COLORTOKENS

TECHNICAL BRIEF

Defending Legacy Systems against Advanced Attacks

Many organizations remain reliant on legacy systems due to the complex nature of migration and the continued dependence of core enterprise applications residing within data centers. These outdated solutions, however, pose a significant security challenge. Legacy systems often lack crucial security updates, including operating system (OS) patches and software upgrades, due to discontinued vendor support. This renders them susceptible to various cyberattacks that could compromise the entire network. Attack vectors include exploitation of known vulnerabilities through phishing attempts, self-propagating malware, and zero-day exploits – previously unknown weaknesses attackers can leverage. The ever-evolving cyber threat landscape outpaces the ability of security teams to update or replace legacy systems entirely. Therefore, securing these outdated systems against cyberattacks has become a paramount concern for organizations.

The infamous WannaCry ransomware attack of May 2017 serves as a cautionary tale. This attack, exploiting an unpatched vulnerability in a legacy system, crippled the UK's National Health Service, incurring an estimated cost of £9.2 million.

The recent cyberattack on Change Healthcare in February 2024 highlights the critical importance of robust cybersecurity measures. Despite the company's founding in 2007, some core systems handling sensitive patient data reportedly ran on legacy operating systems, potentially 40 years old. Security experts believe this reliance on legacy OS may have played a significant role in the attack's success.

Security Perils of Unprotected Legacy Systems

Keeping legacy systems secure is a constant battle. These vital systems often lack ongoing updates, leaving them exposed. Patching them can be risky too - updates might destabilize the system. Vulnerability scanners also struggle with legacy systems due to outdated databases and complex code, leading to inaccurate results. Additionally, the lack of automation in legacy systems requires manual patching, increasing human error and delaying security fixes. To effectively mitigate these security risks, organizations must adopt a proactive Zero Trust framework for safeguarding legacy systems. This entails implementing granular least-privilege policies to restrict unauthorized access to legacy workloads. Additionally, organizations should employ Zero Trust identity-based segmentation techniques and maintain comprehensive, continuous visibility and assessment of their security posture to ensure robust protection against evolving threats.

Exploring Your Options with ColorTokens

With ColorTokens, you have two available options. If you choose the agent-based approach, we provide support for certain older operating system versions(Please refer Appendix). Alternatively, for devices that cannot accommodate agents, ColorTokens offers an agentless Gatekeeper solution. This option enables protection for any legacy device, mainframe, AIX system, or other compatible infrastructure.

ColorTokens' approach to enabling proactive cybersecurity with Gatekeeper Appliance

As organizations grapple with the intricate terrain of legacy devices, the ColorTokens Xshield Enterprise Microsegmentation Platform with the Xshield Gatekeeper Appliance emerges as an indispensable solution. The imperative of securing legacy devices cannot be overstated, and the Xshield Gatekeeper Appliance epitomizes a comprehensive security solution, seamlessly extending its protective capabilities to a myriad of devices. It embraces robust security measures that enable streamlined management, auto-tagging, and context-aware policies, thereby facilitating swift responses to emergent threats. With its templatized policy management and comprehensive firewalling capabilities, organizations can exert granular control over all connected devices, heightening their cybersecurity posture in an ever-evolving threat landscape. The Xshield Gatekeeper appliance supports both static and dynamic IPs, as well as all network topologies, offering multiple deployment options. Serving as a holistic and pragmatic choice for safeguarding industrial processes, and by aligning with the Purdue Enterprise Reference Architecture (PERA) model, organizations can proactively confront the challenges of Legacy devices and IoT/OT security, mitigate lateral movement vulnerabilities, and fortify their critical infrastructure against evolving cyber threats.

How ColorTokens' Xshield performs micro-segmentation on legacy workloads

Solution Approach

1. 

Comprehensive Legacy Assets Idnetification, Discovery & Mapping

2. 

Visualize traffic flows to identify legitimate traffic communication

3. 

Define Zero Trust Segmentation Policies

4. 

Develop a Secure and Legacy-Compatible Template-Based Blueprint for expansion of new clusters

Deployment Approach

ColorTokens (CT) - Gatekeeper Device Bring up and Configuration :

Power on CT-Gatekeeper

Access the Appliance Console and configure

- Configure the WAN interface with upstream router IP as default gateway
- Configure the LAN interface with IP from the Subnet which needs to be segmented

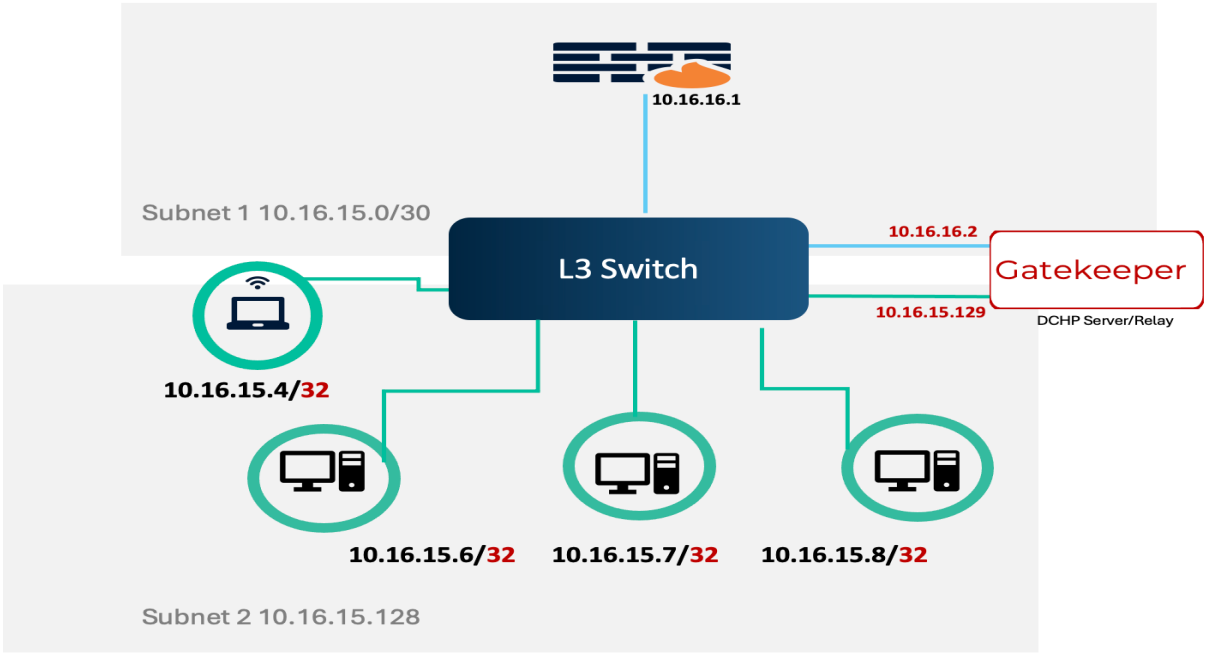
Configure Upstream router :

- Disable the DHCP pool for subnets which are protected using CT-Gatekeeper

On Endpoints :

- As part of DHCP renewal the devices will automatically receive /32 IP address from the CT-gatekeeper
- For devices with static IP , change the netmask to /32 and gateway as CT-gatekeeper LAN IP

Reference – Example of a typical environment with Legacy devices



All traffic is routed through Gatekeeper delivering full visibility and granular policy enforcement

Sequence

- CT-Gatekeeper is installed next to L3 switch with two arms (interface) connected to L3 switch.
- CT-Gatekeeper becomes the default gateway for all the devices within the protected VLAN(s) 10.16.15.0/24
- DHCP relay enable devices will receive existing IP with an isolated mask of /32
- For devices with static IP subnet mask should be updated to /32 & gateway to CT-Gatekeeper's IP

ColorTokens' Gatekeeper solution addresses the unique security challenges posed by legacy devices with its robust, agentless approach tailored specifically for such environments. By establishing a secure, virtualized micro-perimeter around the legacy device, the Gatekeeper effectively segregates it from the wider network, thereby significantly reducing the potential attack surface and thwarting the lateral movement of potential threats. Furthermore, the Gatekeeper's capability to monitor and regulate network traffic to and from the legacy device enables real-time anomaly detection and automated mitigation measures, thereby further fortifying the overall security posture. This agentless methodology eliminates the need for intricate installations or modifications to the legacy system itself, rendering the Gatekeeper a user-friendly and efficient solution for safeguarding these critical assets.

Appendix

Xshield Agent OS versions Support:

All server agents are supported only for X86_64 (X86 64-bit architecture).

Platform	Support(Yes/No)	Notes
RHEL 4.x	No	
RHEL 5.x	No	
RHEL 6.x	No	
RHEL 7.3 and Above	Yes	
Rocky Linux 8.x	Yes	
Rocky Linux 9.x	Yes	
AIX 7.1, 7.2	Yes	AIX 7.1 on power 6 and AIX 7.2 on power 8 only
Solaris 11.0(x86)	No	
Windows MS Windows Server 2003	No	
MS WIndows Server 2008 Enterprise	No	
MS WIndows Server 2008 R2 Enterprise	Yes	
MS WIndows Server 2008 Standard	Yes	
MS WIndows Server 2008 Standard	Yes	

Xshield Agent OS versions Support:

Platform	Support(Yes/No)	Notes
MS WIndows Server 2012	Yes	
MS Windows Server 2016	Yes	
MS Windows Server 2019	Yes	
MS Windows Server 2022	Yes	
Oracle Linux 6.x	No	
Oracle Linux 7.x	Yes	
Debian 7.7	No	
Debian 9	Yes	
Debian Ubu 18, 20	Yes	
Centos 7.3 and Above	Yes	
Suse 12	No nftables is not supported	
Suse 15	Yes	Only x86 architecture is supported. PPC is not supported

About ColorTokens:

ColorTokens, the leading enterprise microsegmentation company, stops the lateral spread of ransomware and malware within an organization's diverse network topology. The ColorTokens Xshield platform visualizes traffic flows between workloads, devices, and the internet, enforces granular micro-perimeters to stop unauthorized traffic, and isolates crown-jewel assets and compromised systems in response to a breach. ColorTokens protects organizations by stopping ransomware and malware in their tracks, saving millions of dollars in business operations interruption.