COLORTOKENS

WHITEPAPER

Secure User Access

Introduction

During the late 1990s, administrative overheads of providing application access to users and revoking their access was becoming complex. IT teams were struggling to streamline this task as ad-hoc processes, scripts, and excel sheets were used to manage user access. Over time, the number of applications and users increased. Organizations started adopting native tools like Active Directory to streamline user access management.

This approach worked for flat networks and on-premise resources. However, with applications moving to clouds and the users of these applications connecting from multiple campuses, coffee shops, and geographically spread offices, the challenge of providing user access with the same privileges started escalating. There was also mounting pressure from government legislation (SOX) to adopt sound identity and access management methodologies. Additionally, the collaboration between eco-system partners and supply chain vendors across various industries like retail, healthcare, transportation, and financial services for business agility was increasing, and in turn expanding the blast radius of the attack.

> Users are intentionally or unintentionally are responsible for almost 90% of cyber-attacks.

The spike in the number of applications coupled with the fragmentation of users has widened the security gaps. While there are multiple technologies for providing user access to on-premise and cloud resources like VPN, SDP, and CASB among others, deploying these tools means that the IT team needs to manage multiple-point tools, collate several reports, and analyze every user's activity to identify malicious user.

Multiple protocols and standards for user access management also bring in integration challenges. Poor security hygiene by employees and partners continue to make users the weakest link in security. Users are intentionally or unintentionally are responsible for almost 90% of cyber-attacks. A majority of the breaches take place due to ignorant users acting on a phishing email, while malicious insiders continue to be another major cause of security breach. These breaches cause considerable revenue loss as well as exposure of critical business assets, despite spending millions of dollars on traditional access management security technologies.

Current State of Security

Most organizations invest heavily (almost 80% of security budgets) on perimeter security and endpoint security solutions that are not adequate in a rapidly evolving threat landscape. Traditional network security technologies see and act on north-south traffic only and are usually blind to east-west, south-north, and insider threats. Signature-based antivirus products largely fail to detect and prevent advanced zero-day attacks – making security ineffective and reactive. These security solutions also do not flag or prevent the user's and endpoint's malicious behavior including unauthorized attempts made by the users to access critical business applications and resources.

To bridge this gap, organizations use Identity and Access Management (IAM) solutions that identify the users and implement authorized access to business applications and resources. However, IAM products are unable to detect and prevent users and their machines from spreading malware and invading into the critical business resources. Also, IAM products do not easily integrate with other security solutions used by the organization, and thus fail to provide adequate secure user access control.

VPN is another commonly used security measure to ensure secure access for employees and contractors who work remotely and access internal applications. A major drawback of VPN technology is that it extends access across the entire corporate network on the insecure public internet, thereby increasing the attack surface. You might as well be extending your corporate network and critical resources to a coffee shop.

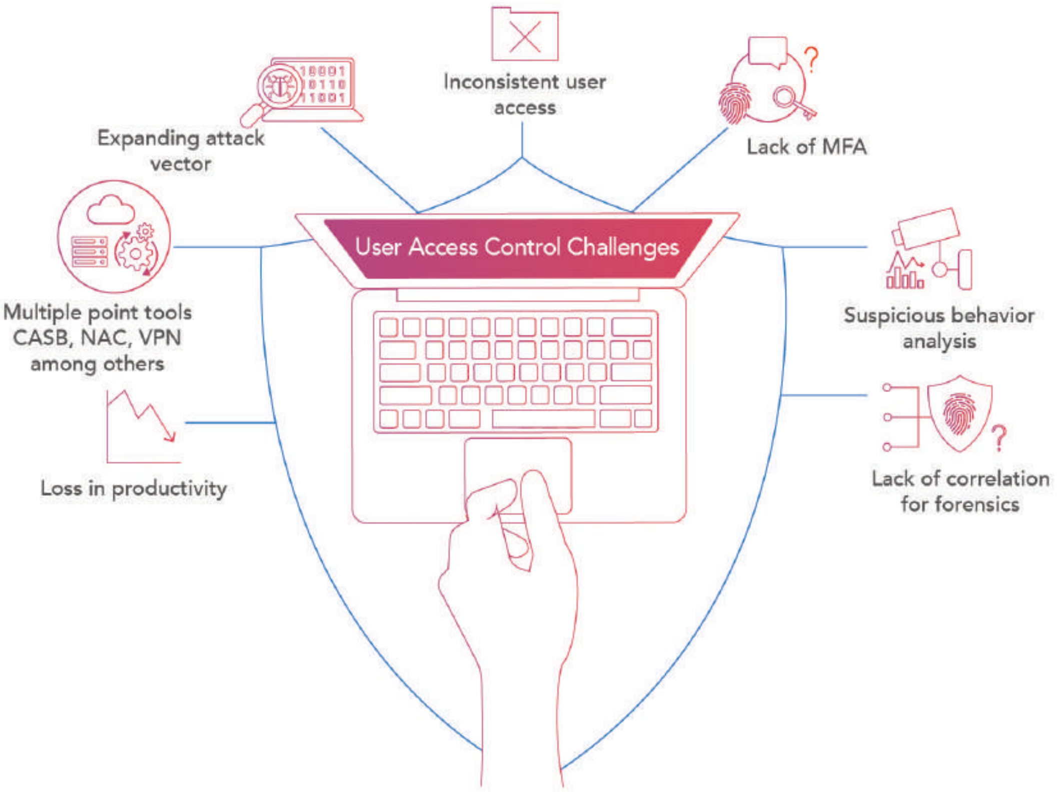
User Access Control Today

User authentication and access management technology has grown significantly in recent years. Single sign-on (SSO) and multi-factor authentication (MFA) have become common across organizations. SSO eases the user's pain of signing in with different credentials for accessing various applications. MFA not only ensures the identity of the person but also reduces the possibilities of identity theft.

Most organizations today have user access control systems in place with access to applications tied to the user's identity. Since applications are mostly distributed – organizations have some apps running in the local network while others running in the cloud – user access contro al systems also need to adapt to these hybrid environments. Unfortunately, this is not the case. Organizations use multiple point products like CASB for cloud applications, NAC for local network access, VPN for remote access, etc.

Though there are multiple user access control solutions for different requirements, the solutions are not integrated and do not synchronize with each other. They do not have a common management interface, leaving the administrators with the tough task of configuring and managing multiple products, often resulting in inconsistent enforcement across products.

To protect users from evolving cyber attacks, the user access control solution should provide uniform access control for aemployees, partners, and contractors regardless of their location and the devices they use.


Inconsistent user access
Expanding attack vector
Lack of MFA
User Access Control Challenges
Multiple point tools CASB, NAC, VPN among others
Suspicious behavior analysis
Loss in productivity
Lack of correlation for forensics

User Access Control Challenges

Users are the weakest link posing a significant challenge to ensuring the organizations' security. Hackers are increasingly using phishing campaigns to bypass perimeter defense solutions and trick users into clicking on malicious links. According to Verizon's 2018 Breach Investigations report, 92% malware is still delivered by email. The need of the hour is for organizations to have a robust user access control solution in their security arsenal. However, the user access management and control solutions today have multiple challenges.

- IAM products enable administrators to provide access to critical resources based on roles and privileges and prevent access to users who do not have privileges. But IAM products do not restrict unauthorized users from accessing critical applications at the network layer. Unauthorized users can still scan the application servers and exploit vulnerabilities to gain access.

- An increasingly distributed workforce and distributed applications also pose a major challenge to user access control. Organizations today have large number of employees working remotely. In addition to remote employees, organizations have contractors and partners who access applications belonging to the organization. At the same time, organizations often use applications running in the cloud as well as in-house applications running in local data centers. Administrators face the daunting task of providing uniform access of distributed applications to local and remote users.

- Most user access solutions do not authenticate the identity of the user device, enabling attackers with stolen credentials to gain unauthorized access to critical business applications. Also, many user access control solutions are static in nature and do not use contextual information like user's location, device type, etc., thereby allowing attackers with stolen credentials to access the application from an unexpected location using an unexpected device type.

Secure User Access Control and Visibility Checklist

To safeguard critical business resources and IT infrastructure, from insider threats and advanced security attacks, businesses should consider the following:

✓ **Effective User Access Solution**
Block L3-L7 access to the applications from unauthorized users.

✓ **User and Device Identity**
Validate the identity of users as well as the identity of user devices.

✓ **Dynamic User Access Policy**
Contextual user attributes like location and device type – to enforce different access policies depending on the user's location or type of device.

✓ **Unified Management**
Single management interfaces for defining access policies for local users or applications and remote users or applications.

✓ **User Behavior Visibility and Analytics**
Deep visibility into what applications and resources a user device is accessing and leverage telemetry data for analytics.

ColorTokens Secure User Access – A Complete Access Control and Visibility Solution

ColorTokens Secure User Access (SUA) is a micro-segmentation solution built on the zero-trust model. The solution extends micro-segmentation right to the user level. It provides user identity-based segmentation, enabling administrators to define access policies based on the user's identity.

ColorTokens offers a unified platform that provides user access control and user traffic visibility for all local and remote employees, contractors, and partners. It safeguards the organization's critical resources, applications, and data irrespective of their location – inside the campus, inside public or private cloud, SaaS, etc. from unauthorized access.

Most importantly, ColorTokens SUA provides deep visibility into traffic, to and from user devices. This granular visibility enables security administrators to view unauthorized and malicious access attempts made by the users.

ColorTokens Secure User Access Benefits

L3-L7 Protection
Malware on infected user device cannot access and scan protected business application and resources.

Dual Authentication
Increases the level of security by denying application access to unauthorized users and devices.

Zero-Trust Based Granular Access
Users allowed access to whitelisted applications only - all other access attempts are blocked.

Dynamic and Granular User Access Policies
Contextual policy attributes control user access based on user's geo location, type of OS, department, role, home/ remote location, and WiFi.

Integration with Active Directory
User authentication with Active Directory. User's group and Department details fetched from Active Directory.

Supports Single sign-on using SAML.

Operational Ease
No configuration changes for new and separated employees. The administrator is not required to configure or remove the access policies for new and separated employees.

Access Control without Changing Application
Access control to applications without requiring changes to the applications. Access control to applications that don't natively support authentication.

Passive Authentication
Visualization without requiring the user to log in, based on the user machine login. The user login id validates against Active Directory, and the same is used in visualization to display traffic to/from the user's device.

Powerful Visualization
Department-wise user access to applications. The administrator can see session details like what did the user access, at what time, bytes of data transferred, including user identity and device identity.

ColorTokens Secure Remote Access

Application Access

Remote users get access only to specific applications and not to the entire corporate network, thereby reducing the perimeter of the attack surface.

Integrated Platform

A single management interface for onsite and remote user access.

Seamless Activation

Auto on/off: the remote access gets auto activated when the user accesses a corporate application from a remote location and is disabled when the user connects to the office network.

Mobile Policies

Access policies are consistent for onsite and remote users. To ensure the security of critical applications, the administrator can prohibit remote access to critical applications.

Heightened Security with Encryption

Traffic from remote users is encrypted end-to-end using strong encryption, AES-GCM-128, and AES-256.

Geo View

Geo view displays connected user's location along with other details like user identity, device identity, remote access duration, bytes transferred in and out, and more.

Built-in Multi-Factor Authentication

Remote access is allowed only after validating the device and user identity, escalating security, even when user credentials are stolen.

Enterprise Network Security

Enhance security by disallowing IP/Network level access and allowing access only to authorized whitelisted applications.

Not Limited to Web Applications

Remote users can access internal applications over any protocol.

Seamless User Experience

No technical skills needed. Auto on/off and a single sign-on experience delivered with SAML integration, even for remote users.

Conclusion

There is no denying that users are the weakest link in security. But providing flexibility to users and collaboration with your eco-system partners is critical for business agility and success. Despite significant investments in traditional user access security, end-users continue to be the prime cause of breaches and data exposure. Using an effective and secure access control and visibility solution will enable organizations to drastically reduce the attack surface, thereby increasing the overall security of critical business applications and resources.

Research sources:
https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html
https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/
https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf
https://www.gartner.com/smarterwithgartner/next-generation-trends-in-identity-and-access-management/
https://securityintelligence.com/current-trends-in-identity-and-access-management-july-2017/

COLORTOKENS

colortokens.com sales@colortokens.com

ColorTokens is a Silicon Valley company, backed by legendary investors and advisors who have helped structure the IT industry over last 30+ years. ColorTokens' core team brings deep and innovative industry experience from brands such as Cisco, Juniper, VMware, Microsoft, and Zscaler in domain areas including cybersecurity, networking, and infrastructure. With customers and partners worldwide, ColorTokens is headquartered in Santa Clara (Silicon Valley), CA, USA with a major center of development and sales in Bengaluru, India.