Deep Visibility and Software-Defined Identity-Based Segmentation

A Modern Approach to Segmentation

The dramatic rise of east-west traffic inside the network and the inability of perimeter firewalls to provide visibility into the internal network has made it challenging to block hackers and users on the inside. Most traditional hardware-based solutions such as VLANs and firewalls are complex and costly to deploy inside the network, do not deliver granular segmentation, and are ineffective at preventing lateral movement and breaches. Today’s enterprises need a modern approach that provides complete visibility, both north-south and east-west, into internal traffic, proactively discovers vulnerabilities, and protects business critical assets such as servers, applications, and workloads with identity-based segmentation based on a Zero Trust architecture.

The threat landscape is continuously evolving across enterprise assets running business-critical workloads that need proactive security solutions to protect from hidden and emerging threats. Segmenting these assets, improving security, and ensuring compliance constitute the best strategy to protect against threats, but implementing this strategy can be time-consuming and challenging with traditional security solutions. Enterprise IT environments have grown from primarily on-premises data centers and private cloud into hybrid cloud consisting of on-premises, private, public and multi-cloud. This has complicated security requirements many fold. Even after investing in several high-capacity firewalls and intrusion detection systems, enterprises always worry about security breaches that may be lurking ‘undetected’ across their hybrid cloud assets.

Key attributes to look for in a micro-segmentation solution

- VISIBILITY
- COVERAGE
- ADAPTABLE
- GUIDED EXPERIENCE
- TIME TO VALUE
- NON-DISRUPTIVE IMPLEMENTATION
The Solution: Identity-based Micro-segmentation

Identity-based segmentation, or micro-segmentation for hybrid infrastructure, delivers a zero trust approach to address the security flaws that plague today’s enterprises.

It is a security best practice that divides the business critical network and associated applications (crown jewels) into granular, isolated segments so that traffic to and within these segments can be monitored and controlled.

In doing so, organizations proactively reduce the attack surface to a minimum while preventing any unauthorized lateral movement. Micro-segmentation is a vital pillar of the zero trust security framework.

Analysts recommend that organizations implement micro-segmentation to defend against stealthy attacks inside the network, whether on-premises or in the cloud.

Choosing the Right Micro-Segmentation Solution

The thought of undertaking a significant security project like micro-segmentation can be daunting – especially for large organizations that have thousands of applications and users, as well as numerous locations and clouds.

But with the right micro-segmentation solution, organizations can quickly secure and protect their crown-jewels without requiring a time-consuming installation or a lot of ongoing maintenance.

Key attributes of a micro-segmentation solution

Visibility: Organizations need deep visibility into lateral traffic and contextual data that helps them make policy decisions based on business intent.

Coverage: Micro-segmentation should be network infrastructure-independent, so it covers workloads across the data center and cloud. It allows micro-segmentation investments to be future-proof and avoid vendor lock-in or vendor lock-out.

Adaptability: Micro-segmentation solutions should adapt to changes in security needs with little to no human intervention.

Guided experience: Even for a small IT asset environment, micro-segmentation can be hard to implement. The solution should guide the security team with policy recommendations and automatic policy enforcement.

Time to value: Organizations should see value from a micro-segmentation tool in days, if not hours, and deployment should not involve months of planning and roll out. Every delay in planning and deployment, however small, is an additional opportunity for bad actors.

Non-disruptive implementation: Micro-segmentation should not disrupt your business and should be minimally invasive to your infrastructure and team.

We have to recognize that using micro-segmentation /micro-perimeter technology is a must for any organization seeking the benefits of a Zero Trust strategy”

Forrester
ColorTokens Xshield

ColorTokens’ software-defined, cloud-delivered platform simplifies application micro-segmentation and environment separation, reducing the attack surface and improving the overall security posture of your business-critical assets. ColorTokens Xshield enables enterprises to visualize and define micro-segment boundaries (micro-perimeters) for work assets using customizable tags and attributes.

Xshield auto-recommends policies based on the concept of least privilege, simulates the policies to remove uncertainty and then enforces seamlessly without disrupting business operations. This powerfully streamlined and secure Zero Trust architecture blocks the exfiltration of sensitive data from known or unknown insiders or bad actors. It protects assets at the workload level, whether on-premises or in the cloud, with a proactive approach to preventing advanced attacks.

Figure 1: Xshield Dashboard/ Architecture
Business Benefits

**Protection for business-critical applications**
Reduce the attack surface for your most vital applications and sensitive data.

**Cross-cloud visibility**
Gain unparalleled visibility into assets, applications, and data flows across your entire hybrid infrastructure, along with contextual data such as built-in vulnerability, threat, and exposure intelligence.

**Compliance assurance for PCI, HIPAA, and NIST**
Simplify compliance – and cut costs and time by reducing audit scope with segmentation and reporting.

**Environment separation**
Ensure hygiene of your production, test, and development environments by segregating environments in shared infrastructure.

**Cloud adoption and multi-cloud security**
Create application blueprints and migrate them with confidence, secure your data center and cloud applications with a single comprehensive platform.

**Breach containment and future-proofing**
Stop breaches from spreading laterally and proactively protect your business from future attacks.
The Xshield Approach to Micro-Segmentation

The Xshield approach to identity-based segmentation provides an intuitive user interface for understanding communications flows and implementing policies.

Figure 2: Top-down visibility to your environments, applications, and users
## Conclusion

In closing, it is critical for organizations to understand and acknowledge that attackers are well-adapted to bypass the security of traditional tools. As the industry-leading micro-segmentation platform, ColorTokens Xshield enables organizations to take back control by locking down internal enterprise networks, be it within their data center, or across clouds.

<table>
<thead>
<tr>
<th>Discover and visualize</th>
<th>Define and simulate</th>
<th>Enforce and protect</th>
<th>Report and refine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover assets in real-time</td>
<td>Define policies using the learning engine’s auto-recommendations</td>
<td>Protect with one-click policy enforcement</td>
<td>Generate reports for compliance needs</td>
</tr>
<tr>
<td>Visualize application access and communications</td>
<td>Identify and block unauthorized traffic patterns</td>
<td>Monitor policy violations</td>
<td>Leverage robust reporting tools for management</td>
</tr>
<tr>
<td>Understand security gaps and vulnerabilities</td>
<td>Adjust policies before enforcement</td>
<td>Secure unsafe communications with out-of-box encryption</td>
<td>Proactively plan and refine security posture of the organization</td>
</tr>
</tbody>
</table>

SOLUTION BRIEF
ColorTokens Inc. is a leading innovator in SaaS-based Zero Trust cybersecurity solutions, providing global enterprises with a unique set of products and services for securing applications, data, and users across cloud and hybrid environments. Through its award-winning Xtended ZeroTrust™ Platform and context-aware machine learning-powered technologies, ColorTokens helps businesses accurately assess and improve their security posture dynamically.

As cloud adoption grows, traditional perimeters get redefined, and new attack vectors and threat actors materialize, corporations recognize their security posture needs to reflect their Zero Trust philosophy. ColorTokens’ technology allows customers to achieve Zero Trust by utilizing rich, meaningful contextual information about the application, microservice, or protected resource, so customers can apply Zero Trust with as secure of a perimeter as they can. ColorTokens’ cloud-based SaaS platform can automatically deploy next-generation security controls and increase security posture dynamically without any new hardware, downtime, reboots, or changes to a client’s existing systems.

With a team of over 400 people, ColorTokens has global office locations in Santa Clara, California; New York; London; Copenhagen, Denmark; and Bengaluru, India.

For more information, please visit colortokens.com