COLORTOKENS

USE CASE BRIEF

Defending Legacy Systems against Advanced Attacks

Many organizations are still dependent on legacy systems because they're hard to replace and because many core enterprise applications still run on legacy systems inside the data center. Since these legacy solutions no longer receive technical support or OS patches/software upgrades, they are vulnerable to cyberattacks that could compromise the entire network. Additionally, legacy systems are inherently vulnerable to exploitation by bad actors using phishing and self-spreading malware—a memorable example being the WannaCry ransomware attack in May 2017, which cost the National Health Services of the UK close to £9.2 million (approx. US $12 million). With the cyberthreat landscape evolving faster than security teams' ability to update and replace legacy systems, securing legacy systems against cyberattack has become a key priority for organizations.

Security risks associated with unprotected legacy systems

Unsupported legacy systems give attackers opportunities to infiltrate the network and move laterally to gain access to sensitive data and critical applications. With no support or patches to address these security vulnerabilities, legacy systems can put businesses at risk for costly data breaches. Hackers make use of the end-of-support dates available online to find zero-day exploits that haven't been patched. One notable example is the BlueKeep vulnerability in May 2019, which affected more than 240,000 machines worldwide. In the wake of recent zero-day attacks, organizations must focus on taking the right cybersecurity steps across all systems while keeping their operations up and running. This is critical as it prevents downtime of their operations, potential revenue loss, and regulatory penalty.

Traditional security vs. proactive security

Network firewalls and network-based segmentation approaches don't address unpatched vulnerabilities associated with legacy workloads. Also, deploying these tools can be complex and expensive. In order to mitigate the security challenges posed by traditional practices, organizations need a proactive Zero Trust approach to securing legacy systems. Legacy workloads must be secured from any and all unauthorized access using granular least-privilege policies, implemented through Zero Trust identity-based segmentation and comprehensive, continuous visibility and assessment of security posture.

Securing legacy workloads based on Cyber Security Framework

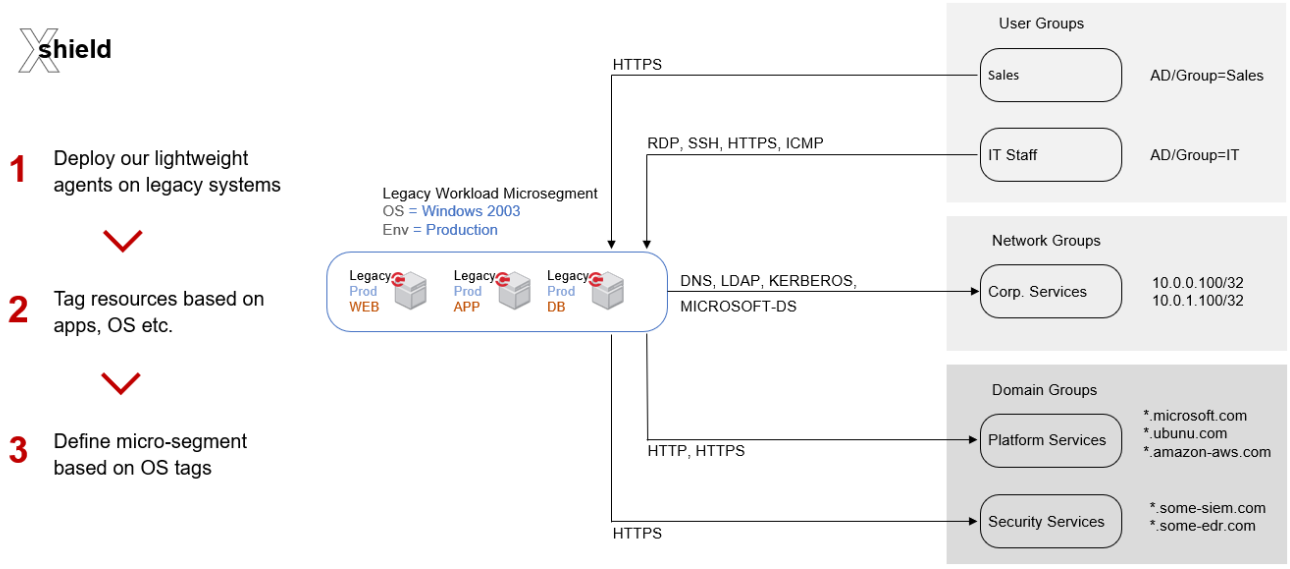
Identity-Based Micro-Segmentation	
Define and Observe Security Policy	• Observe Mode • Zero Trust Secure Zones • Group Using Attributes
Enforce Policy	• Dynamic Policy • Secure Role-Based User Access

Visualize Network	
Record	• Capture Network Data and flows • Preserve Evidence of breach
Dynamic Views	• See Transactions in Real Time • 3000 Feet To 3 Feet Views
Search / Metadata	• Over 2000 Attributes • App Awareness

ColorTokens' approach to enabling proactive cybersecurity

ColorTokens extends support to data center legacy systems, including vulnerable and unpatched applications running Windows 2003, XP and above by performing identity-based segmentation and offering comprehensive network visibility. Many cybersecurity vendors don't offer support for legacy systems beyond Windows 7, which can increase vulnerability for customer assets that share applications or have traffic flowing in a hybrid environment. Our solution ensures that the customer can manage their unpatched systems without compromising the security of their assets or network. Our solution also investigates security issues while providing complete visibility and reducing lateral movement.

How ColorTokens' Xshield performs micro-segmentation on legacy workloads



Protect legacy workloads in 3 simple steps using ColorTokens' Xshield

1

Get a detailed, contextual visualization of your assets and associated threat posture, with vulnerability exposure

2

Deploy granular micro-segmentation, isolate and protect sensitive or critical legacy workloads

3

Easily manage security policies for multi-cloud, data center and legacy environments, with one consistent view

Xshield is available for the following OS versions

Supported user OS

Xshield agents for clients (end users) are available for MacOS and Windows OS families.

OS Family	Supported Versions
MacOS	OS 10.10 and above
Windows 64-bit	OS 7 and above

Supported Workload OS

Xshield agents for workloads are available for AIX, Linux, and Windows OS families.

OS Family	Supported Versions
Windows 32-bit	OS XP SP3 and above
Windows 64-bit	OS 2003 SP2 and above
MacOS	OS 10.10 and above
Ubuntu	OS 12.4 and above
Redhat	OS 6.7 and above
CentOS	OS 6.7 and above
SUSE	OS 12 and above
AIX	OS 7.1 and above

Schedule a Demo

or send your query to info@colortokens.com

About ColorTokens

ColorTokens is a leader in delivering innovative and award-winning cyber security solutions. It is a US corporation headquartered in Silicon Valley with offices in the US, the UK, Europe, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please go to **colortokens.com**

© 2024 ColorTokens. All rights reserved.