed June 2006
- Company Mission: Create Products That Protect Data at the Point of Creation and Absolutely, Positively Guarantee Your Data Will be There When You Need It!
- Innovative provider of Data Protection Solutions which protect data at the point of creation and maintain that protection throughout the entire data lifecycle.
- Product Development for past 18 months – launched first solutions in early May 2008

Webinar Outline

- Data Protection
  - The problem (how big is it, examples, etc.)
  - The different solutions out there, including pros and cons; what industry experts/analysts say about these different solutions
- Overview of the WhiteNoise Solution
- IT/Business Alignment and Tips for you to win the battle
- Q&A

Data Protection

- **Data Protection is Essential to Move Forward:**
  - Avoid expensive (and embarrassing) data breaches and losses
  - Allow for business continuity and disaster recovery
  - Comply with government regulations
    - Sarbanes-Oxley
    - HIPAA
    - SEC
    - Patriot Act
  - Ensure customer confidence

Magic Number

- **149,250,000**
- 49% of US population
- 4.6% of World population
- Population that over the past 18 months was directly affected by theft of computer data/information

Source: Identity Theft Resource Center

Chronology of Devastation

Date	Company	Event
January 17, 2007	The TJX Companies Inc.	Experienced an "unauthorized intrusion" into its computer systems initially affecting 45,700,000 credit and debit card account numbers. 48,000,000 additional people were affected for a total of more than 94 million.
Jan. 22, 2007	Chicago Board of Elections	About 100 computer discs (CDs) with 1,300,000 Chicago voters' SSNs, birth dates and addresses disappear.
Feb. 12, 2007	Johns Hopkins University	Backup computer tapes containing payroll information on 52,000 employees, including SSNs and in some cases bank account numbers.
April 10, 2007	Georgia Dept. of Community Health	A computer disk containing personal information for 2,900,000 people including addresses, birthdates, dates of eligibility, full names, Medicaid or children's health care recipient identification numbers, and Social Security numbers
Jan. 17, 2008	GE Money / Iron Mountain	Personal information on customers of J.C. Penney and up to 100 other retailers are compromised after a computer tape went missing. The missing information includes Social Security numbers for about 150,000 people.
Mar. 17, 2008	Hannaford Bros. Supermarket Chain	This security breach affected 4,200,000 individuals. Credit and debit card numbers were stolen during the card authorization transmission
Mar. 22, 2008	Agilent Technologies	A laptop containing sensitive and unencrypted personal data on 51,000 current and former employees of Agilent Technologies was stolen from the car of an Agilent vendor. The data includes employee names, Social Security numbers, home addresses and details of stock options and other stock-related awards.
Aug. 2, 2008	Countrywide Financial Corp.	The FBI arrested a former Countrywide Financial Corp. employee who stole and sold sensitive personal information from 2,000,000 people, including Social Security numbers. The breach occurred over a two-year period.

Threat Spectrum

Today's Business Situation

- Industry pundits say that perimeter security has outlived its effectiveness and some even go so far as to suggest perimeter security is "Dead".
- New business pressures mean that organizations need to share data across ever-widening organizational and geographical areas.
- At the same time, companies face increasing accountability for ensuring their data is properly protected, even when it resides on infrastructure over which they have little or no control.
- The new mantra is "Data-centric" security but mainstream data-centric security tools capable of handling vast amounts of data are not available... Until SecureNOW!

The Battle is Heating Up!

- Cyber criminals today use highly sophisticated software tools:
  - Require no knowledge of computer programming or hacking techniques to operate.
  - Enable the criminal to infiltrate and steal financial information from thousands of PCs simultaneously.
  - Provide an efficient way to sort through the mountains of information they've stolen and quickly monetize the data.

The Battle Inside Is No Better

- In a Study Conducted in Q1 2008 by YouGov and Posted in Security News
  - Businesses face a serious security threat from inside
  - Employees Were Asked: “What type of information would tempt them most?”
  - The survey also highlighted an external risk

Treacherous Landscape

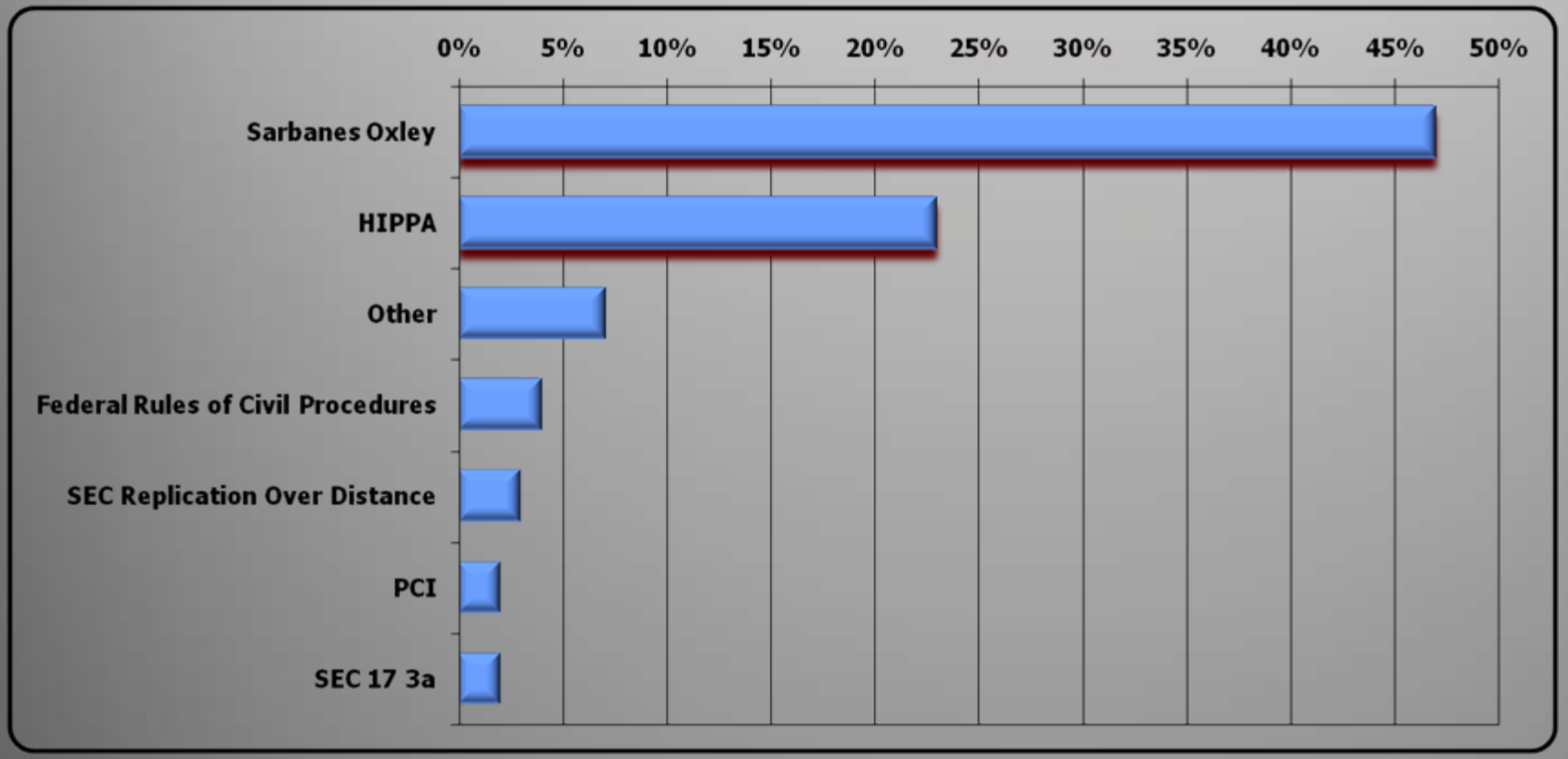
- Survey of Global 2000 suggests laptops are mostly stolen at work.
- Insider Exposure
- Applications Targeted
- Browsers Under Siege

Source: Reconnex Study

Business Continuity

- Users often have critical information on their local resource – desktop or laptop that if lost or stolen can cause tremendous problems.
- Multiple versions of documents cause challenges for organizations (Storage and Usage)
- Compliance adds levels of complexity to data storage and availability.

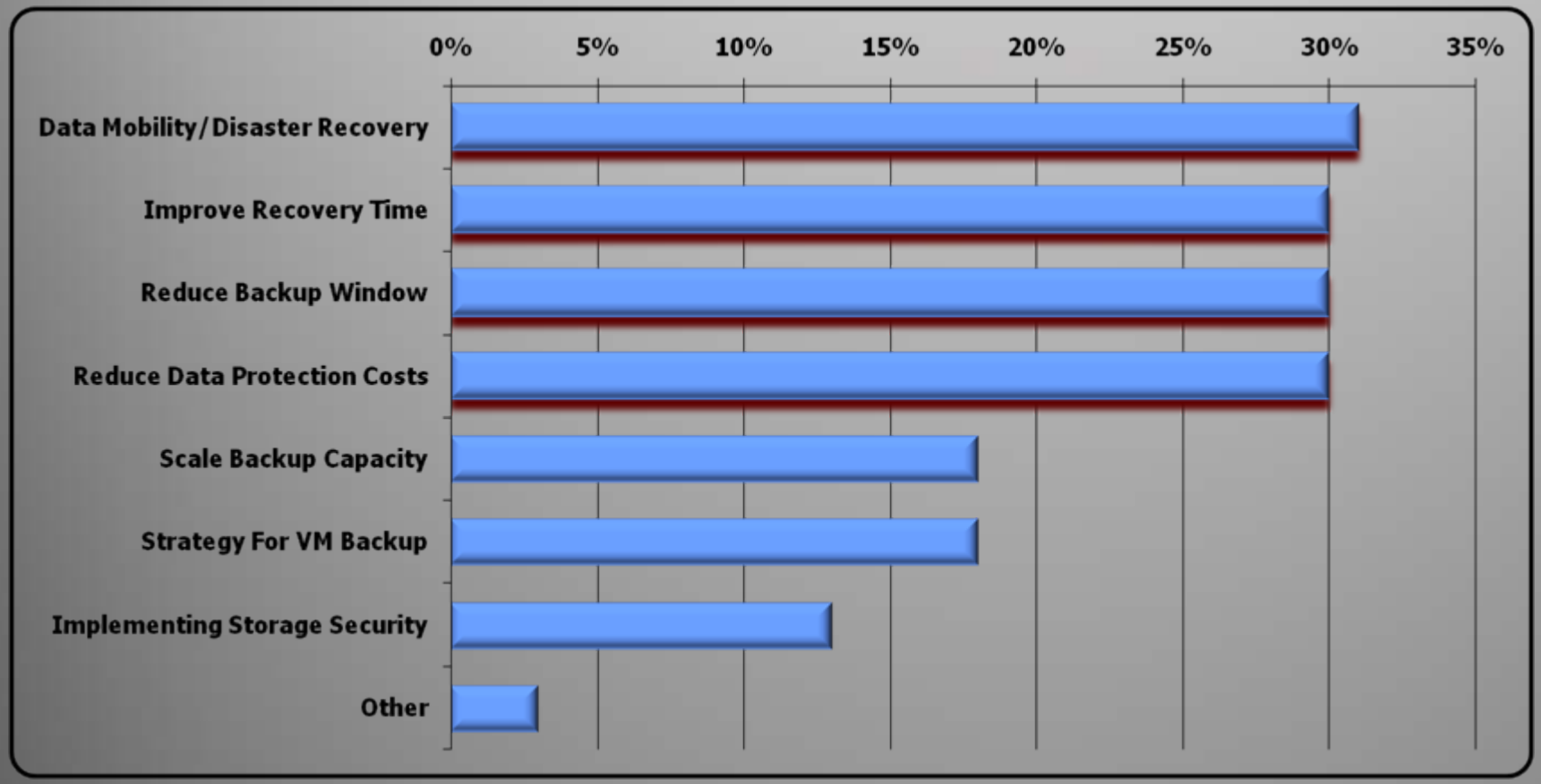
Compliance is a PAIN!



Disaster Recovery

- Natural Disasters affect more data than any other impact.
- Man-made disasters cause major data losses
- The time to recover can range from days and weeks to months and even years after a disaster
- The costs to recover data after a disaster often exceed $Millions

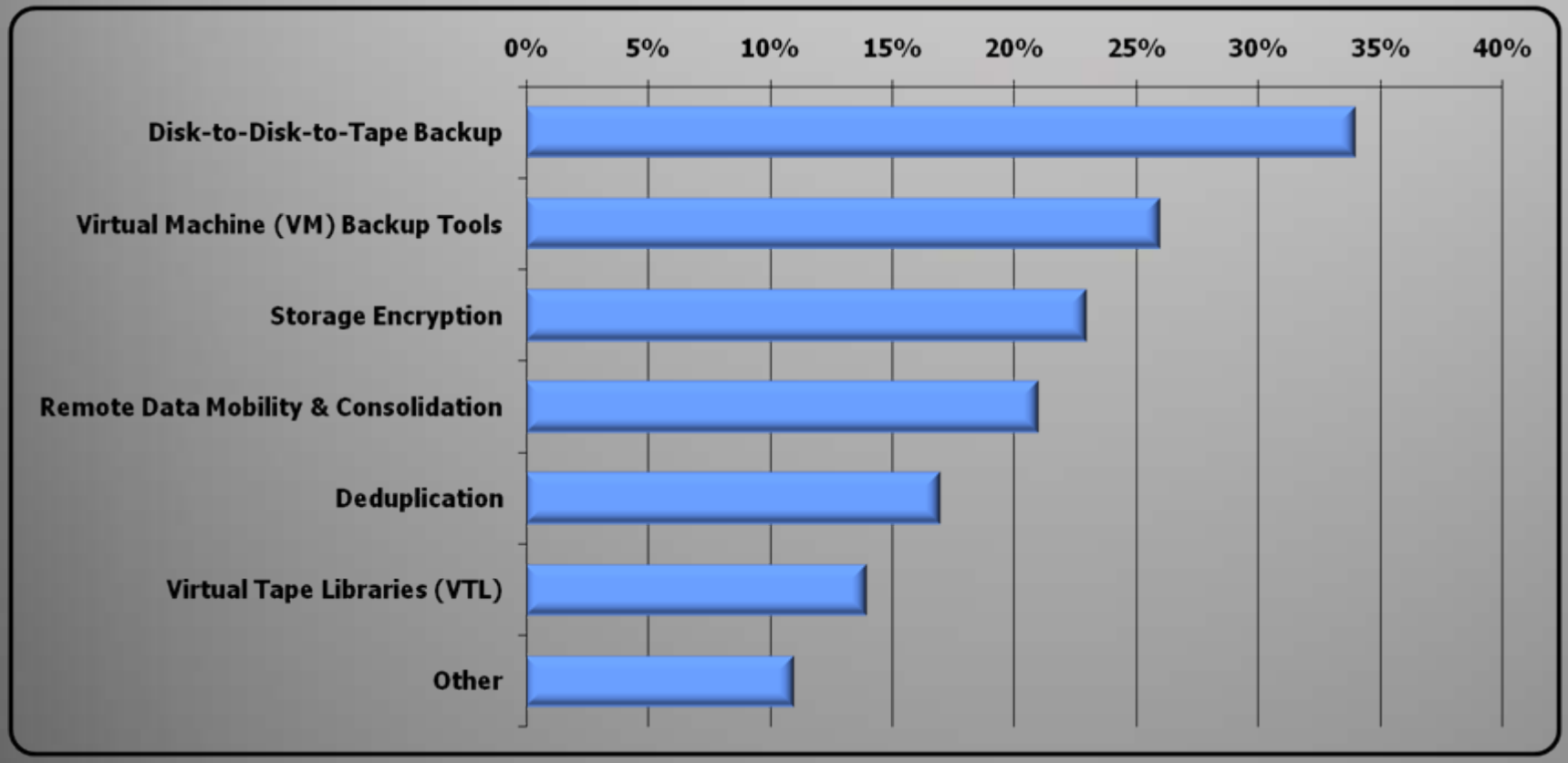
Key Data Protection Concerns



The Situation

- Company Executives
- Business Managers
- John Morency, a research director at Gartner,
  - “for many organizations, time required to recover critical business processes…has dropped by roughly an order of magnitude from what it was 10 years ago, but it is still lacking important components for a comprehensive recovery plan.”
  - “the business continuity market has notably shifted in the past few years, with greater focus on availability and recoverability, as well as intense interest in auditing and validation.”

Current Thinking



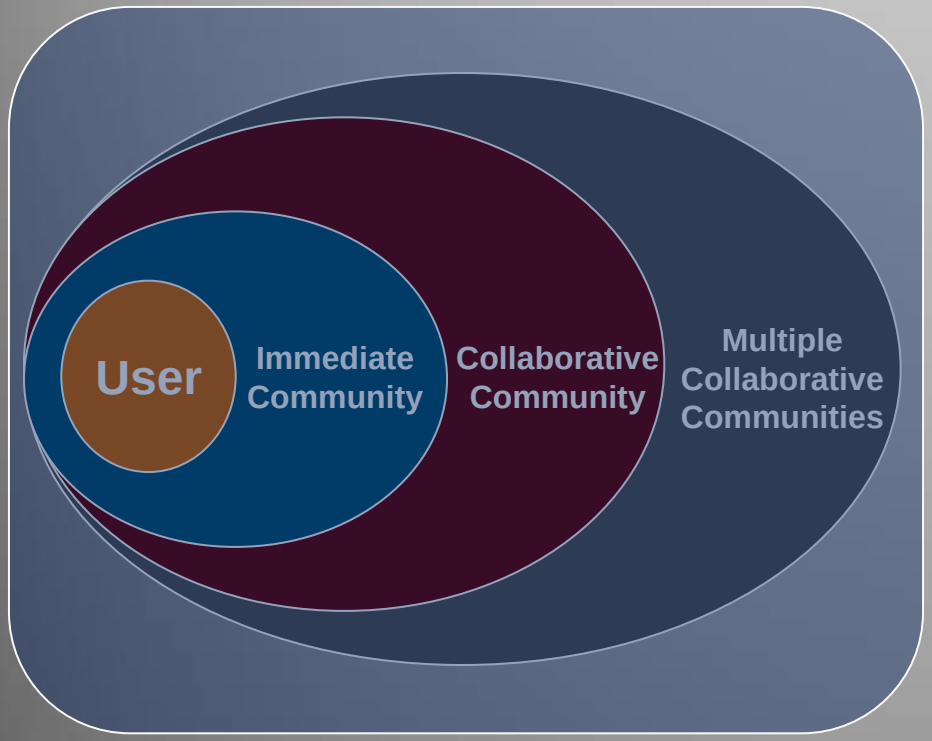
Appliances – Answer?

- Data Protection appliances are defined as a combination of
  - Hardware with a hardened operating system (OS)
  - A limited applications software set with no user software installation
  - Networking technologies to perform specific security functions
- Why are people buying appliances?
  - Convenience
  - Ease of installation
  - Centralized management

Appliance Problems

- Point to Point Solutions
  - Do not scale
  - Very expensive
- Appliance
  - Negatively impacts customers availability
  - Requires multiple appliances to achieve high availability
  - No facility to upgrade encryption -> forklift upgrade
- Key Management
  - Inability to maintain keys w/ data
  - Requires a costly strategy for key management/bunkering
  - Storage Facility: bunkering keys for decades
  - High TCO for key management
- Data Confidentiality
  - Susceptible to platform subversion
  - Secure and unsecure information is located in a single location
- Data Integrity
  - No audit mechanism for continual verification
  - Inability to maintain keys w/data
  - Not a Global Information Grid Solution

What Users Need To Succeed



Easily Lock Down Data on Laptops & Desktops

Securely Communicate With Community

Collaborate on a Project - Globally & Within a Secure Environment

Collaborate on Multiple Projects - Globally & Within a Secure Environment

Maintain Business Continuity and Recover FAST From Disasters

SecureNOW! Solutions

- SecureNOW!*personal*
  - Standalone Product Solution

- SecureNOW!*professional*
- SecureNOW!*smb*
- SecureNOW!*enterprise*
  - Three different SaaS Solutions
  - Eight tier-1 datacenters on-line
  - 99.999999% uptime network infrastructure available

- All Solutions – Available September, 2008

SecureNOW! Solutions

- Solutions Deliver Four Key Value Propositions
  - Data Confidentiality
  - Data Integrity
  - Continuous Data Availability
  - A new Total Cost Ownership (TCO) for key management

SecureNOW! Benefits

- Allows you to **“Hide Data in Plain Sight!”**
- Form secure communities of interest (COI’s) in minutes
- Supports cross domain information protection (CDIP)
- Information is accessed at local speeds
- Storage has been abstracted so that ANY storage can be used
- Enables any potential customer to understand data shredding
- The cost & effort to setup POC is minimal

SecureNOW! Eliminates

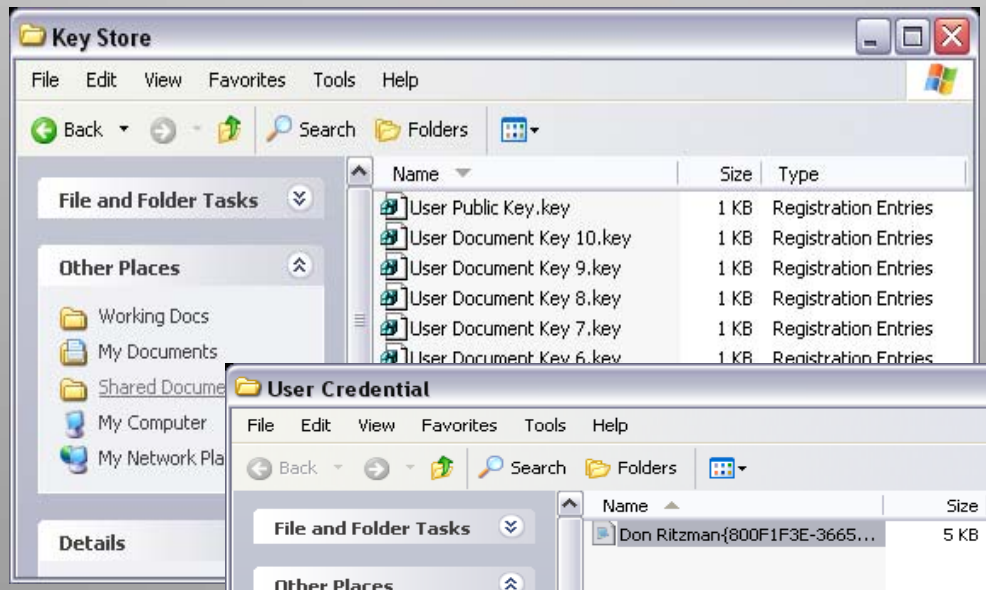
- Denial-of-Service (DOS) attacks on your data
- The barriers for 100% trading partner participation
- Data replication for disaster recovery/business continuity
- Active-passive storage solutions
- File Key management
  - Long-term storage for keys
  - Costly effects of re-keying

SecureNOW! Assures

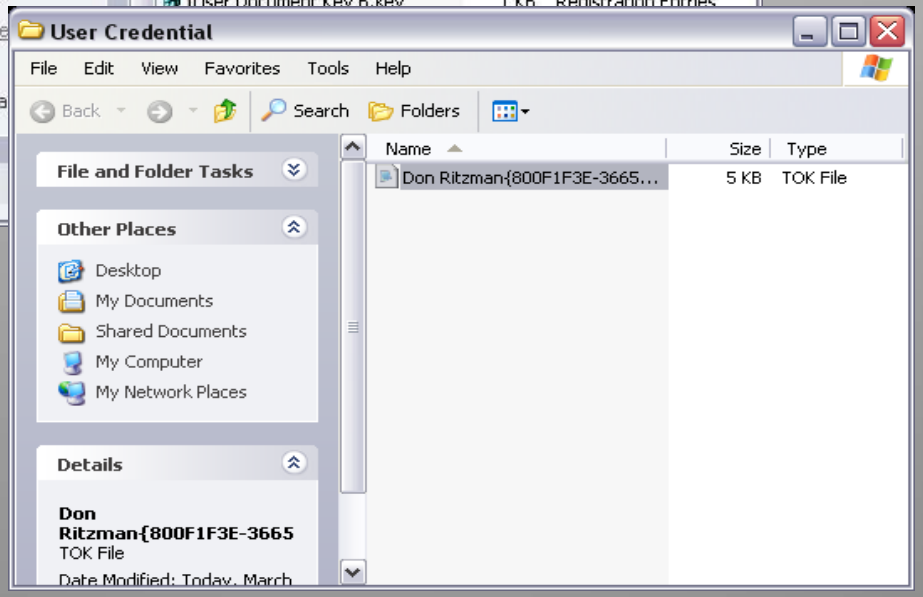
- Constant access to your data
- Your data has not been changed by unauthorized access
  - Ability to recover from unauthorized data tampering
- Data Recovery: Recovery Point Objective (RPO) & Return To Operations (RTO) of near ZERO
- No discernible data
  - is present in a single location
  - is sent over a network
  - to capture and playback
- Information security - handheld device to enterprise
- Only appropriate information is presented to authorized personnel

Credentials vs. Encryption Keys

- Too Many Keys



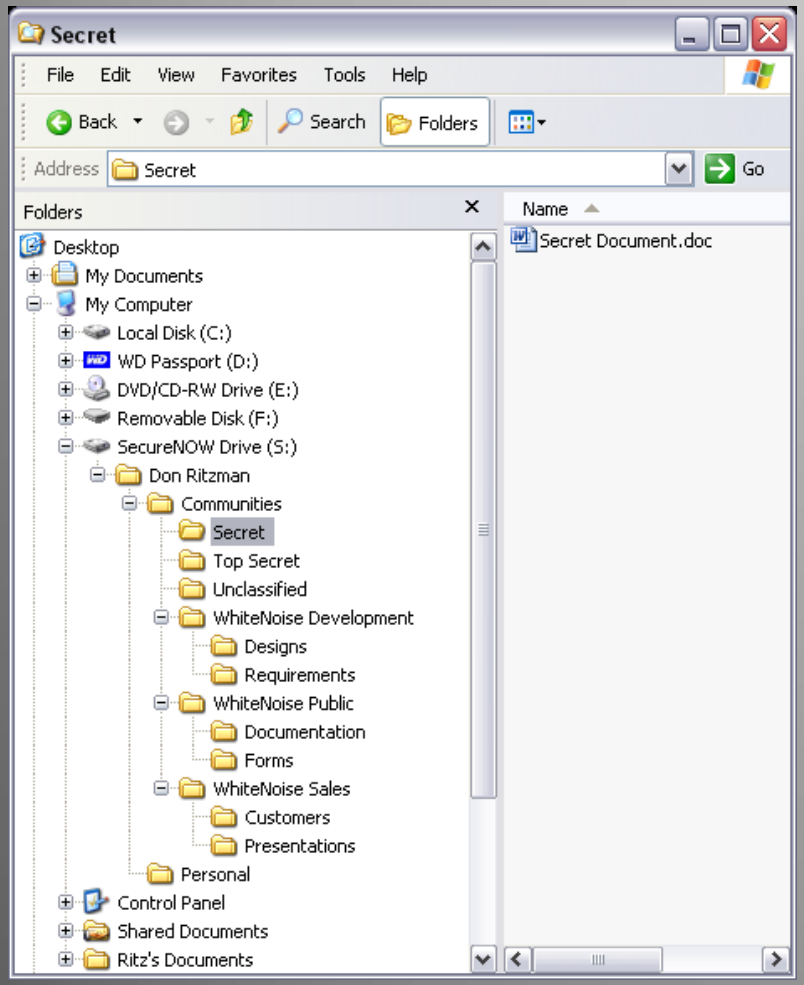
- One Credential

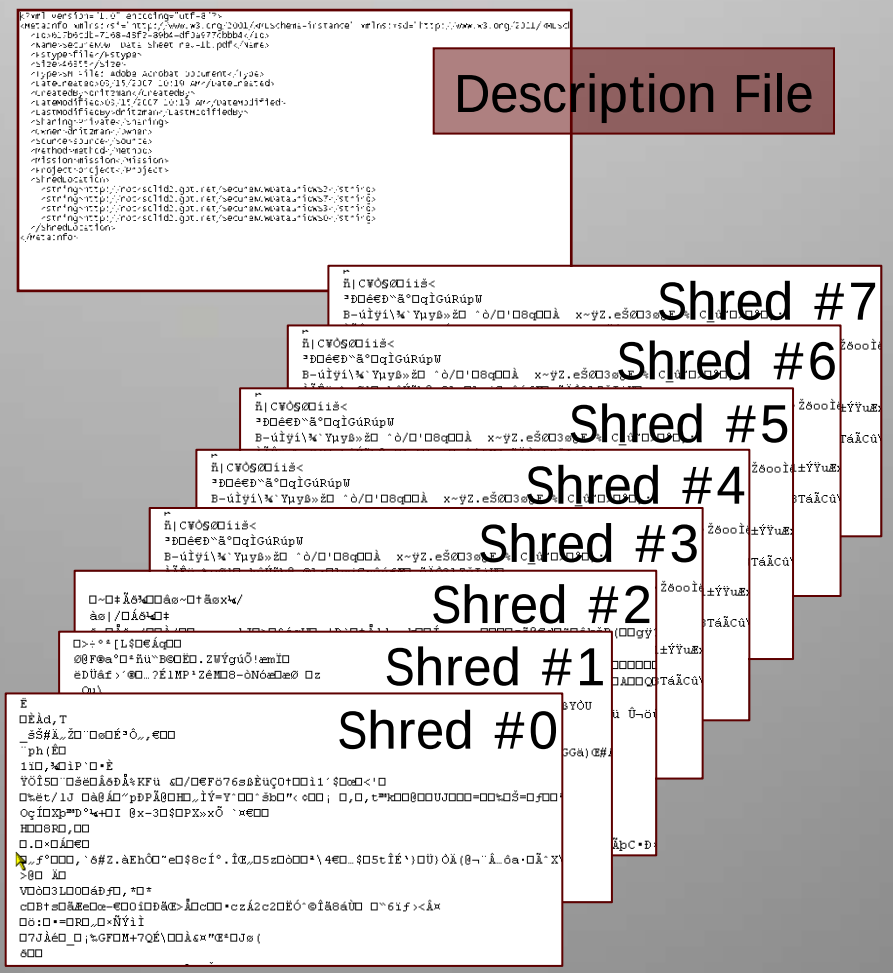


SecureNOW! Solutions

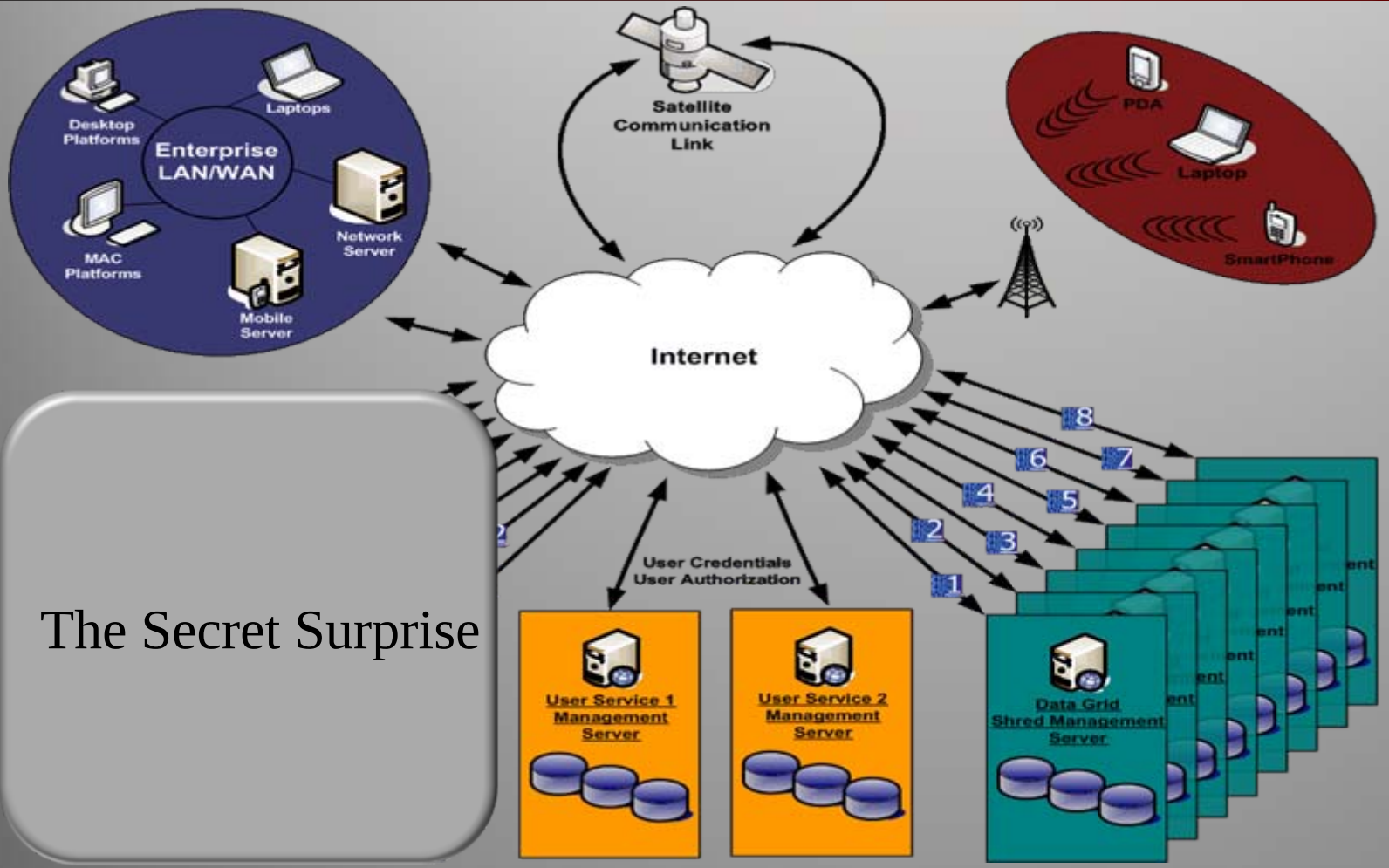
- Fully integrated into Windows Explorer
- Utilizes our proprietary “Shred and Stitch” and Constructive Key Management (CKM) technologies
- Accessible from public and private networks
- Supports individual to Enterprise user including secure collaboration, remote office and mobile data protection
- Product and SaaS solutions are available

How SecureNOW! Works



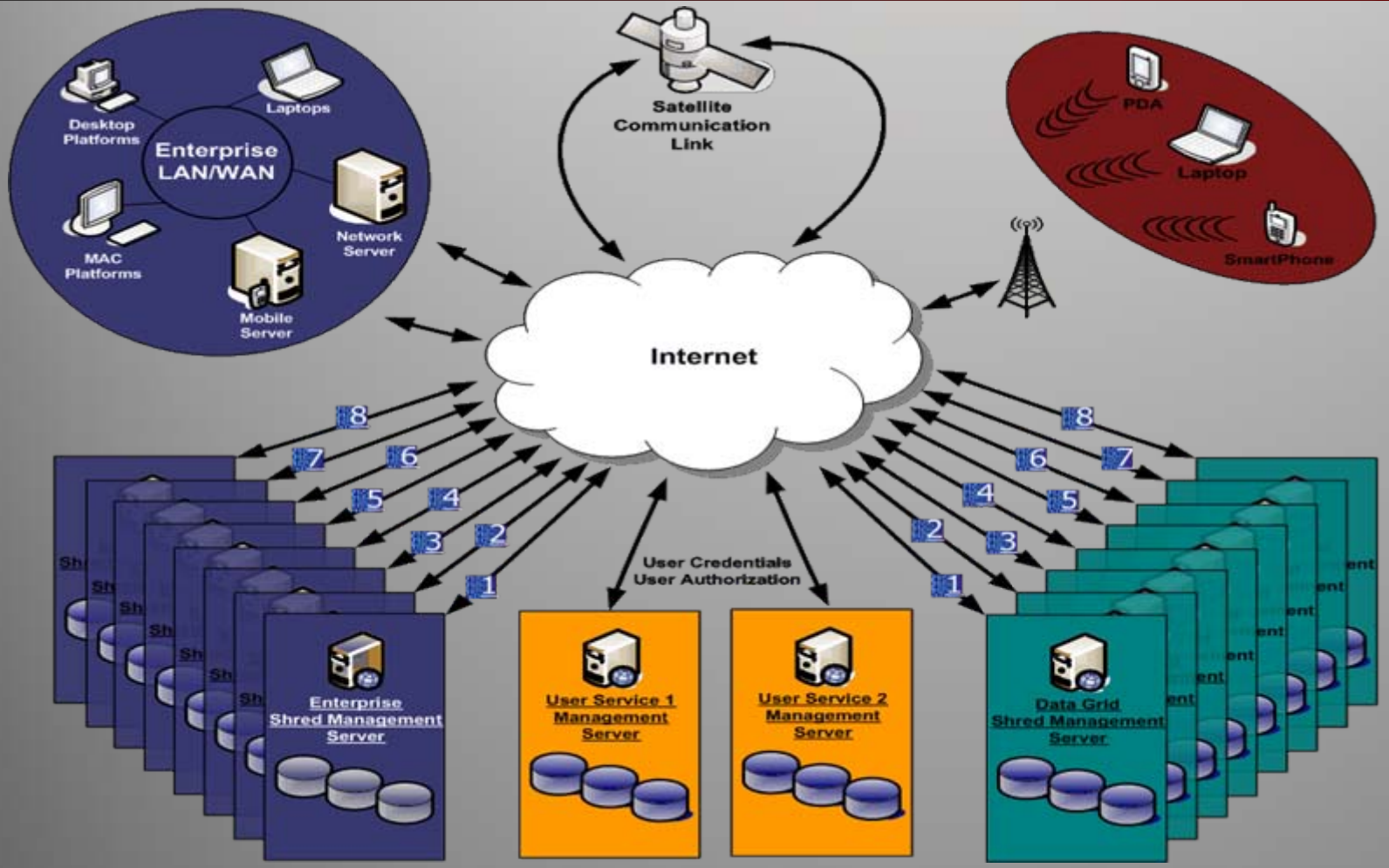


Opaque Data Cloud Architecture



The Secret Surprise

Opaque Data Cloud Architecture



Opaque Data Cloud

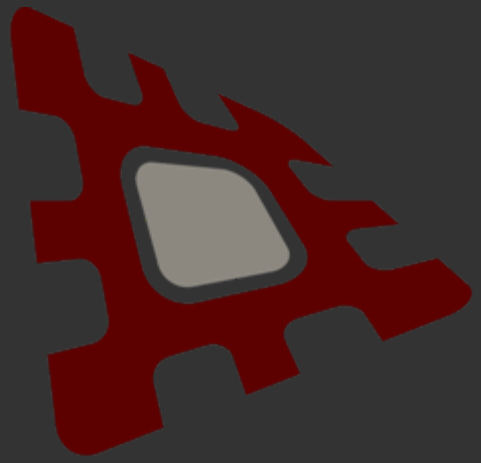
- **All data** in the cloud is
  - Unreadable
  - Spread across multiple datacenters; no meaningful data resides at a single location.
  - Immediately recoverable in the event of a catastrophic failure and is not impacted by weather, regional power outages, human error and subversive threats.
- **All data** is only available at the edge
  - Laptops
  - Desktops
  - Mobile Devices
- **All data** access is enforced cryptographically
  - Personal
  - Business
  - Community

Where Do You Go From Here?

- Below are some key areas of concern to ensure your IT department is aligned with your business requirements, and is able to recover critical applications and data when needed.
  - Can you identify critical applications?
  - Is your most important information recoverable in an acceptable “business window”?
  - Are you maximizing the utilization of your storage resources?
  - Are you using mirroring or replication to its greatest efficiency?
  - Do you know what is missing from your recovery process?
  - Have you tracked where all your data is by key process – and how you plan to retrieve it in the event of an emergency?
  - How do you handle data corruption vs. technology or environmental disruption?

Tips to Win The Battle

- Plan for one layer of your security controls to be bypassed
- Review and understand data retention rules.
- Conduct annual third-party security audits
- Employ need-to-know access
- Protect from the inside out
- Prioritize risks
- Encrypt-shred on-line content, stored content and backups



WHITENOISE

SYSTEMS