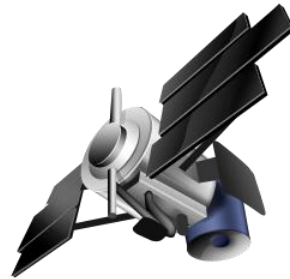
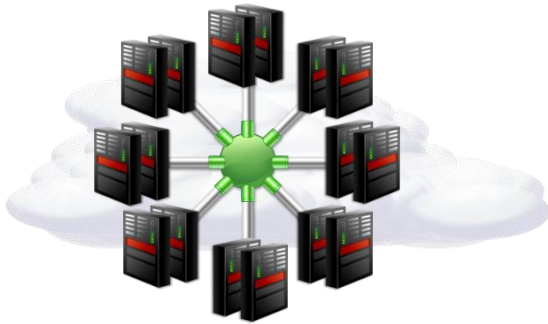




**– Absio Overview for Defense –**  
Information Distribution Control – Secure in Motion and on Devices

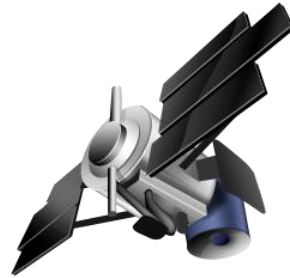
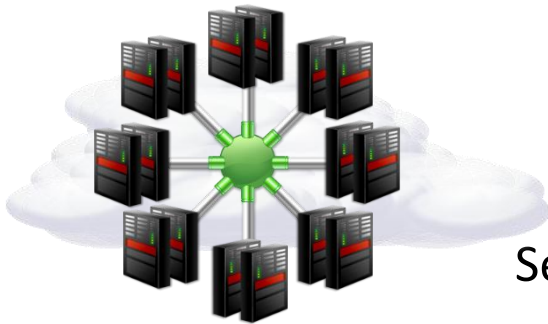
# Defense in Depth



You need to take your information to war.  
How can you protect it outside the wire?



# Defense in Depth



Absio Concert  
Secures your information in the field



# Information for the Warfighter Outside the Wire



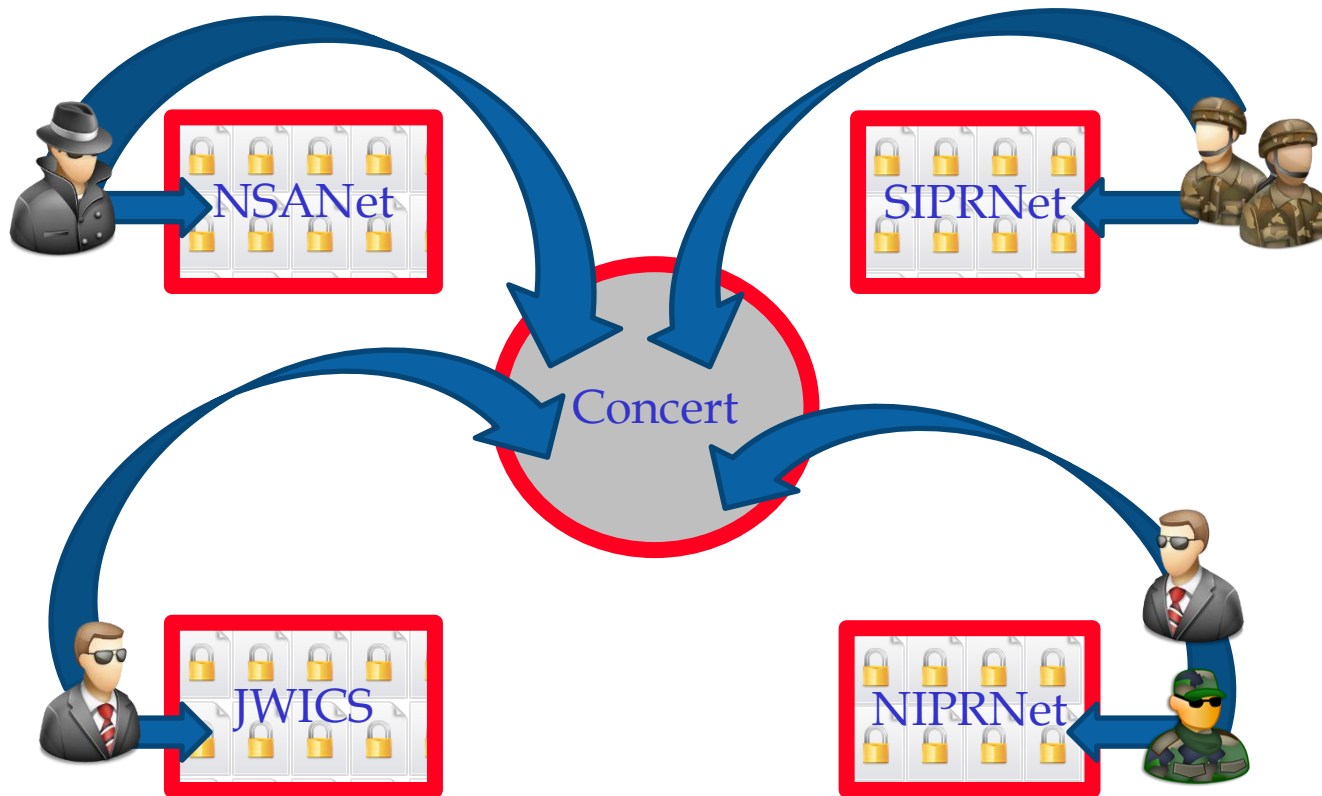
- Secure local store (information at rest)
- Secure transmission (information in movement)
- Information can be compartmentalized by user clearance, role, AOR, need to know...
- Works on smartphones, tablet, laptops, and specialized hardware
- Supports multi-factor authentication, duress passwords, honeypots, and expiration
- Fully functional in DIL environments
- EM Covert
- Rich and fast UI
- Secure synchronization between devices
- Secure storage and com can be “snapped in” to existing applications

# Working in Concert

---

- Concerts enable secure cross-domain information sharing without the need to grant cross domain access
- Concerts are easily created and administered intermediate logical networks
- Concerts do not require new hardware
- Concerts can inherit the security credentials of members from different domains
- Each Concert has its own security, distribution rules, and audit
- Templates simplify administration and user's experience
- Concerts enable rational, step-by step reduction in the number of networks

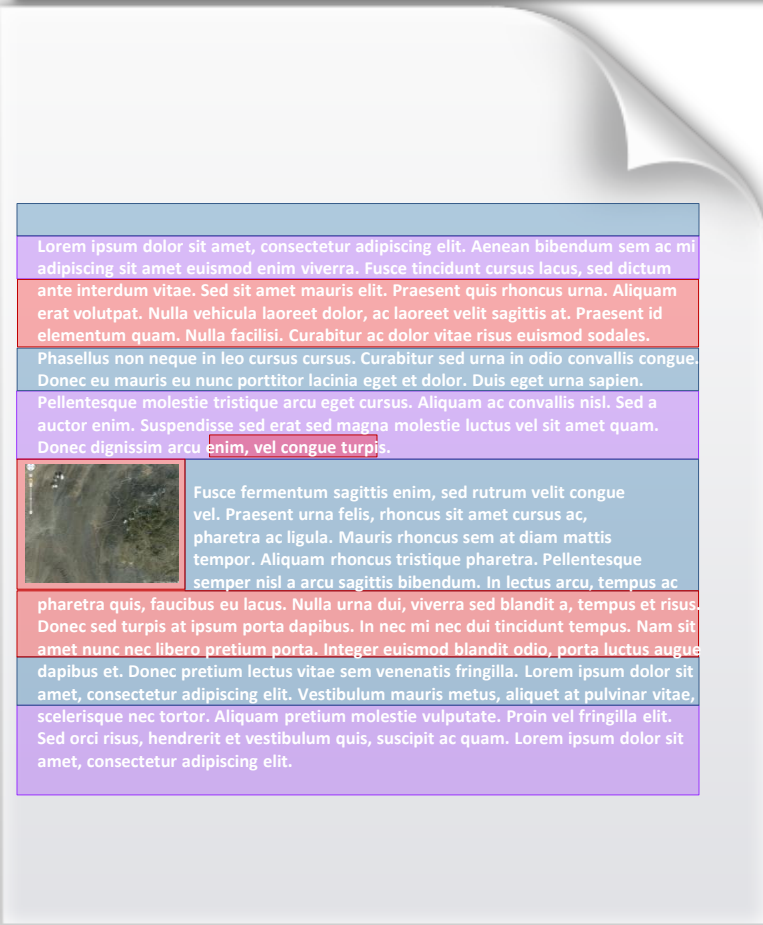
# Share Information, Not Access



# Auto-Redaction

## ■ Features:

- ❑ Higher security clearance overlays point to lower security overlays and base docs.
- ❑ Lower clearance overlays or base documents have no knowledge of higher clearance overlays
- ❑ Overlay structure and classifications can be created ad-hoc or from organizational templates.
- ❑ Redactions can be set to either visible/invisible in lower security documents/overlays



Unclassified

Secret

Top Secret

# Architecture Comparisons: Security Paradigm

---

## Current

- Perimeter security—control is located at the edge of the network
- Focus on outsider threat
- Access control grants access to unsecured objects
- Object security (if it exists) is disjoint from access control
- Limited secondary distribution control

## Absio

- Object level security—control is located in the information itself
- Focus on insider threat
- Access control security is integrated with object security and distribution control (Concert)
- Persistent Distribution Control

# Architecture Comparisons: Encryption

---

## Current

- Encryption is an exception
- Encryption management requires high user effort and compliance
- Encrypted with one or few keys
- Encryption algorithm is static

## Absio

- Encryption is universal
- Encryption requires little user involvement
- Encrypted with unique keys
- Encryption algorithm is configurable

# Architecture Comparisons: Authentication

---

## Current

- Many applications support anonymous access
- Ad hoc and/or limited authentication between the device, application, user and content
- Difficult to implement authentication

## Absio

- No application level anonymity
- Integrated authentication of users and applications
- Multiple methods of authentication are assumed in the architecture

# Architecture Comparisons: Availability

---

## Current

- Information is available only when connected to the secure network.
- Intolerant of disconnected, intermittent and low bandwidth environments
- Slow
- Primitive UI for many applications

## Absio

- Information is available on secure networks, unsecure networks (Internet) and offline
- Works in disconnected, intermittent and low bandwidth environments
- Fast
- Rich UI for all applications

# Architecture Comparisons: Operational Security

---

## Current

- Secure applications are too easy to identify
- Encrypted traffic is relatively easy to identify
- Assets are easy to exfiltrate
- Asset movement has little or no audit trail
- Captured devices often have sensitive data that's easy to extract

## Absio

- Secure operations embedded within a ubiquitous commercial application
- Encrypted traffic becomes the norm
- Assets are difficult to exfiltrate
- Asset movement is auditable
- Sensitive data is difficult to extract from captured devices

# Architecture Comparisons: Cross Domain Information Sharing

---

## Current

- May require an access device per network  
–and/or–
- Sharing requires cross domain connections
- Rights may not be sufficiently granular
- Access control only, no distribution control
- Insufficient auditability

## Absio

- Possibility of single access device
- Sharing does not require interconnected domains
- Rights are sufficiently granular
- Full distribution control
- Fully auditable

# Architecture Comparisons: Strategic Information Asset Management

---

## Current

- Information assets are poorly defined, making them difficult to find and organize—for humans or AI
- Provenance is easily lost or subverted
- Networks proliferate
- No auto-redaction for PII or security classifications

## Absio

- Information assets are well defined, making them easier for humans and AI to organize and find.
- Provenance is automatic and is not easily subverted
- The number of networks can be reduced
- Supports auto redaction for PII and security classification

# Architecture Comparisons: Costs

---

## Current

- Server based processing significantly increases network operating costs
- Securing the information against insider threats is difficult and expensive

## Absio

- Client processing dramatically reduces network build and operating costs
- Migrating information could be costly—but far less costly than the current effort to

# The Big Questions

---

**If you could snap your fingers and every security initiative you are working on today was completed....**

**Would your information be secure?**

**Would it be available when and where your people need it?**

### Absio Corporation Contact Information

Absio Corporation	Dan Kruger: CEO	Jim Hansen: Director, BD
8321 S. Sangre De Cristo Road Suite 302 Littleton, CO 80127-6426 <ul style="list-style-type: none"> <li>• Office: 720-981-2969</li> <li>• Fax: 303.736.4105</li> <li>• <a href="mailto:Inquiries@absio.com">Inquiries@absio.com</a></li> <li>• <a href="http://www.absio.com">www.absio.com</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="mailto:dan.kruger@absio.com">dan.kruger@absio.com</a></li> <li>• Cell: 303-910-7623</li> <li>• Office: 720-981-2969</li> <li>• Fax: 303.736.4105</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="mailto:jim.hanson@ip3corp.com">jim.hanson@ip3corp.com</a></li> <li>• Cell: 608-213-1702</li> <li>• Office: 720-981-2969</li> <li>• Fax: 303.736.4105</li> </ul>
Mitch Tanenbaum: CTO	Tim Anschutz: CMO	
<ul style="list-style-type: none"> <li>• <a href="mailto:mitch.tanenbaum@absio.com">mitch.tanenbaum@absio.com</a></li> <li>• Cell: 303-905-7169</li> <li>• Office: 720-981-2969</li> <li>• Fax: 303.736.4105</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="mailto:tim.anschutz@absio.com">tim.anschutz@absio.com</a></li> <li>• Cell: 720-879-4930</li> <li>• Office: 720-981-2969</li> <li>• Fax: 303.736.4105</li> </ul>	

### Absio Corporation Commercial Software License and Services Agreement (“SLSA”)

The Absio Corporation software is provided pursuant to Absio’s commercial Software License and Services Agreement (“SLSA”). Any Absio software acquired with United States Federal Government funds or intended for use within, by, or for any United States federal agency are provided as “Commercial Computer Software” as defined in DFARS 252.227-7014, and “Restricted Computer Software” as defined in FAR 52.227-14, Rights in Data-General, including Alternate III, as applicable, with “Limited Rights,” in accordance with the SLSA’s terms and conditions. Absio must be notified in advance of any license grants to United States Federal Governmental entities.