ICE
TRUSTED IT PARTNER

ICE'S ULTIMATE GUIDE TO

PROTECTING A BIOTECH STARTUP

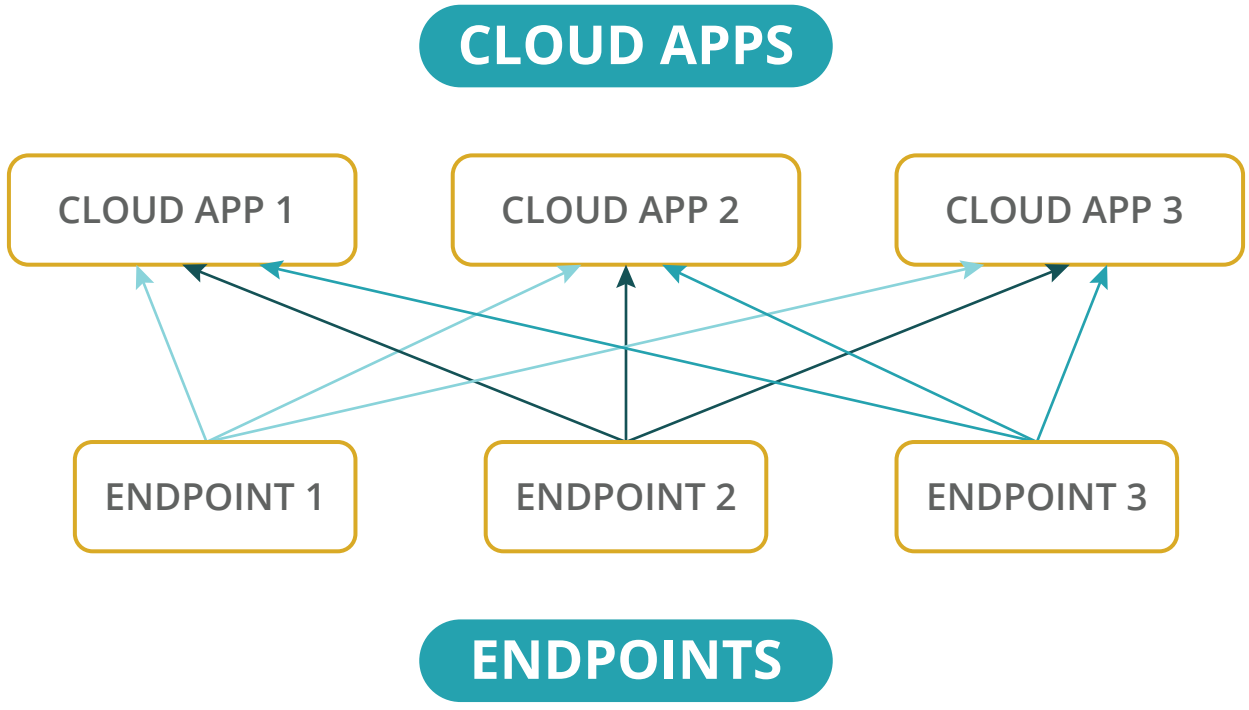
THE IMPORTANCE OF A SECURE CLOUD IT INFRASTRUCTURE

The rise of cloud technology has streamlined IT infrastructures for many startups, often comprising just a few endpoints (such as notebooks, desktops, lab systems, and mobile devices) and a handful of cloud applications for data storage and computing. Gone are the days of setting up extensive on-premises IT systems. Additionally, most startups operate from shared spaces like incubators, labs, or university facilities, reducing the need to build their own IT foundations.

Therefore, many companies overlook investing in their own cybersecurity, assuming these providers are responsible for it. This misconception poses significant risks, as IBM revealed that 82% of data breaches in 2023 involved data being stored in public and private cloud solutions.

Cybercriminals don't breach cloud providers to access stored data; instead, they exploit your unprotected endpoints to infiltrate your cloud applications.

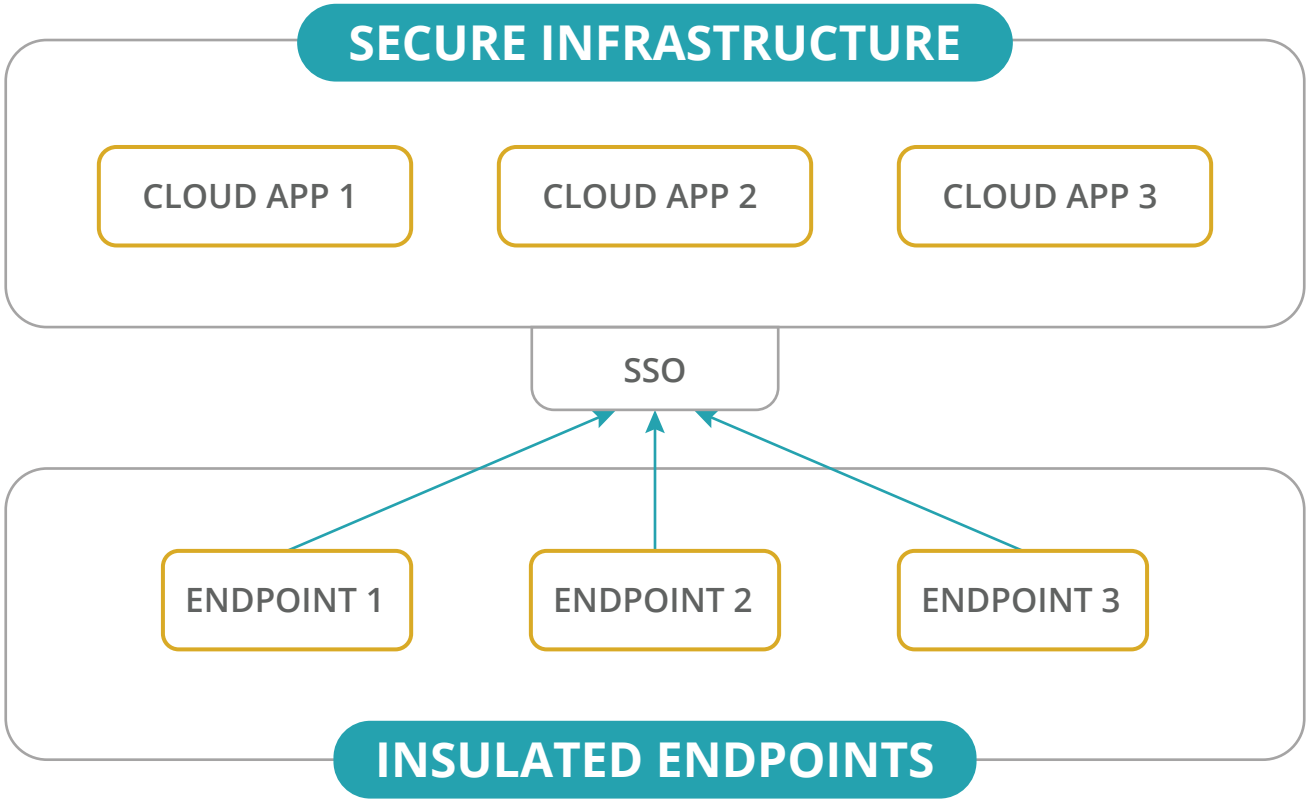
Illustrated below is the common setup utilized by most startups: a few endpoints through which users autonomously connect to a selection of public or private cloud applications.



Such configurations leave you vulnerable in multiple ways. As previously stated, hackers target not the cloud providers, but rather your users' endpoints. Typically, users log into each cloud application individually, requiring them to remember multiple passwords. This frequently leads to the use of easily recallable, weak passwords, inadvertently assisting hackers in their malicious activities.

Many endpoints primarily rely on basic antivirus software, which merely alerts users to recognized viruses. However, these solutions are vulnerable to cybercriminals who can easily evade detection. They lack the capacity to counter or confine cyber threats, whether a device is compromised remotely, lost, or stolen. Detecting their intrusion aftermath without adequate solutions in place proves highly arduous, often recognized only after it's too late.

Here is an illustration of a secure cloud-based IT infrastructure that protects all your user's endpoints and governs how you interact with the various cloud applications you utilize.



The protective shield encompassing the endpoints and cloud applications is forged through the collaborative efforts of various security solutions.

What exactly are these solutions and how do they work to insulate your infrastructure effectively?

PROTECTING ACCESS TO YOUR DATA & CLOUD APPS

#1

Single-Sign On

We highly recommend integrating a cloud-based Single Sign-On (SSO) application with industry-standard SAML authentication. This solution allows every user to access your suite of cloud applications with a single sign-in, eliminating the need to remember numerous passwords. By using robust passwords for each app, it enhances security measures and reduces vulnerabilities.
The implementation also includes feature-rich dashboards and a comprehensive security package to fortify application security. Simplify onboarding and offboarding processes while enhancing security by adopting this approach. Additionally, we will set up multi-factor authentication (MFA) for an added layer of security.

#2

Deploy universal directory services as a centralized identity management solution

Implementing Single Sign-On (SSO) necessitates a centralized identity management solution that oversees user management, password security, group organization, and system security.
By integrating an Identity Management solution, you can securely regulate access to all resources through centralized permission management, dictating user's resource accessibility.

#3

Configure Secure FIle sharing

Many startups share information externally or with remote collaborators using public cloud applications, insecure connections, or email, making interception easy. Therefore, it is crucial to establish a secure file-sharing solution protected by your Single Sign-On (SSO) barrier to ensure confidentiality.

#4

Deploy group policies such as Password Policy

Efficiently set up and apply various group policies, covering password rules, account lockout policies, and additional configurations.

ICE TRUSTED IT PARTNER
888-423-4801
www.iceconsulting.com
info@iceconsulting.com

PROTECTING YOUR ENDPOINTS

#5

Mobile Device Management

MDM enables automated control and robust security of administrative policies on various devices connected to an organization's network, including laptops, smartphones, and tablets. In case of a compromised, lost, or stolen device, quick quarantine measures are implemented to prevent unauthorized access to applications and networks.

#6

Deploy Centralized Endpoint Detection & Response

EDR has supplanted antiquated antivirus software, delivering robust protection for company data and users' computers through the implementation of continuous, centralized, AI-driven detection and response endpoint security. This cutting-edge solution not only identifies breaches but also promptly takes measures to nullify the threat.

#7

Deploy Endpoint Encryption

Endpoint encryption involves utilizing advanced mathematical functions to encrypt data stored on a hard drive. Data within an encrypted hard drive remains unreadable to individuals lacking the necessary key or password. This robust approach shields your systems from unauthorized physical access to the data residing on such devices.

#8

Deploy Centralized managed Endpoint Backup

Safeguarding your data from potential loss is paramount, with an enterprise-grade endpoint backup system acting as the cornerstone. By implementing a robust backup solution, all your devices can be shielded, enabling swift recovery whenever needed. This solution seamlessly captures and archives every version of each file across all your computers, leaving no data exposed. Whether through continuous or scheduled backups, the system ensures your files' integrity, preventing any corruption or loss. Trust in this reliable solution to consistently fortify the security of your data.

#9

Implement email security

Ensuring strong email security is vital to protect your inboxes from malware, phishing, and spam. It sets the benchmark for mailbox security. Proactively enhance security by setting up and configuring an email protection system to block spam, phishing, and malware effectively from reaching users' inboxes.

THE IMPORTANCE OF CYBERSECURITY IN THE LIFE SCIENCES

Life science startups rely on consistent funding, attracting significant media attention and making it a prime target for cyber attacks. According to Accenture, life science organizations are projected to suffer a staggering $657 billion loss due to direct cyber attacks within the next four years. IBM's data breach report reveals an alarming trend: 43% of data breaches in 2023 targeted small businesses. Irrespective of their size, every company operating in this industry should consider the aforementioned solutions as essential for their operations.

Implementing these solutions has become remarkably cost-effective. With a range of options providing a comprehensive suite, the initial costs are minimal, averaging around $15 per user. These IT frameworks comprise enterprise solutions tailored to expand seamlessly with business growth. A sturdy foundation ensures effective progression as your company scales up or operational needs change.

Curious about the solutions that align with your needs? Connect with us today, and we'll expertly steer you towards the ideal options for your organization. We'll also provide a comprehensive view of the necessary investment to elevate your security measures.

CALL OR EMAIL TODAY TO SCHEDULE A FREE CONSULTATION

ICE
TRUSTED IT PARTNER

888-423-4801
info@iceconsulting.com