ProFile Eclipse Cloud
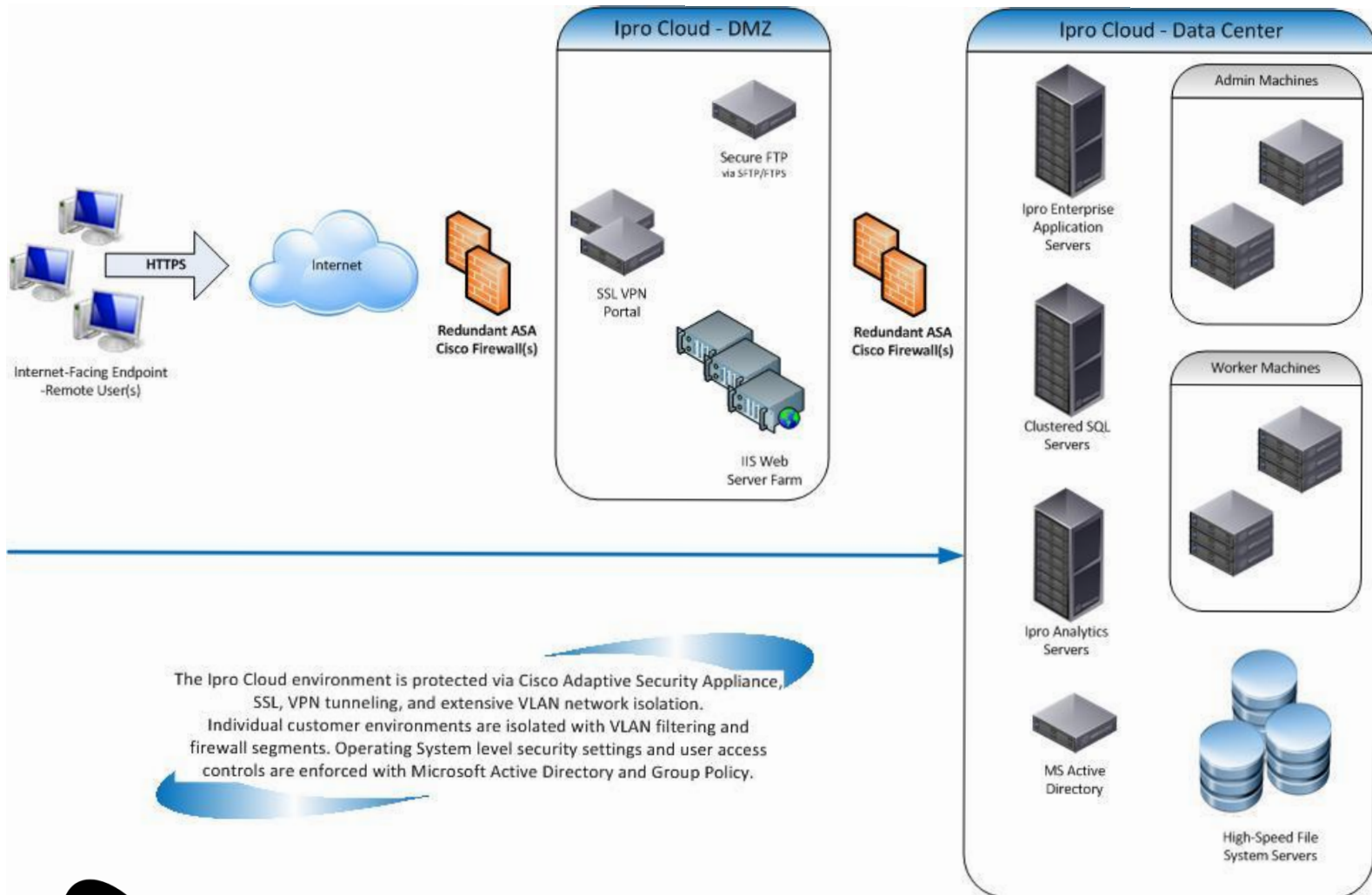
▸ The Ipro Cloud is an innovative service that allows law firms, corporate legal departments and application Services Providers to leverage a highly advanced IT infrastructure and support team to help capital investments and overall costs associated with ingesting, analyzing, reporting, processing, reviewing, producing and storing litigation related data by providing flexible access to Ipro's powerful Enterprise applications for on-demand or annual usage. Pay for what you need, when you need it, and we manage the rest.

▸ The Ipro Cloud is delivered in multiple models:

1. SaaS (Software as a Service) – Subscription based pricing
   - On-Demand usage of Ipro's Enterprise applications on a project or case basis
   - Time based contract (annual, monthly, weekly, daily)
2. SaaS (Software as a Service) – Per GB based pricing
   - On-Demand usage of Ipro's Enterprise applications on a project or case basis
   - Contract based on data ingested, processed and/or hosted
3. IaaS (Infrastructure as a Service)
   - Annual agreement to leverage Ipro's Infrastructure as a Service
   - Allocation of all required systems to host your subscribed software applications

Ipro Cloud Conceptual Architecture

The Ipro Cloud environment is protected via Cisco Adaptive Security Appliance, SSL, VPN tunneling, and extensive VLAN network isolation. Individual customer environments are isolated with VLAN filtering and firewall segments. Operating System level security settings and user access controls are enforced with Microsoft Active Directory and Group Policy.

Redundant Network Components

▸ Multiple WAN Connections

▸ Enterprise Firewall in Automatic Failover

▸ Load Balanced / Automatic Failover SaaS Portal Web Servers

▸ Load Balanced / Automatic Failover SaaS Gateway Servers

▸ Load Balanced / Automatic Failover SQL Servers

▸ Load Balanced / Automatic Failover IIS Servers

▸ Fully redundant 10Gb back-bone network

▸ Multiple redundant (multi-head) storage systems

▸ Backups using Grandfather-Father-Son Snapshot rotation

Ipro Security - Intrusion Prevention

Cisco ASA

▸ Redundant Cisco ASA firewalls with IPS (Intrusion Prevention System) are used to prevent unauthorized access to our internal or customer networks. Users do not connect directly to the firewall but utilize an additional SSL VPN system located in a DMZ. The internal network is split up into multiple VLANs and DMZs to isolate client environments to specific servers.

Ipro Cloud Portal/Terminal Service Gateway

▸ In order for clients to access the Ipro Cloud environment, they must successfully authenticate over SSL with their own unique username and password to the Ipro Cloud Portal. Then if their individual accounts have been granted access by your own account administrator, Application Links will be provided that use a Terminal Service Gateway infrastructure to establish remote desktop (RDP) connections to the specific application servers. The Ipro Cloud Portal is hosted in a DMZ and has limited access to our internal network. To maximize security, access to the eCapture environment workers are not exposed to the end user via the Application Links.

Ipro Security - Internal Data Security

Active Directory

Clients who gain access to our network through the SSL VPN are restricted to just their companies specific servers. These servers have Group Policies applied so that clients that connect are limited to the changes they can make, files they can access and programs they can run. Once again users have to be in specific groups to gain access to these servers.

SAN/NAS

Unique shares are created for each Customer and security is set based on RBAC (Role Based Access Control) using Active Directory group membership. All users need to be members of their companies group to view client data. Customers cannot see or gain access to other customer's data.

Physical Media

▸ Media sent to our secure Ipro Cloud datacenter is photographed when received and audited with all Chain of Custody documentation and forms maintained throughout the process

▸ Media sent to the Ipro Cloud datacenter should not be the original or only copy. Whether you receive multiple copies and choose to send one of those to us or create the copies yourself, it is important to always have an original copy. Take due diligence to ensure any copies that you make are forensically sound and do not alter the metadata of the original files.

▸ It is also recommended that when sending a package that contains evidence on physical media that the package include a letter documenting the serial # or barcode # of each piece of hardware in the shipment. This enables the recipient to verify the contents are complete. As mentioned in the previous section any Chain of Custody documents should also be kept with the physical media at all times and included in the shipped package.

▸ When shipping data, it is recommended to use shipping companies with end to end tracking systems like FedEx or UPS. If the shipment is very sensitive, a bonded carrier may be necessary.

FTP Transfers

▸ A secure FTP transfer connection is offered as part of the Ipro Cloud and can be used for smaller data sets. It is advised that you compress your files into .ZIP or .RAR format prior to uploading and should preserve metadata.

▸ When you are ready to download your data from the storage system you can use the WinRAR utility provided to compress prior to transfer.
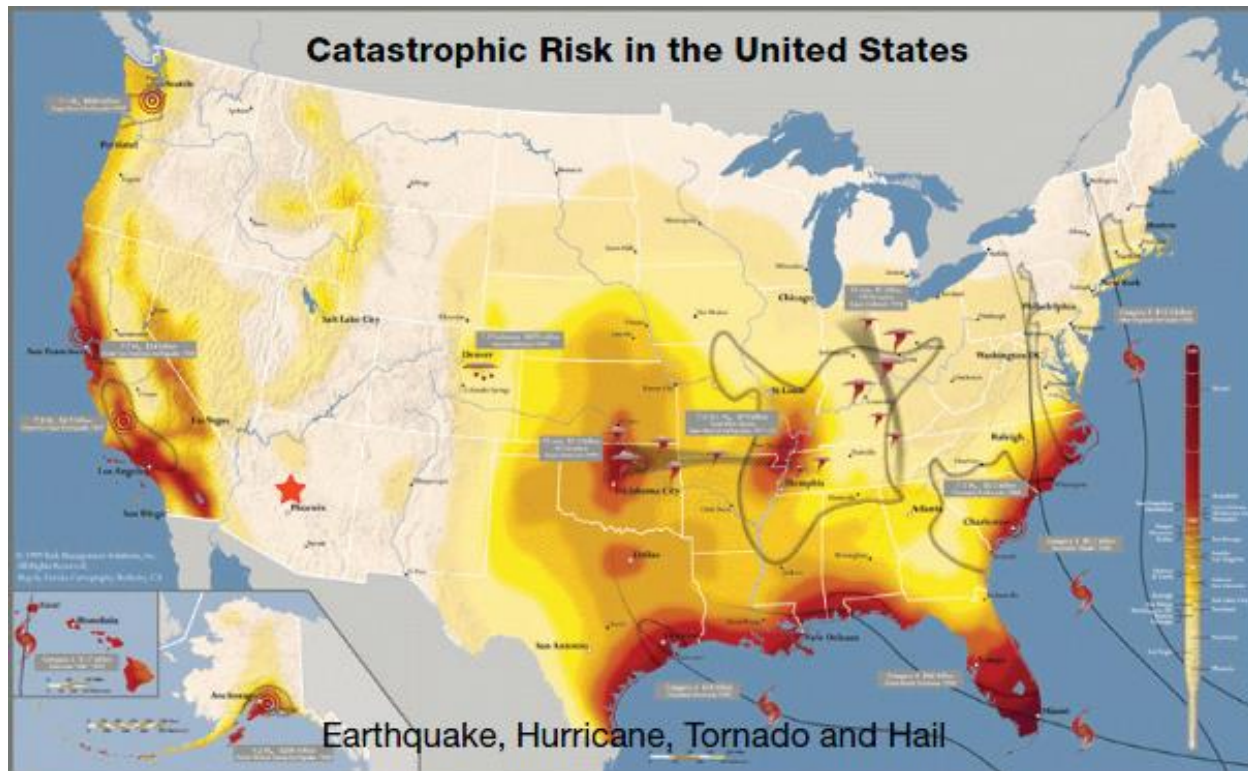
Ipro Cloud - Data Center Details

DEFINITION:

A **Data Center** is a facility used to house computer systems and associated components. It includes redundant power supplies, communication connections, environmental controls, and special security devices.

Where IT Lives™

Ipro Cloud Location

▸ Ipro's Data Center is within the Phoenix/Metro area. The Phoenix climate and geography form a highly stable environment for data center operations. Ranked consistently in the top 5 for cities with least risk.

◦ Area free of natural disasters

◦ No 'mega city' political risks

◦ Compelling power and utility infrastructure

Ipro Cloud - Data Center Details

Security

- SSAE 16 Type II
- Security System: State-of-the-art access control system with CCTV
- Biometric Security: Iris
- 24x7x365 Security: Yes
- 24x7x365 Operational Staff: Yes

Redundancy

- The Data Center is capable of 100% uptime for power and communications systems
- Multiple backup generators with onsite fuel storage
- Redundant cooling systems for stable environment
- Multiple fiber carriers for redundant Internet connectivity

Power Systems

- Utility: Arizona Public Service
- Core Power: 12 Mw(redundant dedicated feeders) with ability to further upgrade to 24Mw
- Power Conditioning: 9.4 Mw of UPS
- Power Backup Batteries: VRLA - 5 minutes of runtime at 100% load
- Power Backup Generators: Two (2) 1.75 Mw and two (2) 2.00 Mw Caterpillar Generators
- Fuel Storage: 8500 gallons

Ipro Cloud - Data Center Details

Cooling Systems

- Cooling: Fully redundant chilled water plant with
- Stulz Air Handlers
- Piping: Welded bi-directional design for redundancy and maintenance
- Humidification: Ultrasonic, ultra clean water
- Water Treatment System: RODI
- Backup Water System: 8000 gallon storage facility on site
- Leak Detection: Rope style throughout data centers

Telecommunications

- Core Fiber: Multiple redundant/diverse paths
- Fiber: Multiple carrier options including Cox, Qwest and AT&T
- Facilities: Carrier neutral

Fire/Security

- Fire Suppression: Interlocked pre-action dry pipe with VESDA (Very Early Smoke Detection Alarm)