Zscaler™

Compliance enabler for Indian banks

Contents

zscaler™

Cloud vs. security or cloud and security

The inevitable march of cloud adoption has often been held up at the barrier of security. A conversation with any Bank's business or IT heads invariably turns to how the CISO isn't keen to allow cloud adoption to happen. While the CISOs do have valid reasons for their objections, how feasible is it going to be for them to continue delaying the inevitable?

For sure, no security professional would advocate blindly adopting the cloud without the necessary due diligence and security controls. Yet a blanket ban on cloud adoption for even the largest financial institutions is no longer possible. With the flood of asset-light, service-heavy business models that are becoming far more successful than traditional businesses, it is important for Banks to look at cloud services positively. Disruption will not come from once-in-a-decade upgrades to the monolithic core banking systems, but rather from born-in-the-cloud, API-driven innovations.

Regulatory viewpoint

Regulatory clarity in this regard is important. Let's look at what the Reserve Bank of India – the Banking sector regulator in India has to say. The RBI has never banned the use of cloud computing. In fact, the RBI's technology arm – the Institute for Development and Research in Banking Technology (IDRBT), released a Cloud Security Framework outlining how Banks should adopt cloud computing in 2013. Going even further, the IDRBT established the Centre for Cloud Computing with the background note stating that:

Cloud Computing is attracting everyone's attention, right from service providers to businesses and government, as a means of cost effective provisioning of IT resources. Cloud computing can provide broad capabilities that banks need on a flexible basis to help them do much more than cut infrastructure costs. Cloud computing helps banks to transform their business processes and enhance their ability to grow in new sectors or regions without the time and cost burdens involved with establishing a physical presence. It also helps to create new markets and services to differentiate from competition and improve the ways customers' access and use the bank's products and services.

A more recent RBI Report of the Working Group on FinTech and Digital Banking provides the following view on cloud computing:

Cloud-based IT services can deliver internet-based access to a shared pool of computing resources that can be quickly and easily deployed. Infrastructure, Platform, Service and Mobile backend as a service are offered under cloud-based services. The use of these services is an important enabler for new entrants to the financial services arena to set up quickly and with low start-up cost, with easy options to expand their capability as the firm grows.

Depending on the type of services of the cloud service availed, it can potentially pose several challenges including the ability of jurisdictional enforcement authorities to effectively ensure security of data.

While adopting cloud-based services, especially those that are running in public cloud, it is important to pick right cloud based security architecture that is built to scale with cloud application adoption and also simplifies adoption of such cloud based services.

On the other hand, the RBI's Cybersecurity Framework for Banks released on June 2nd 2016 does not make any mention of cloud security.

In light of this, the stance that most Banks in India have taken is that adoption of cloud computing is fine as long as customer data (demographic and transactional) remains within Indian jurisdiction. This has prompted banks to look positively at cloud service providers such as Amazon Web Services, Microsoft Azure and others that have data centers within India and the legal contract is with the Indian legal entities of these service providers.

What is Zscaler

Born and built 100% in the cloud, Zscaler operates a massive, global cloud security infrastructure, delivering the entire Secure Internet Gateway stack as a service. By providing fast, secure connections between users and applications, regardless of device, location, or network, Zscaler is transforming enterprise security for the modern cloud era. In fact, companies like Zscaler not only provide a highly secured computing environment for the services that they enable but facilitate the deployment of additional security controls and capabilities, which traditional on-premises solutions simply cannot.

For instance, with Zscaler in place, it is now much easier to enforce a global Internet security posture for your roaming users – including enforcing controls such as DLP, APT protection besides regular URL and content filtering. Since traffic for all users – whether they are in your office premises or roaming – is routed through the Zscaler security cloud, the same rules get enforced without the need for multiple security products to be deployed and managed.

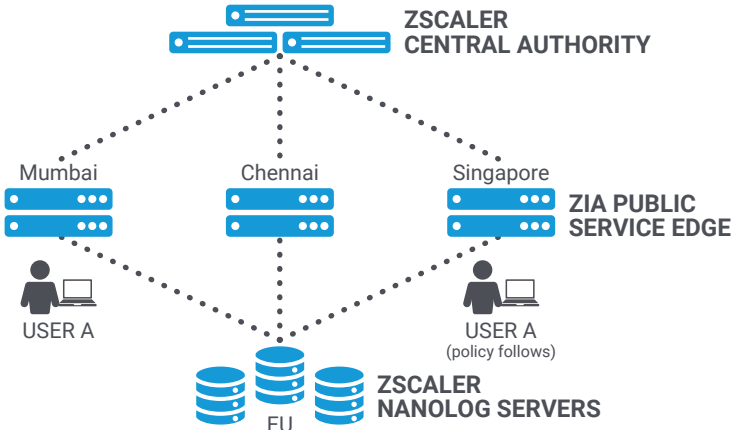
Zscaler security measures

The worst-case scenario with any cloud adoption is a compromise of the cloud service provider's infrastructure. Let us explore how Zscaler protects clients from such a black swan event.

First of all, the Zscaler solution wasn't built first and then had security bolted on later. Rather security has been part of the entire product philosophy and is embedded into the core design of the platform.

Let's understand the Zscaler architecture a bit better to see how security and privacy controls function:

The three-tiered Zscaler platform components comprise the control plane (Zscaler Central Authority), the data plane (ZIA Public Service Edge), and the logging and statistics plane (Zscaler Nanolog Servers).



Controls at the web transaction level

- ZIA Public Service Edge is a cloud-based edge firewall proxy located within Zscaler data centers around the world.
- ZIA Public Service Edge never stores any web transaction content or personally identifiable information (PII).
- Web transaction content is never written to disk; all inspection takes place in memory.
- Customer transaction logs (customer logs) are transferred to Zscaler's Nanolog clusters (Nanologs) in an encrypted format over a secure TLS connection.
- Customer logs are only available via the Zscaler web user interface by authorized administrators with appropriate privileges.

Controls at the network level

- Zscaler's cloud infrastructure is hardened against DDoS attacks and monitored 24x7x365.
- All communications between the ZIA Public Service Edge and Nanologs are encrypted using TLS.
- Customer logs are transmitted as indexed, compressed, and differential logs.
- Nanologs are tokenized, indexed and use differential logging that ensures that a single log is meaningless without a complete string of historic logs.
- Customer logs are never stored in clear text.

Controls at the cloud administration level

- Administrative access is protected using several layers of security.
- Zscaler's cloud is only accessible through jump systems accessible via Zscaler's private VPN.
- Access to the restricted jump systems requires multi-factor authentication. Including a hardware token.
- Each ZIA Public Service Edge is protected by a built-in firewall and administrative traffic is protected by AES 128, or AES 256 encryption.
- Once the VPN access has been granted, the administrators are authenticated with a user name and password and an individual certificate (public key authentication).

Controls at the facilities level

Zscaler's global hub data centers:

- Provide a high level of physical security.
- Are hosted in secure telecommunications centers at major Internet exchange points globally.
- Have 24x7x365 security management and site access via security operations center.
- Have strict access to authorized personnel including full biometric entry scanning.
- Are certified with ISO 27001, SAS 70, or a similar local certification.
- Have been security tested by governments as well as large multinational corporations.

How Zscaler enables compliance

Far from being a risk in terms of security or non-compliance, Zscaler enables banks to comply with multiple regulatory requirements. Let's see some of these below:

RBI's Cybersecurity Framework for Banks - Baseline Cyber Security and Resilience Requirements[1]
1) Inventory management of business IT assets With increasing adoption of cloud computing via SaaS models, there is a high probability that a bank's IT assets exist outside its data centers. Zscaler Cloud Application Control gives you complete visibility into shadow IT that may exist within your organization. See the section on shadow IT below.
2) Preventing execution of unauthorised software Zscaler's advanced security capabilities, including True File Type detection, Cloud Sandboxing, Antivirus modules, etc., prevent the download of any installers on the user's endpoints. In fact, with Zscaler Cloud Firewall, banks can eliminate appliance sprawl at branches by simply having the users connect to the internet via secure local internet breakouts that reduce costs and complexity and scale the same security policy elastically.
3) Environmental controls Zscaler data centers: • Provide a high level of physical security. • Are hosted in secure telecommunications centers at major internet exchange points globally. • Have 24x7x365 security management and site access via security operations center. • Have strict access to authorized personnel including full biometric entry scanning. • Are certified with ISO 27001, SOC II, FedRAMP, or a similar local certification. • Have been security tested by governments as well as large, multinational corporations.
4) Network management and security Zscaler facilitates greater network security and simplifies design in a bank's DMZ by reducing complexity of multiple devices (proxy, APT protection, gateway, DLP, etc.) and thereby allows uniform policy enforcement for all users and single pane of glass reporting – whether users are inside the organizational perimeter or outside of it.
5) Secure configuration Through a single administration interface, policies for multiple features can be enforced, thereby reducing complexity. Further, absence of any on-premises solutions obviates the need for security configuration reviews of multiple security technologies.
6) Application Security LifeCycle (ASLC) Not applicable
7) Patch/Vulnerability and change management Not applicable
8) User access control/management Fine-grained user and role-based policies allow the organization to decide based on not just user ID, but also device type, location of the user, and time of the day in which policies should be enforced.
9) Authentication framework for customers Not applicable

[1] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0

10) Secure mail and messaging systems

Not applicable

11) Vendor risk management

Not applicable

12) Removable media

Not applicable

13) Advanced real-time threat defense and management

Zscaler performs full content analysis of every single byte coming and going, and provides unlimited capacity to inspect ALL your traffic, including SSL and trusted content. You can find and stop all the bad stuff like browser exploits, scripts, zero-pixel iFrames, cross site scripting, and botnet callbacks. So you can block more threats and finally inspect everything without compromises.

With an inline cloud sandbox, you can provide full APT and zero day threat protection against unknown and emerging threats, no matter where you users go, or how they connect to the internet. Get always-on zero-day protection and ransomware protection, and in-depth visibility into the behavior of malware targeting your users. And you can also hold onto file delivery until sandbox confirms that it is clean.

14) Maintenance, monitoring, and analysis of audit logs & setting up and operationalising Cyber Security Operation Centre (C-SOC)

The Zscaler cloud security platform sits inline between your users and the internet, inspecting every byte of traffic and monitoring sensitive information. Zscaler's DLP functionality is in the perfect place to protect you against data loss, across all users and device types, including transaction content and SSL-encrypted or compressed traffic. Maintain data privacy and compliance with industry, local, and regional regulations, including HIPAA and PCI. Leverage our standard DLP dictionaries or define custom dictionaries to create granular policies for different employee populations. Advanced logging ensures you can view any compliance issue – immediately. And you retain complete control over which traffic to inspect, so you can maximize security while ensuring privacy. Zscaler also has advanced Data Fingerprinting/Exact Data Match capabilities to learn customer's sensitive information on premise and do DLP on it in cloud using fingerprints of sensitive data in Zscaler cloud.

15) Data leak prevention strategy

Built into Zscaler Cloud, Nanolog technology performs lossless compression of logs, which are transmitted to Nanolog servers over secure connections and multicast for redundancy. Also logs are routed to appropriate logging cluster irrespective of user location. Zscaler customers can mine billions of transaction logs to generate reports that provide insight into network utilization and traffic. Zscaler continuously update our dashboards and reporting and can stream logs to a third-party Security Information and Event Management (SIEM) service as they arrive which could be hosted in customer's DC or other clouds. Customers can choose to have logs written to disk in a physical location that complies with regional regulations.

Zscaler's founding concept was simple: as applications move to the cloud, security needs to move there as well. With Zscaler, global organizations transform into cloud-enabled operations.

The shadow IT problem

As observed earlier, business heads are adopting the cloud even if the CISO and the IT department may have different views on it. The business head is able to bypass any IT or CISO objections by transacting directly with a cloud service provider – typically of some Fintech innovation company. This leads to the phenomenon of Shadow IT, which is now such a serious issue.

Gartner recommends that enterprises should deploy shadow it discovery and data protection tools to enable the safe selection, deployment and notification of unauthorized cloud services[3].

Zscaler Cloud Application Control gives you complete visibility and control in a single click:

- **Reduce the risk of Shadow IT.** Eliminate the threats posed by unknown apps on the cloud and ensure that users follow policy. It also provides detailed visibility and reporting on which application your employees are using.
- **Enable proper use of business apps with policy and control.** Make sure that business apps don't bring in any malicious content, even if the traffic is encrypted, and make sure that they get the bandwidth that they need.
- **Ensure that sensitive data doesn't leave your network.** With full inspection of all content using pre-built DLP as well customer defined dictionaries and engines, you prevent data exfiltration.
- **Preserve optimal user experience.** With Zscaler, you'll get all of these benefits without adding hardware, software or latency and also be able to do traffic shaping by providing right bandwidth to right apps.
- **Integration with select CASB vendors.** Extend your policy control and visibility to out-of-band cloud applications via integrations with select CASB vendors.

On Office 365 already?

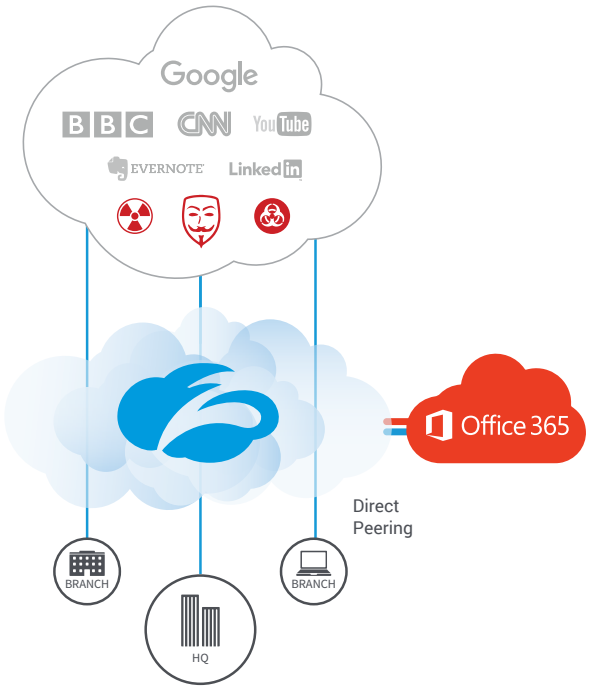
If you are an existing Office 365 customer, then you have already experienced the power of the cloud. You may also have experienced some of the downsides of Office 356 adoption such as the significant increase in bandwidth (reported to be nearly 40% on average). Therefore, deploying Office 365 requires hardware upgrades and constant firewall updates.

Zscaler increases your Office 365 deployment efficiency multi-fold. Offices and users directly connect to the Zscaler cloud, and the Zscaler cloud directly peers with the nearest Office 365 data center. Why is this a better deployment?

> "**Gartner predicts** by 2020, one third of successful attacks experienced by enterprises will be on their Shadow IT resources.[2]"

[2] https://blogs.cisco.com/cloud/gartner-report-says-shadow-it-will-result-in-13-of-security-breaches
[3] https://www.gartner.com/smarterwithgartner/dont-let-shadow-it-put-your-business-at-risk/

- **Quick deployment.** Because there's no hardware or software to upgrade prior to deployment, you can be up and running in minutes.
- **One-click configuration.** Automatically configure Office 365 connection requirements with a single click.
- **Bandwidth control.** Prioritize Office 365 to ensure that business-critical traffic takes precedence over recreational activities.
- **Avoid hardware refreshes.** The Zscaler cloud has unlimited capacity to scale as your user demands grow. Appliances just can't compete with that.



Conclusion

What we see is that Zscaler helps address multiple security challenges arising out of regulatory requirements, Shadow IT, and an overload of security gear. By moving an entire stack of security appliances into a service delivery platform hosted on bulletproof data centers, Zscaler gives clients the ability to enforce a large number of security controls through a single policy interface that is intuitive to deploy and easy to manage. The logging capability can be easily integrated with an on-premises or cloud-based SIEM and provide complete visibility of all user activity. With its native Office 365 integration, cloud application control platform, and advanced threat protection capabilities, the value proposition is simply unbeatable!

About Zscaler

Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com