Abacus Private Cloud Security

Securely access all your sensitive data and vital applications from anywhere, anytime.

APC puts your critical practice data and vital applications into a Compliance-Ready private virtual workspace, while removing IT management burdens and costs and maximizing your organization's performance.

Optional intro

AbacusNext was founded in 1983 and provides mission critical, compliance-ready, fully integrated and cloud-enabled technology solutions to the legal, accounting, banking and insurance sectors.

The center piece of AbacusNext's products and services portfolio is Abacus Private Cloud (APC)-a fully integrated private cloud ecosystem that combines desktop-as-a-service, fully managed IT, and full spectrum cybersecurity with strict regulatory compliance and 24x7 technical support. APC is the center of their clients' technology universe, creating a secure digital workspace that's software agnostic and that seamlessly integrates the firm's mission critical applications and data so they're accessible anywhere, anytime, from any device.

SECURITY

AbacusNext's APC is designed to provide a secure private environment for customers to store and access a wide variety of customer data. Built into APC as the default services is a robust suite of security services and compliance policies, such as two-factor authentication, single sign-on, five tiers of physical, network and data security, information handling and data privacy protocols all in accordance with NIST standards. By default, your data copied to geographically redundant data centers. All the services from the data floor to user access controls is audited and managed to the SOC 2 Type 2 compliance standards to ensure your business safe and protected 24 x 7.

- IPS/IDS – Intrusion Prevention Services / Intrusion Detection Services

- Access to the environment with RDP TLS 1.2 – Encrypted connections
- Client Data Encryption at rest using 256bit AES
- PaaS Database Encryption with 256bit AES
- Sophos A.V.
  - Tamper Protection
  - DCP
  - AV Lockdown
- Sophos Intercept X (Ransomware)
- 2 Factor Authentication
  Multi-factor Authentication
- DDOS Protection
- Ongoing Penetration Testing Management
- Vulnerability Management using CVSS
- Operating System & App Patch Management
- Dedicated Logging and Monitoring

INFRASTRUCTURE REDUNDANCY

AbacusNext is the owner and operator of its own computing and storage infrastructure used for APC giving us full control and insight to need any client requirement. AbacusNext has designed, built, and optimized APC for the specific needs of our industry professionals and the software utilized in these industries. This includes all AbacusNext Software and 3rd party software. All audited and managed to the SOC 2 Type 2 compliance standards.

AbacusNext operates out of a variety of geographically dispersed data centers across three countries. Locations are setup in a Primary/Secondary configuration to ensure Disaster Recovery objectives are met. The physical components encompassing the APC ecosystem include multiple data center facilities, enterprise computing and storage infrastructure, Cisco networking equipment, and Unified Threat Management (UTM) firewalls.

Abacus Private Cloud Security

AbacusNext has designed and built computing farms that consist of many servers clustered together for high-availability and no single point of failure. Virtual computing technologies are utilized for the virtual servers and virtual storage area networks (SAN). This provides the flexibility to move customers environments if there is a problem with the physical hardware or when it's time to upgrade.

- Compute clusters N+1
- Storage clusters 2N
- All communication fabrics are 2N (including EDGE firewalls)
- *Owner/Operator of APC
- Dedicated WAN IP
- Dedicated Firewalls

COMPLIANCE

AbacusNext is one of the only companies to provide **enforced compliance** all the way to the user level. AbacusNext and all the Abacus Private Cloud services and support is SOC 2 Type 2 compliant and audited by CoalFire Controls. AbacusNext will maintain at all times enterprise-class security and standards protecting its Abacus Private Cloud ecosystem located in the United States, Canada, and the United Kingdom. While most cloud and software provide have a shared security and compliance standard, that means you, and your staff are ultimately responsible for the secure design, upkeep, and enforcement 24 x 7. Not only is APC providing a secure and compliant service. APC is fully compliance, managed 24 x 7, and **enforcing compliance** by including and providing system administration management at the systems level and all the way to the users level. This level of compliance is not common in the industry but given most of customer are in the highest regulated industries we made the investment to take compliance to the highest level.

AbacusNext Certifications

- SOC2 Type 2
- ISO 27001 in process

Data Center Certifications

- SOC1 Type 2
- SOC2 Type 2
- SOC3
- MPAA
- PCI DSS - AOC
- PCI DSS – ROC
- ISO IEC 27001
- HIPAA Type 1
- Schellman confirmation of Engagement HIPAA Attestation

MANAGEMENT

TECHNICAL SUPPORT STAFF and EXPERTISE

AbacusNext APC operations are the combined and coordinated effort of the System & Networking Engineering, Pre-Sales, Implementation, and Support teams. These teams consist of:

DATA PROTECTION

AbacusNext's APC is designed to provide a secure location for customers to store and access a wide variety of customer data from any desired location securely. Customers determine the nature and extent of the data that will be stored in APC. Likewise, customer's decide what users should have access to APC, as well as access to certain classifications of data once stored in APC. Additionally, APC included fully managed backups consisting of the following:

1. A dedicated team manages data backups 24 x 7. The APC support teams consist of individual teams focused on specific disciplines. The APC backup team manage and monitor the backup environment providing around the

clock protection and access to your data.

2. All data is encrypted with 256-bit encryption that uses a 256-bit key to encrypt and decrypt backup data or files. It is the most secure encryption standard.
3. 3-2-1 Backup Rule: By default, APC includes 3-2-1 backups that include;
    a. Three (3) copies of your data:
        1) Production data
        2) Backup at the primary data center
        3) Backup replication to geographic diverse data center.
    b. Two (2) backup copies on different storage media
    c. One (1) of them located offsite (secondary data center)

APC System & Networking Engineering

This department encompasses Network, Virtualization, Automation, Identity, Data Protection and other specialized Systems Engineers that support the underlying APC platform. This department acts as an escalation point for all other APC operational departments and provides 24/7/365 mission critical coverage to ensure the maintenance of service level commitments.

APC Pre-Sales Engineering

Pre-Sales Engineers work with prospective clients to understand the technical needs of their business and design APC solutions that are tailored to meet them. Engineers will do a full technical assessment of your current environment at no cost to you. The technical assessment will provide a full report of computing environment and health which includes the following:

1. A full security assessment with your security vulnerability scope and corrective actions
2. Full inventory of your current computing, storage space,
3. Full inventory of your operating systems and all application.

Engineers on this team coordinate closely with the clients account representative and subsequent implementation project manager and team, to ensure clients APC solution and subsequent deployment are aligned at all

phases.

APC Implementation Engineering

The implementation engineering team is directly responsible for the onboarding of new clients to the APC environment. This includes configuration of user access and roles, data migration (subject to an additional fee for complex migrations), application deployment, device integration and post migration support.

- Dedicated Logging
- Dedicated Monitoring
- Dedicated Identity Management Solutions
- Company-wide 2 Factor Authentication when accessing client environments Multi-factor Authentication
- Single Sign On (SSO)
- Global Support
- Technical Account Manager (TAM)

TECHNICAL INDEX

SECURITY

- **IPS/IDS Intrusion Prevention/Detection Services -** IDS (Intrusion Detection System) are systems that detect activities that are inappropriate, incorrect or anomalous in a network and report them. Furthermore, IDS can be used to detect whether a network or a server is experiencing an unauthorized intrusion. IPS (Intrusion Prevention System) is a system that actively disconnects connections or drops packets, if they contain unauthorized data. IPS can be seen as an extension of IDS.
- **RDP TLS 1.2 -** Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

Abacus Private Cloud Security

- **256 bit AES encryption at rest** - is a data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files. It is one of the most secure encryption methods after 128- and 192-bit encryption, and is used in most modern encryption algorithms, protocols and technologies
- **PaaS Database Encryption -** Platform as a Service (PaaS) is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app. Database encryption can generally be defined as a process that uses an algorithm to transform data stored in a database into "cipher text" that is incomprehensible without first being decrypted.
- **Sophos Anti-Virus -** Sophos Anti-Virus is the virus protection software recommended by MIT. This software detects and cleans up viruses, Trojans, worms, spyware, adware and other potentially unwanted applications.
    - **Tamper Protection -** Tamper Protection is a new setting from Windows Defender Antivirus, available in the Windows Security app, which when on, provides additional protections against changes to key security features, including limiting changes which are not made directly through the Windows Security app.
    - **DCP -** Here is an explanation of what this means exactly, and how it's beneficial to any organization, etc... blah blah blah.**?**
    - **AV Lockdown -** Here is an explanation of what this means exactly, and how it's beneficial to any organization, etc... blah blah blah.
- **Sophos Intercept X (Ransomware) -** Intercept runs as a standalone agent, alongside your existing antivirus or combined with Sophos Endpoint Protection. Intercept X gives you next-generation anti-exploit, deep learning malware detection, anti-ransomware, root cause analysis, and advanced system clean technology.
- **2 Factor Authentication / Multi-Factor Authentication -** Two-factor authentication (also known as 2FA) is a type, or subset, of multi-factor authentication. It is a method of confirming users' claimed identities by using a combination of *two* different factors: 1) something they know, 2) something they have, or 3) something they are. A good example of two-factor authentication is the withdrawing of money from an ATM; only the correct combination of a bank card (something the user possesses) and a PIN (something the user knows) allows the transaction to be carried

out. Two other examples are to supplement a user-controlled password with a one-time password (OTP) or code generated or received by an authenticator (e.g. a security token or smartphone) that only the user possesses.

- **DDOS Protection -** DDoS is short for Distributed Denial of Service. DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.
- **Penetration Testing -** A penetration test, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. The test is performed to identify both weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.
- **Vulnerability Management using CVSS -** The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.
- **OS & App Patch Management -** Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system.
- **Dedicated Logging and Monitoring -** Security event logging and monitoring is a process that organizations perform by examining electronic audit logs for indications that unauthorized security-related activities have been attempted or performed on a system or application that processes, transmits or stores confidential information.

INFRASTRUCTURE

- **Computer Clusters N+1 -** Clusters are usually deployed to improve performance and availability over that of a single computer, while typically being much more cost-effective than single computers of comparable speed or availability. N+1 redundancy is a form of resilience that ensures system availability in the event of component failure. Components (N) have at least one independent backup component (+1).

- **Storage Clusters 2N -** Here is an explanation of what this means exactly, and how it's beneficial to any organization, etc... blah blah blah.
- ***Owner/Operator of APC -** Here is an explanation of what this means exactly, and how it's beneficial to any organization, etc... blah blah blah.
- **Dedicated WAN IP -** A wide area network (WAN) is a telecommunications network that extends over a large geographical area for the primary purpose of computer networking. Wide area networks are often established with leased telecommunication circuits. Business, as well as education and government entities use wide area networks to relay data to staff, students, clients, buyers, and suppliers from various locations across the world. In essence, this mode of telecommunication allows a business to effectively carry out its daily function regardless of location.
The Internet may be considered a WAN. An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
- **Dedicated Firewalls -** In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

COMPLIANCE

- **AbacusNext Certifications -** Here is an explanation of what this means exactly, and how it's beneficial to any organization, etc... blah blah blah.
    - **SOC2 Type2 -** A SOC 2 audit, or Service Organization Control 2, is an audit of a service organization's non-financial reporting controls as they relate to the Trust Services Criteria – the security, availability, processing integrity, confidentiality, and privacy of a system.
    - **ISO 27001 -** ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

- **Data Center Certifications -** Here is an explanation of what this means exactly, and how it's beneficial to any organization, etc... blah blah blah.
  - **SOC1 -** A SOC 1 Report (System and Organization Controls Report) is a report on Controls at a Service Organization which are relevant to user entities' internal control over financial reporting.
  - **SOC2 Type2 – Data Center -** A SOC 2 audit, or Service Organization Control 2, is an audit of a service organization's non-financial reporting controls as they relate to the Trust Services Criteria – the security, availability, processing integrity, confidentiality, and privacy of a system.
  - **SOC3 -** A Service Organization Control 3 (Soc 3) report outlines information related to a service organization's internal controls for security, availability, processing integrity, confidentiality or privacy. These five areas are the focuses of the AICPA Trust Services Principles and Criteria.

MANAGEMENT

- **Dedicated Logging -** A security log is used to track security-related information on a computer system.
- **Dedicated Monitoring -** A system monitor is a hardware or software component used to monitor system resources and performance in a computer system.
- **Dedicated Identity Management Solutions -** Identity management (IdM) describes the management of individual identities, their authentication, authorization, roles and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks.
- **Company-wide 2 Factor Authentication/MFA -** A good example of two-factor authentication is the withdrawing of money from an ATM; only the correct combination of a bank card (something the user possesses) and a PIN (something the user knows) allows the transaction to be carried out. Two other examples are to supplement a user-controlled password with a one-time password (OTP) or code

generated or received by an authenticator (e.g. a security token or smartphone) that only the user possesses.

- **Single Sign On (SSO) -** Single sign-on (SSO) is a property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to any of several related systems.
- **Global Support -** Here is an explanation of what this means exactly, and how it's beneficial to any organization, etc... blah blah blah.
- **Technical Account Manager (TAM) –** A TAM works closely with the sales and business account management team to win new business (presales as well, RFPs and technical proposals) and maybe increase current business value with existing customers. and strengthen customer relationships. A TAM does at least a subset of the following:

  - Provide guidance and advice as a subject matter
  - Provide top-quality technical service before and after a sale
  - Conceive, design and develop or oversee innovative solutions for clients
  - Discovery and elicitation of needs
  - Engage with customer support and ensure client satisfaction and strengthen ties with customers
  - Engage in product management and / or roadmaps
  - Manage engagements
  - Travel to visit customers
  - Risk management, proactive anticipation
  - Future strategies and tech roadmaps