COLORTOKENS

SOLUTION BRIEF

Zero Trust Security to Protect Banking, Financial Services & Insurance Systems

Colortokens Eases Regulatory Compliance, Protects Your Customers, and Keeps Critical Business Services Operational – Even in the Face of a Breach

It's been reported that when Willie Sutton, the famous bank robber of the 1930s, was asked why he robbed banks, he replied, "Because that's where the money is." Modern cyber criminals seem to have come to the same conclusion. In 2022 almost 20 percent of all cyberattacks were against financial services companies. In addition to attacks affecting business operations, customer records were a prime target. According to Forrester, last year alone saw multi-millions of financial customer records lost. TransUnion suffered a data breach that affected 10,200,000 customer records. CashApp reported 8,200,000 customer records compromised. Gemini lost 5,700,000 records, Nelnet lost 2,500,000, OpenSea lost 1,800,000 and GiveSendGo lost 92,000.

In addition to the immediate damage a successful attack causes to the business and clients of financial institutions, there are downstream effects and even the possibility of systemic risk and the loss of public trust and confidence. So it's no surprise that financial regulatory bodies have responded by imposing more and stricter cybersecurity standards and regulations on the banking, financial services and insurance sector. Financial sector cybersecurity regulations such as the Operational Resilience Initiative by the UK's PRA, the new Digital Operational Resilience Act in the EU, the Cyber Security Framework of the Reserve Bank of India, the Insurance Regulatory and Development Authority of India, and in the US the Gramm–Leach–Bliley Act, the SHIELD Act and Federal Financial Institutions Examination Council (FFIEC) are increasing the onus on financial services institutions to prove compliance with cyber security standards and practices. And these financial-specific regulatory regimes are over-and-above the regular menu of GDPR, PCI, NIST CSF and ISO 27001 standards.

The Requirement: Satisfy Continuously Evolving Regulatory Regimes While Protecting Critical Systems and Data

Cybersecurity compliance is a moving target for leaders in financial services companies. It seems that just when you have successfully complied with the existing regime, a new one is enforced, with new audits and certifications. Financial industry CISOs and IT leaders must be able to demonstrate to their stakeholders, the C-suite, and the board of directors that they have postured their organization's technical architecture to get ahead of the curve and avoid being compelled to constantly play catch-up.

At ColorTokens, we believe that the way to approach this is to first cover the basics by adopting the fundamental principles of Zero Trust security:

- Approach your cybersecurity design by anticipating that a breach will occur.
- Protect regulated applications with granular segmentation policies with micro-perimeters to stop ransomware, malware, and data exfiltration.
- Enforce policies for secure remote and local user access to network resources using the least-privilege-needed paradigm.
- Provide network asset and traffic visibility across the entire landscape, mapping dependencies of applications, and monitoring policy and connectivity for compliance violations.
- Provide audit files and reports to show consistent and on-going improvement in cyber security posture, attack surface reduction and blast radius containment.

[1] IBM Security X-Force Threat Intelligence Index 2023 | IBM

[2] Forrester TRENDS REPORT, Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2022, Feb. 24th, 2023

With these measures in place, financial organizations will be better able to comply with emerging security audit requirements. They will be able to assure stakeholders, including customers, that they have the resilience needed to continue to provide service and protect client records even in the face of a perimeter breach. They will also have established a firm footing for successful mitigation of any attack by their security operations.

The Technical Challenge: The Financial Services Network Topology is Often Complicated and Diverse

It spans across on-prem data centers, multiple clouds, containers, and even employees' homes and third-party networks. This has caused the fragmentation of security into multiple products and interfaces, making implementation and day-to-day management of Zero Trust highly complex — and complexity is often the enemy of security.

Because of this, despite its clear benefits, Zero Trust has not been widely adopted at scale. Traditional segmentation solutions, using hardware firewalls and VLANs, require significant upfront costs in hardware, and lengthy and costly deployment and maintenance. Solutions that require proprietary software firewalls introduce further complexity. With the increase in remote and hybrid workforces, the need to provide secure user access to microsegments introduces yet another layer of complication.

The Solution: A Unified Platform for Secure Remote Connectivity Along With Software-Defined Microsegmentation for Any Asset: Remote, On-Prem or in the Cloud.

Zero Trust network segmentation, when done right, can completely block lateral movement and kill ransomware. It involves applying a firewall "micro-perimeter" around every asset in the network, allowing only necessary traffic. But Zero Trust is not just about the network — it's not really Zero Trust unless it controls user access to apps and data in those microsegments.

ColorTokens has unified the disjointed pillars of network security – segmentation and Zero Trust user access — into a single, simple platform. This allows a unified approach to visualizing and controlling network traffic in all modes: workload-to-workload, workload-to-user, and user-to-user. The unified administration console lets you centrally monitor and protect workloads in multiple cloud environments such as AWS, GCP and Azure, on-premise datacenters, in containerized deployments, as well as controlling access for both local and remote users.

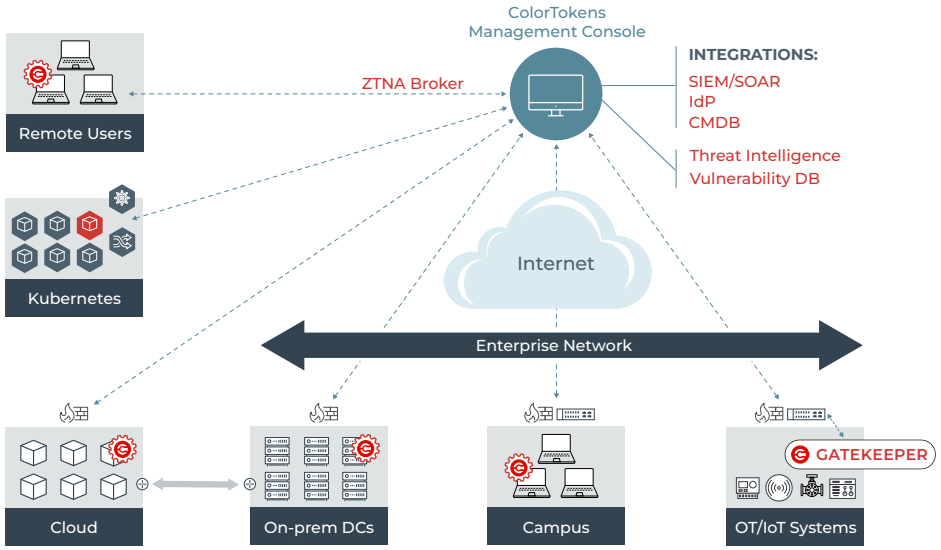


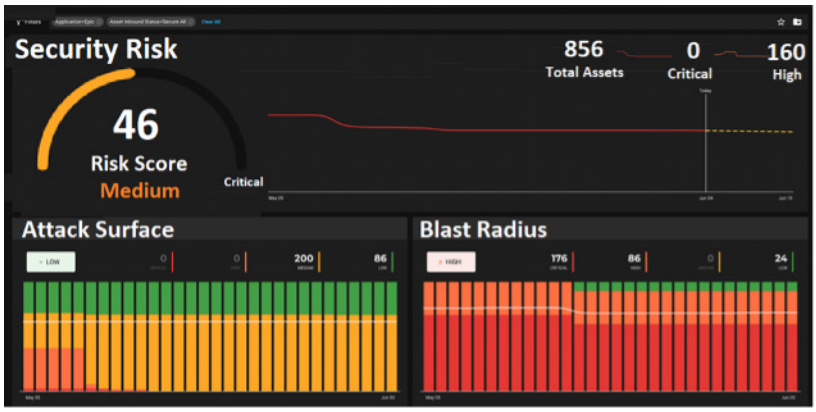
Figure 1: ColorTokens Unified Zero Trust Platform

Colortokens Simplifies Your Journey to Zero Trust Architecture

The ColorTokens solution leverages the hundreds (or thousands) of host-OS based firewalls you already have in your environment. We provide the central policy engine which configures these native firewalls on Windows, Linux, Unix, and Mac operating systems so you can easily manage them as policy enforcement points. You can choose to use our lightweight agent on your endpoints, or you can use our agentless access gatekeeper software to control traffic, especially for IoT and devices with legacy operating systems.

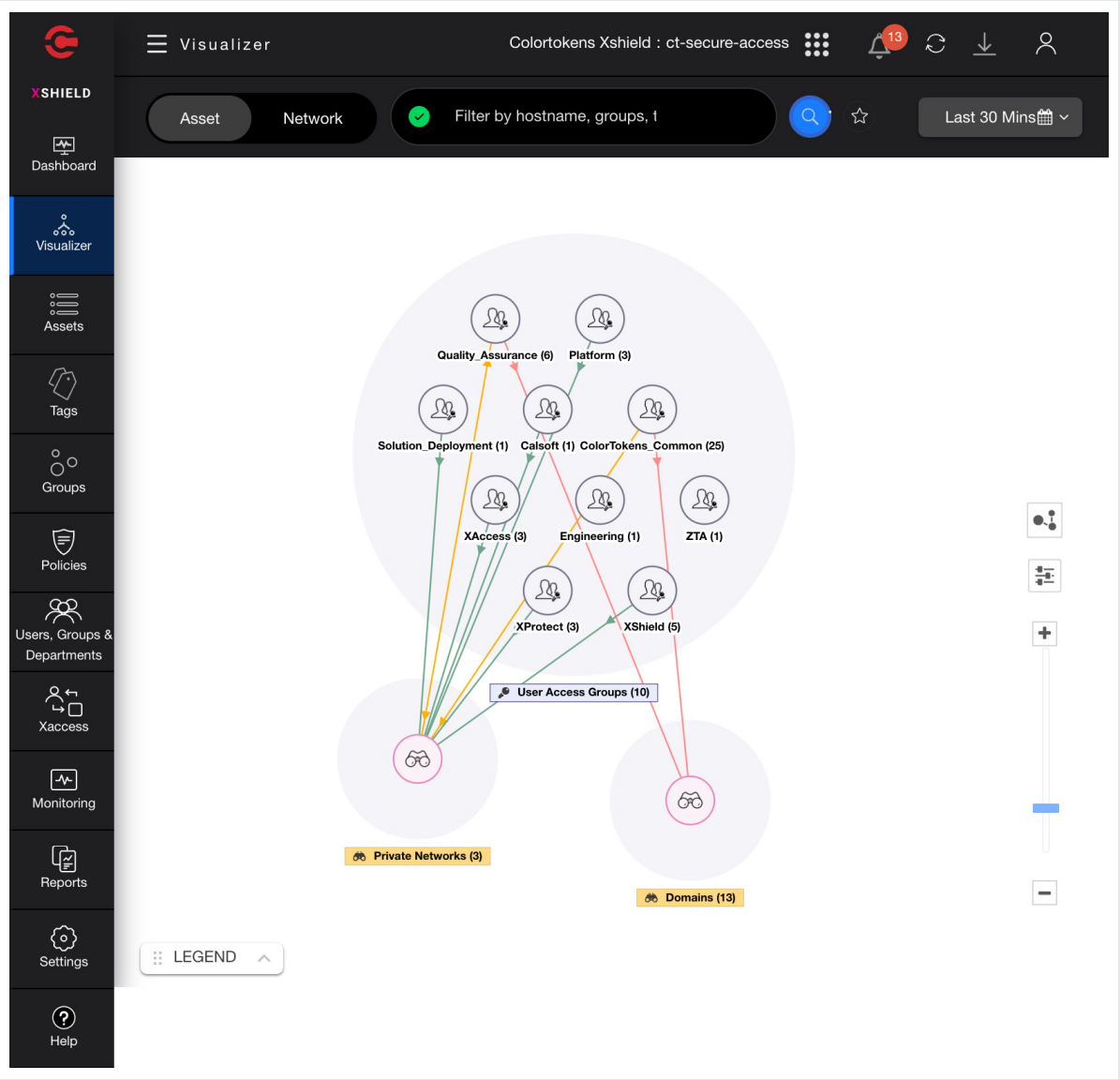
Visualize and Communicate Your Improving Cyber Defense Posture

Today, many CISOs report to the CIO, CFO or CEO. These stakeholders aren't interested in technical reports about the number of endpoint agents installed, or number of servers segmented, or number of traffic polices enforced. The C-suite and board of directors are interested in quantifiable improvements in their company's resilience and sustainability. The CISO must justify the company's investments in cyber security. They're interested in audit readiness, and they want to see a quantifiable reduction in risk. They want to know how the company is prepared for the upcoming SOC audit, or ISO 27001 compliance, or ESG audit. (The cybersecurity score can be the difference between ESG silver and gold status — out of 700 points, cybersecurity is 100 points.) ColorTokens gives you the ability to communicate and justify your cybersecurity initiative with your business stakeholders and auditors through clear graphical reports showing the consistent incremental improvement in your cyber defense posture.



A “Single Pane of Glass” Solution is Crucial for Visibility and Management of Zero Trust User Access and Network Segmentation

If separate point solutions are used for secure user access and for network microsegmentation, administrators would need to manually maintain coherence between policies defined in different tools and different management consoles — one set of policies for workload-to-workload traffic in the enterprise network, and another for user-to-workload secure access. Managing policies in separate tools is an administration headache and is more expensive, with greater personnel and training needs. It can lead to increased risk because of policy errors. Our integrated management console gives you a comprehensive approach to zero trust policy definition and enforcement, for both user access and network microsegmentation so that the greatest reduction in attack surface is achieved.



Simplifying Your Journey to Zero-Trust Architecture

ColorTokens is a leader in delivering innovative and award-winning zero-trust cyber security technology solutions such as network micro-segmentation, endpoint hardening and whitelisting, cloud and container security, and zero-trust network access. ColorTokens is a US corporation headquartered in Silicon Valley, and has approximately 400 employees world-wide, with offices in the United States, the United Kingdom, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please visit **colortokens.com**