COLORTOKENS

Technical Brief

RBI COMPLIANCE WITH COLORTOKENS

Meeting RBI Compliance
with ColorTokens Xtended ZeroTrust Security Platform

Introduction

ColorTokens Xtended ZeroTrust Security Platform enables banking and financial institutions simplify their security journey through a proactive cybersecurity approach. ColorTokens zero-trust architecture, signature-less endpoint protection and centralized policy orchestration effectively protects banks and financial institutions from sophisticated cyber threats. ColorTokens isolates critical segments of the banking infrastructure, securing workloads, dynamic application environments, users and endpoints (including ATM kiosks) that are spread across traditional and hybrid data centers.

This document serves as a reference guide on the mapping of the RBI cyber security framework (w.r.t. RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16) to ColorTokens capabilities.

Did you know?

According to Verizon Data Breach Investigation Report 2018, timely breach detection and response within the 'golden 24 hours' of cyber fraud plays a major role in recovering the funds lost.

According to Accenture High Performance Security Report 2016, 59% of the survey respondents say that it takes months to detect a breach.

RBI Compliance Challenges for Banks

The ever-changing digital payment landscape has made traditional banks and financial institutions adopt the latest technologies to improve customer experience, reduce operational expenditure and at the same time, stay ahead of the competition. These have increased the attack surface of the bank network, requiring the need for continuous protection from advanced cyber threats.

- **Continuous Surveillance and Risk Analytics:** Information security managers and key decision makers don't have a unified view of the continuously changing security posture of the bank; thanks to the number of siloed security products. ColorTokens Xview for Visualization solution provides centralized granular visibility of East-West and North-South data center traffic without requiring siloed visibility tools. ColorTokens also provides invaluable insights into residual risks, enabling security leaders to continuously assess and improve the security posture of the bank network.

- **Vulnerable Endpoints and Critical Assets:** Banks have a large number of legacy and unpatched systems making them vulnerable to malware/ransomware attacks. Patch management is a headache and upgrading legacy systems is an expensive exercise. By allowing only the known good (whitelisted) processes to run, ColorTokens Xprotect for Endpoint Detect and Response solution protects ATM kiosks running on legacy/unpatched operating systems, critical servers and endpoints from malware, ransomware and other sophisticated threats. This process-level control secures endpoints and special purpose terminals like ATM kiosks completely prevents the execution of unauthorized software.

- **Proactive Security:** Banks are advised to adopt proactive cybersecurity measures - a shift from the current reactive strategies to protect critical assets from unknown and sophisticated threats like zero-day malware, advanced persistent threats and attacks that are not catalogued in the anti-virus/ anti-malware signature definitions. With software-defined micro-segmentation and intent-based resource access policies, ColorTokens Xshield for Workload Protection solution helps banks realize a zero trust proactive approach without additional investment in expensive hardware.

ColorTokens Xtended ZeroTrust Security Platform Mapping to RBI Compliance Requirements

The following table maps ColorTokens capabilities to RBI cybersecurity regulatory requirements. Information security managers, auditors and compliance executives can see how ColorTokens can provide continuous security, protecting banks from sophisticated attacks by securing critical banking application environments and customer data.

If you have questions or want to know in-depth of how ColorTokens can help you achieve RBI compliance, please do not hesitate to contact us.

	Requirement	ColorTokens
Enterprise Control		
Identity & Access Management		
	Does a process exist to monitor password complexity?	Active Directory (AD) has to have the password complexity implemented. ColorTokens integrates with AD can support this feature.
	Do you mandate periodic password changes?	AD has to have the password complexity implemented. ColorTokens integrates with AD can support this feature.
	Does the organization define and enforce actions when the maximum number of unsuccessful login attempts is exceeded?	AD has to have the password complexity implemented. ColorTokens integrates with AD can support this feature.
	Is the session timeout enforced after a pre-defined period of inactivity?	Session time-out is supported by ColorTokens. Connection to the resource can be restricted if session time-out occurs.
	Do you have a proper provisioning and de-provisioning policy as well as implementation?	Security policy template defines the communication in terms of roles of the resources and access parameters.
	Do you have automated provisioning and removal of digital identity for accounts; managed identity life cycles?	A logical group of applications are created by assigning roles and resources.
	Have you employed the use of multi-factor authentication?	Not applicable.

	Requirement	ColorTokens
	Do you have a unique identity for every individual?	A unique ID is assigned to the users based on the Active Directory (AD) properties. Privileged user IDs are assigned only to roles and restricts to least privileges to perform job responsibilities.
	Do you have hierarchical multi-factor authentication for additional/critical roles?	Not applicable.
	Have you deployed your IAM in a basic identity complemented with a role based access?	The users are created in the ColorTokens console or imported from an active directory and restricted access is assigned depending on their job roles.
Risk Assessment		
	Do you determine the priority of a risk?	Unified residual based OWASP risk metrics provides rich contextual insight into every business application. ColorTokens risk score continuously updates itself based on changes in the environment, maintaining the security posture of the enterprise.
IT Infrastructure Security		
Network Security		
	Have you configured your IDS/IPS to detect/prevent network intrusions?	Supports the customer's existing anti-virus applications and keeps the AV actively running. Granular visibility to view cross segment traffic (both E-W and N-S), with clear indication of suspicious connections and policy deviations.

	Requirement	ColorTokens
Application Security		
	Has the attack surface been analyzed and appropriately minimized?	ColorTokens detects malicious data traffic to and from the applications, helping with remediation.
	Are successful and unsuccessful attempts to access an application logged?	CM displays a central dashboard with information about the state of the applications, which provides various critical metrics like unauthorized connections CM prevented, data transfers over resources, number and status of login attempts from end users, resources protected and their security effectiveness.
	Are changes in access to an application logged?	Every policy change is audit logged with user ID and timestamp.
	Are application logs protected against tampering?	ColorTokens keeps the sensitive application data completely non-reachable and isolated from any unauthorized accesses, based on the policies defined.
Data Security		
	Is remote access to data (through application) logged and monitored?	Every network access and session are recorded and made available through visual and textual means for deeper analysis. Nothing goes by unnoticed. The policy engine ensures that only authorized accesses are allowed to the protected entities/resources.
	Is confidentiality of data maintained at transmission and storage?	ColorTokens offers always-on, point-to-point encryption. A token (CT Agent) is installed on the resources in the customer environment and enforces policies and provides encryption both in-transit as well as at rest.
	Is integrity of data maintained at transmission and storage?	Integrity of data is maintained during communication between its protected entities. Uses TLS protocol during data transmission.

	Requirement	ColorTokens
Endpoint Security: Hardening (Desktops, Mobiles, Tablets)		
Basic Data protection		
	Does your endpoint have a mechanism to encrypt the HDD volumes using industry standard/validated encryption methodology to protect the data on the drive in the event of theft or lost device/ HDD?	No HDD encryption as its done from BIOS.
	Does your endpoint support encryption of the data files at rest from protection against data leakage and misuse by the users themselves intentionally or unintentionally?	Not encryption but we lock the files and also block USB.
	Does your endpoint have capabilities to protect data on the PC/Devices by compartmentalizing the corporate data with personal/consumer applications like Facebook, Twitter, etc.? [Corporate data shouldn't be allowed to communicate with Non-corporate apps	Application can be controlled at the process-level for inbound/outbound network connections.
	Does your endpoint have a DLP (Data Leakage Prevention) solution in place?	We don't do full DLP, but we protect data like files, folder through file protect.
Endpoint Admin Model		
	Do you have a centralized patch management system?	ColorTokens Xprotect completely eliminates the need for patch management tools as the applications are protected at the process level.
Malware Resistance in Endpoint		
	Does your endpoint have anti-malware agent which can protect the system from all known malware and threats?	ColorTokens Xprotect locks down endpoints at the process-level, and malware cannot spawn new processes, protecting the endpoints from known and unknown threats.
	Do you regularly update the malware signatures of the anti-malware agent?	ColorTokens Xprotect is a signature-less product providing best-in-class protection without the need for constant signature updates.

	Requirement	ColorTokens
	Is your endpoint able to use hardware based isolation to protect the most sensitive OS components (e.g.: authentication; system hardening; malware defenses)?	ColorTokens Xprotect enables this protection using endpoint lockdown, Rule Rings and trust vector for processes and modules.
	Is your endpoint configured based on whitelisting of authorized applications?	ColorTokens Xprotect protects endpoints based on the known good (whitelisted) processes.
	Do you regularly update patches of all applications running at endpoints?	Even if the systems are not patched, it will not make the endpoints vulnerable as Xprotect lockdown the processes.
	Is your endpoint protected from zero day vulnerability attacks by allowing only signed code	With process-level lockdown and process-level firewall controls, ColorTokens Xprotect protects the systems from C&C attacks, fileless malware and zero-day threats
	Does your endpoint prevent vulnerability exploit at the kernel level?	ColorTokens Xprotect protects the systems at the kernel level from known and unknown threats.
	Does your endpoint support URL Reputation and Anti-phishing Filter to protect users from visiting phishing websites?	Even if user clicks on malicious website, no script is executed, or no process is spawned, as ColorTokens Xprotect can lockdown folders and processes.
	Is your endpoint enabled for advanced post breach detection, monitoring, and forensics?	ColorTokens RADAR360 supports forensics with all the relevant data pertaining to the endpoints.
	Is your endpoint capable of stopping binary execution (autorun malware or exploit-based malwares) from USB drives?	ColorTokens Xprotect protects the systems at the kernel level from known and unknown malware threats.
	Does your endpoint/web browser have protection against drive-by-download?	With process-level lockdown and process-level firewall controls, ColorTokens Xprotect protects the systems from drive-by-downloads.

	Requirement	ColorTokens
Security Monitoring		
Threat Intelligence/Inventory		
	Is threat information used to enhance internal risk management and controls?	Risk rankings are assigned to the applications.
	Is information about threats shared with law enforcement and regulators when required or prompted?	Not applicable
	Are threats mapped to specific assets that may be affected by them?	Risk rankings are assigned to the applications based on the vulnerability level of the application.
Security Operations Center		
	Are audit log records and other security event logs reviewed and retained in a secure manner?	Audit trails are enabled and access to system components is linked to the individual user.

Conclusion

ColorTokens Xtended ZeroTrust Security Platform helps you ensure that your financial institution complies with RBI requirements to protect critical resources, application environments and endpoints. ColorTokens helps you limit the scope of audits using micro-segmentation and enable secure lock-down of regular endpoints and special purpose systems like automated teller machines (ATMs) with granular visibility and control. Furthermore, ColorTokens helps you prepare for digital transformation exercises without the need for additional security or hardware requirements that could potentially increase costs and slowdown the transformation journey.

colortokens.com
sales@colortokens.com