COLORTOKENS

Use Case Brief

Xshield

Environment Separation

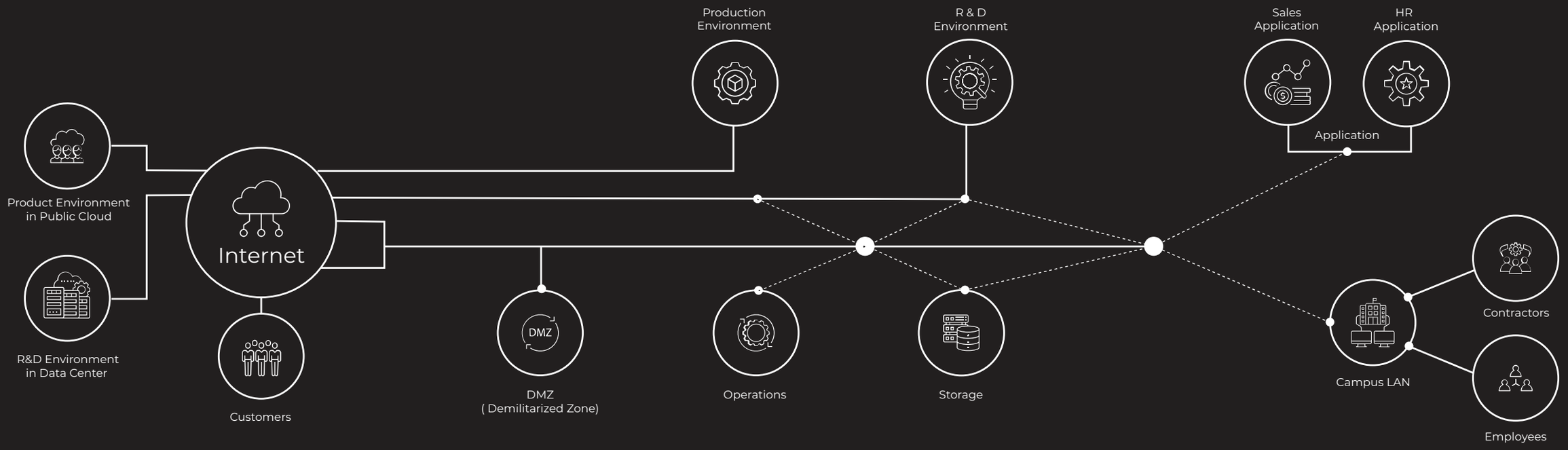
Secure environment separation of applications, workloads, and servers

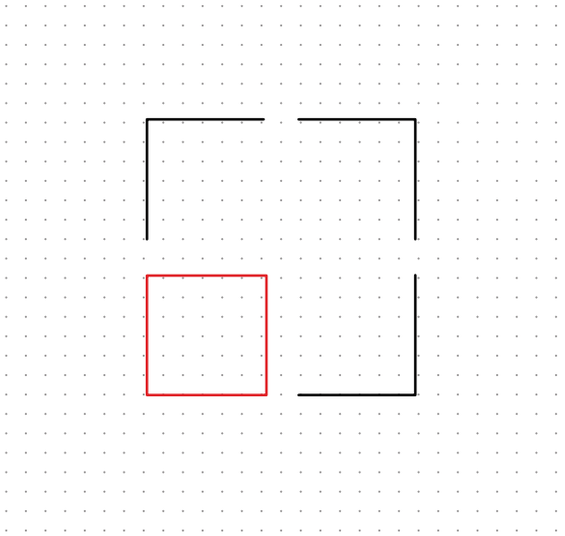
Request a Demo

Overview

Internal networks for enterprise often span hybrid, multi-vendor environments and are primarily flat. The distributed assets cause security and compliance concerns because sensitive corporate assets and systems could be at risk of being breached. Segmenting and isolating sensitive assets and environments can improve security posture and ensure compliance. Traditional segmentation techniques, like VLANs, are static and costly to implement in modern networks where assets are dynamic and distributed. Businesses need agile security combined with simplicity and flexibility when segmenting their distributed systems and environments across different networks.

ColorTokens' Xshield creates flexible, dynamic zero trust secure zones around protected systems, servers, and environments with just a few clicks. The security boundary moves with the infrastructure environment, maintaining separation, reducing the attack surface, and preventing unauthorized or malicious access. It allows customers to isolate and protect their critical systems in development, staging, and production, without impacting the underlying infrastructure.



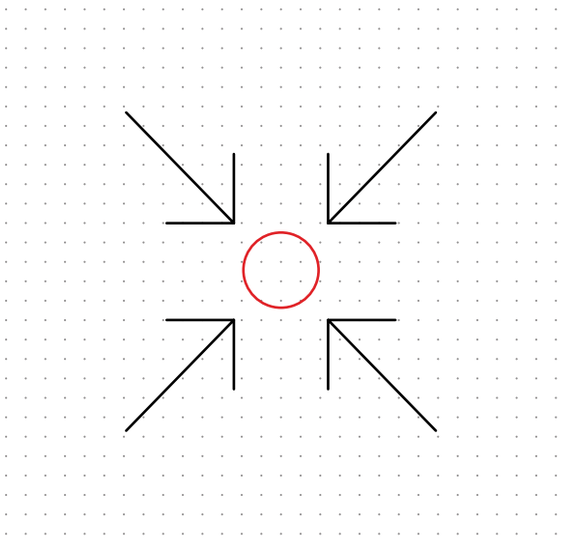


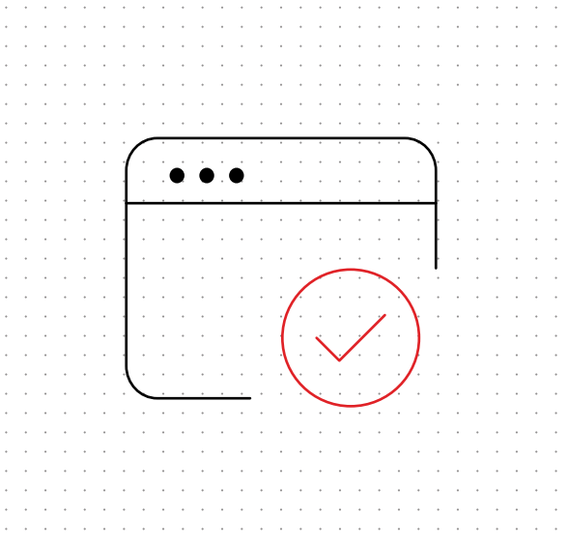
Adopt Micro-Segmentation Faster

Xshield enables enterprises to visualize and define micro-segmentation boundaries for internal network segments using customizable tags and attributes. This powerfully streamlined and secure approach to segmentation blocks the exfiltration of sensitive data from known or unknown bad actors.

Simulate Recommended Policies to Determine Impact

Policies can be built based on automated recommendations and visually modeled to understand the impact of enforcement. For example, it can be intuitive to logically group workloads or systems that grant similar access privileges when endpoints access these assets, and when the tiers in applications or services work independently.





Implement Policy Audits Faster

Xshield enables complete historical visibility of alerts, network, and traffic flow, real-time visibility of availability, health status, and traffic data across a multi-cloud and hybrid environment. A single comprehensive view allows visualization of misconfigured DNS servers or unauthorized access of production servers to the public internet, enabling an audit of compliance issues.

Xshield

Software-Defined Micro-Segmentation

VS

Traditional

Hardware (Network) Based Micro-Segmentation

Accelerated Implementation with Automated Policy Recommendation

Gain reusable security policy templates, server roles, and resource access parameters. Create a corporate policy template to enforce faster implementation.

Scalability

Map business applications to server roles, security, and connection information across the multi-cloud and hybrid environment. Dynamic policy tools adapt faster to the changing IT environment

Interoperability

The platform-agnostic implementation runs across bare-metal servers, end-user computers (Mac, Windows, Legacy OS),or cloud-hosted virtual machines,containers, or instances. It seamlessly integrates with identity apps, SIEM apps, and vulnerability tools.

Resource-Intensive

Segment using subnets, Hypervisor, and firewalls. Not scalable with a multi and hybrid cloud environment. Configuring new assets is resource-intensive and can create challenges in implementation.

Unnecessary Complexity

VMs located on the Hypervisor are not platform agnostic and do not communicate with other resources in a multi-vendor environment. The Hypervisor needs protection to comply with the enterprise security policy.

High Cost and Integration

Capital-intensive advanced firewalls are required to segment the network and ensure no performance degradation in data throughput. It requires creating and managing thousands of firewall rules. Multi-vendor resources may not be compatible with these firewall rules.

ColorTokens Inc., a leader in proactive security, provides a modern and new generation of security that empowers global enterprises to singlehandedly secure cloud workloads, dynamic applications, endpoints, and users. Through its award-winning cloud-delivered solution, ColorTokens enables security and compliance professionals to leverage real-time visibility, workload protection, endpoint protection, application security, and Zero Trust network access—all while seamlessly integrating with existing security tools. For more information, please visit www.colortokens.com.