COLORTOKENS

Solution Brief

PROTECTING BANKING AND FINANCIAL INSTITUTIONS FROM CYBER FRAUD

Enabling the financial industry to become proactively secure and compliant

Overview

In order to keep up with the changing digital payment landscape, traditional banks have adopted newer technologies to enhance customer experience and to stay abreast of competing financial institutions in retaining their customer base. In doing so, banks have increased the attack surface, requiring their IT security teams to always be alert, and ready to mitigate imminent cyber threats.

The 2018 Verizon Data Breach Investigation Report notes that timely breach detection and response within the 'golden 24 hours' of cyber fraud plays a major role in recovering the funds lost. But, how do you gain unprecedented visibility and proactive protection within your vast banking networks?

ColorTokens Xtended ZeroTrust Security Platform vastly simplifies this journey by empowering banking and financial institutions to take a proactive cybersecurity approach. With ColorTokens’ zero-trust architecture and centralized policy orchestration, critical segments of the banking infrastructure can be effectively isolated, while workloads, dynamic application environments, endpoints (including ATM kiosks) and users spread across traditional and hybrid data centers can be secured from sophisticated cyber threats. ColorTokens' technology is infrastructure independent and reduces the CAPEX and OPEX by consolidating point security and siloed networking products.

ColorTokens Solution

With ColorTokens Xtended ZeroTrust Security Platform, banks and financial institutions can systematically equip themselves to enable proactive security against known and emerging cyber threats, while focusing on innovation and improved customer experiences.

Benefits:

- Secure and centralized platform-independent solution for multi-vendor infrastructure
- Decentralized zero-trust architecture for proactive defense against data breaches, APTs and other unknown cyber threats, while meeting compliance and regulatory requirements (PCI, GLBA, RBI, etc.)
- User and application endpoint security without an additional hardware investment
- Continuous security posture visualization and residual risk evaluation across banking application environments, workloads, users and endpoints
- Signature-less endpoint security to protect legacy terminals like ATM kiosks, even if unsupported/unpatched

Cybersecurity Challenges in BFSI

- *Increasing Attack Surface:* Rapid digitization and adoption of web and mobile applications have increased the attack surface of financial institutions. Whilst banks spend millions of USD in deploying the best security tools and increasing the barriers of entry, hackers are constantly finding newer, more sophisticated techniques to steal money and data. The large number of disparate security products, the number of IT personnel and the scope of the network makes detecting an anomaly before the damage is done an enormous challenge.
- *Reactive Security:* According to Accenture High Performance Security Report 2016, 59% of the survey respondents say that it takes months to detect a breach. Most banks and financial institutions relying on traditional cybersecurity tools are stuck to a reactive security approach.

With the disjointed number of security products, Information Security Managers and key decision makers don't have a unified view of the changing security posture of the bank.

- *Vulnerable Legacy Systems & ATM Kiosks:* The vast number of legacy and unpatched systems increase the chances of malware/ransomware attacks spreading laterally to other critical resources in the bank and eventually leading to financial and customer data loss. Upgrading all legacy systems is an expensive and operationally intensive exercise for the banks. ATM kiosks running legacy operating systems are vulnerable to attacks leading to ATM jackpotting and unlimited ATM cashouts.

- *Threats from Within:* At any point in time, the bank's IT personnel must know if one of their valuable assets is being accessed from within their network and by whom. Without this visibility and control, malicious and inadvertent threats from insiders will remain a persistent headache. In a bank with thousands of employees, cyber hygiene is the last thing the bank's IT personnel can expect from the staff. Inculcating cyber hygiene through training is an expensive proposition, with no guarantee that the dos and don'ts will be adhered to.

> A recent cybersecurity report from Accenture states that four out of five banks are confident that they are protected against cyber frauds, but, 33% of the breaches are successful.

- *The Changing Scope of Compliance:* When it comes to compliance audits, it's still a norm for the VLANs/ACLs to be individually accessed and checked for deviations. These audits can run for days, weeks or months, depending on the complexity and scope of the network. By the time an audit is completed, there's no assurance that something wasn't changed in the network while the audit was in progress. The consequences of non-compliance can amount to millions of USD – a costly oversight.

ColorTokens Solution

ColorTokens Xtended ZeroTrust Security Platform helps banks and financial institutions become proactive, with centralized visibility and control across bare-metal, virtual and cloud infrastructure. ColorTokens helps the finance industry with the following core capabilities:

- *Granular Visibility of East-West and North-South Traffic:* Without the need for multiple, siloed visibility tools, ColorTokens Xview enables a centralized view of what's connecting to what across the multi-vendor hybrid data center. Authorized and unauthorized traffic between critical banking and financial applications, servers, workloads and endpoints are clearly visualized, giving insights right down to the ports of the source and destination's IP addresses.

- *Secure Environment Separation and Policy Orchestration to Contain Lateral Threats:* ColorTokens Xshield reduces the attack surface of the banking infrastructure by isolating application environments, critical assets and core banking servers through software-defined micro-segmentation. The segmentation is done using attributes (e.g., server role, application environment, etc.), without dealing with complex network level constructs like VLAN memberships and IP addresses. Centralized policy orchestration helps define resource access policies, tests the security posture with the defined policies and then enforces the policies on the resources to be protected.

Visibility
Micro-
segmentation
Endpoint
Protection
Compliance

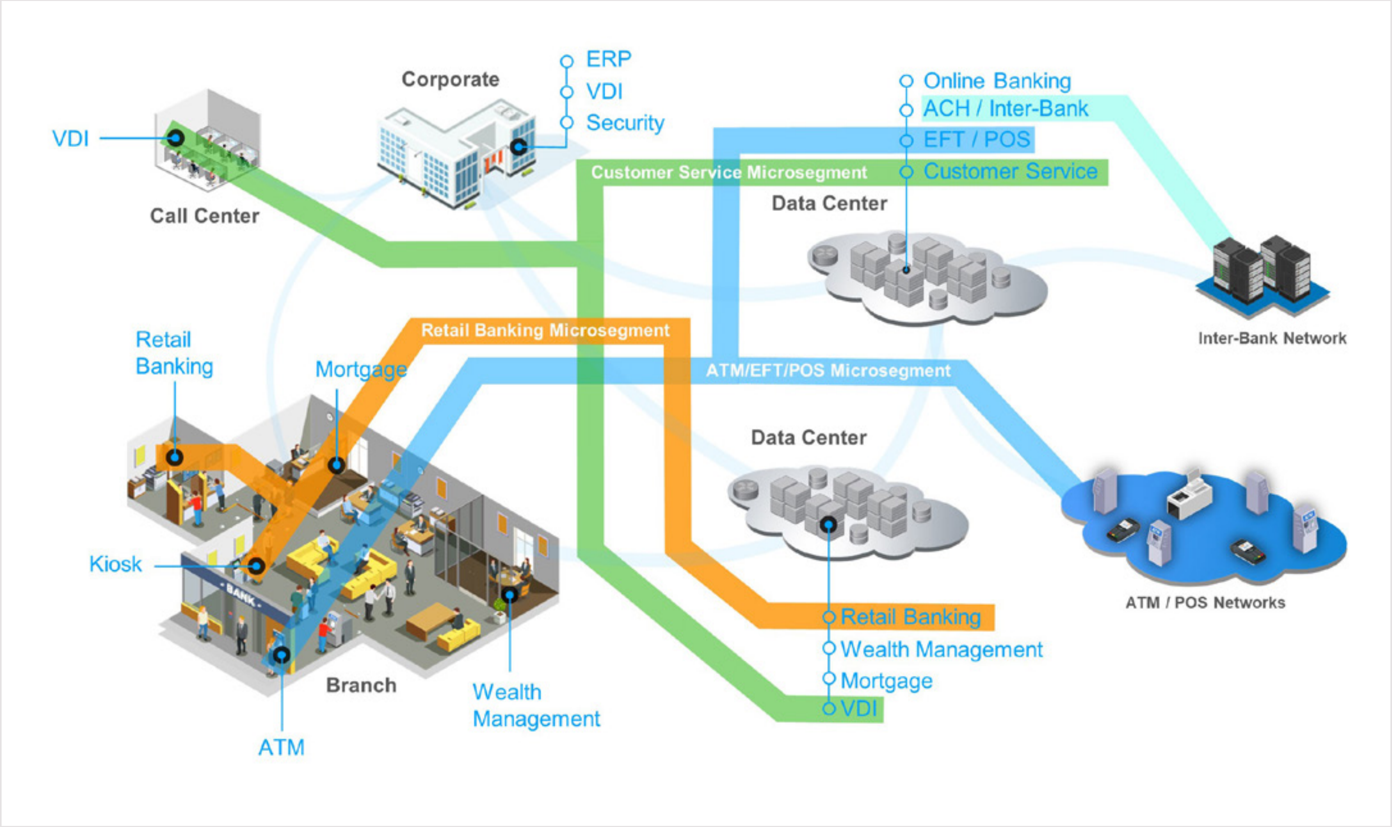
- ***Signature-Less Endpoint Protection for ATM Kiosks, Critical Servers and Endpoints:*** ColorTokens Xprotect protects ATM kiosks running on legacy/unpatched operating systems, critical servers and endpoints from malware, ransomware and other sophisticated threats. On systems protected by ColorTokens, the malware cannot spawn a malicious process to infect the computer and spread laterally. By allowing only the known good (whitelisted) processes to run, ATM kiosks can be completely locked-down, making them tamper-resistant.

- ***Fast and Efficient Compliance Audits:*** Instead of looking at individual ACL tables, visualize the traffic across subnets to check the efficacy of segmentation done using VLANs. ColorTokens Xtended ZeroTrust Security Platform probes the open ports across subnets, giving a clear picture of all open ports on individual resources across the subnets. Combining this with micro-segmentation (limiting the audit scope), policy orchestration and process-level endpoint protection, banks and financial institutions can efficiently demonstrate compliance and save external audit costs and regulatory fines.

Conclusion

ColorTokens Xtended ZeroTrust Security Platform helps you take a proactive approach towards securing your bank/financial institution, creating an effective barrier against sophisticated cyber frauds. ColorTokens saves costs and patch management overhead by protecting legacy and unpatched operating systems powering ATM kiosks. ColorTokens helps banks/financial institutions meet evolving compliance requirements without additional complexity and costs.

Proactive protection from sophisticated cyber threats



COLORTOKENS

ColorTokens Inc., a leader in cloud-delivered ZeroTrust security, provides a modern and new-generation of security that empowers global enterprises with a proactive approach to single-handedly secure cloud workloads, dynamic applications, endpoints and users. Through its award-winning Xtended ZeroTrust Platform, ColorTokens delivers the only cloud-based solution that combines AV, EDR, workload protection and application control into one ultra-lightweight agent. This enables enterprises to instantly visualize and segment their entire IT infrastructure, block advanced malware, contain and respond to APTs and zero-day attacks—all while seamlessly integrating with existing security tools.

colortokens.com
sales@colortokens.com