COLORTOKENS

SOLUTION BRIEF

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 to security. Organizations need complete visibility, north-south, and east-west, into internal traffic, proactively discovering vulnerabilities, and protecting business-critical assets such as servers, applications, and workloads with identity-based segmentation based on a Zero Trust architecture.

The threat landscape continuously evolves 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, complicating security requirements many folds. 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.

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 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.

Key attributes to look for in a micro-segmentation solution

- VISIBILITY
- NON-DISRUPTIVE
- IMPLEMENTATION
- COVERAGE
- ADAPTABILITY
- GUIDED EXPERIENCE
- TIME TO VALUE

Choosing the Right Micro-Segmentation Solution

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

Adaptability

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

Non-disruptive implementation

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

Coverage

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

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 rollout. Every delay in planning and deployment, however small, is an additional opportunity for bad actors.

> ***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 and accelerates the adoption of application micro-segmentation and environment separation, reducing the attack surface and improving the overall security posture of your business-critical assets. Enterprises using Xshield can visualize and define micro-segment boundaries (microparameters) for work assets using customizable tags and attributes. Xshield enables enterprises to discover assets both on-premises and in the cloud in seconds.

Xshield auto-recommends policies based on the concept of least-privilege, simulates the policies using an ML-based policy engine 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.

ColorTokens Xshield Dashboard / Architecture

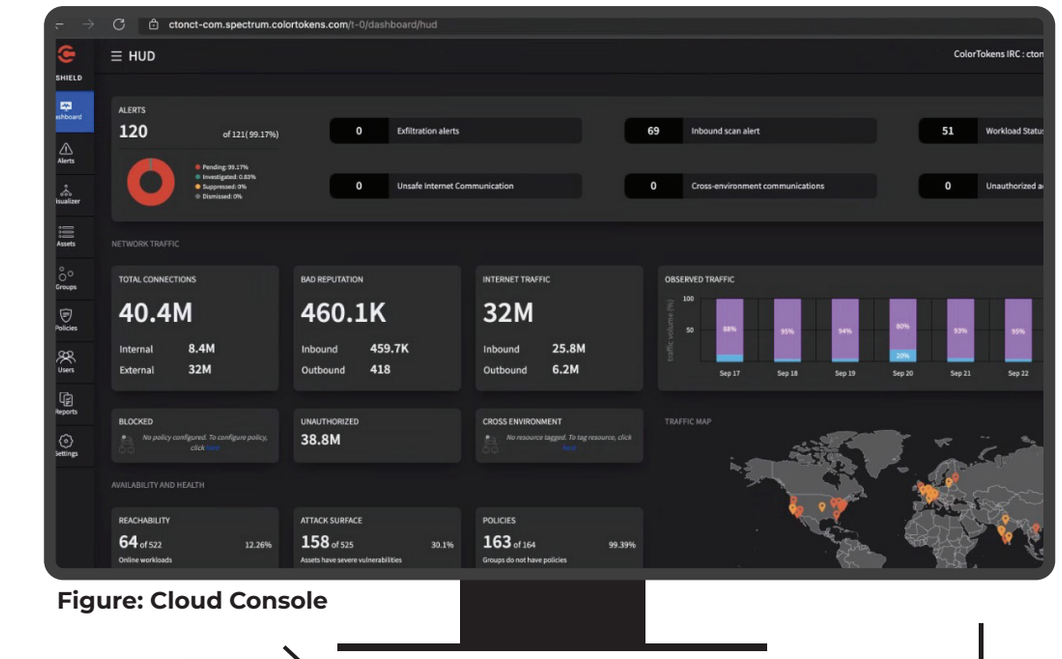

Figure: Cloud Console

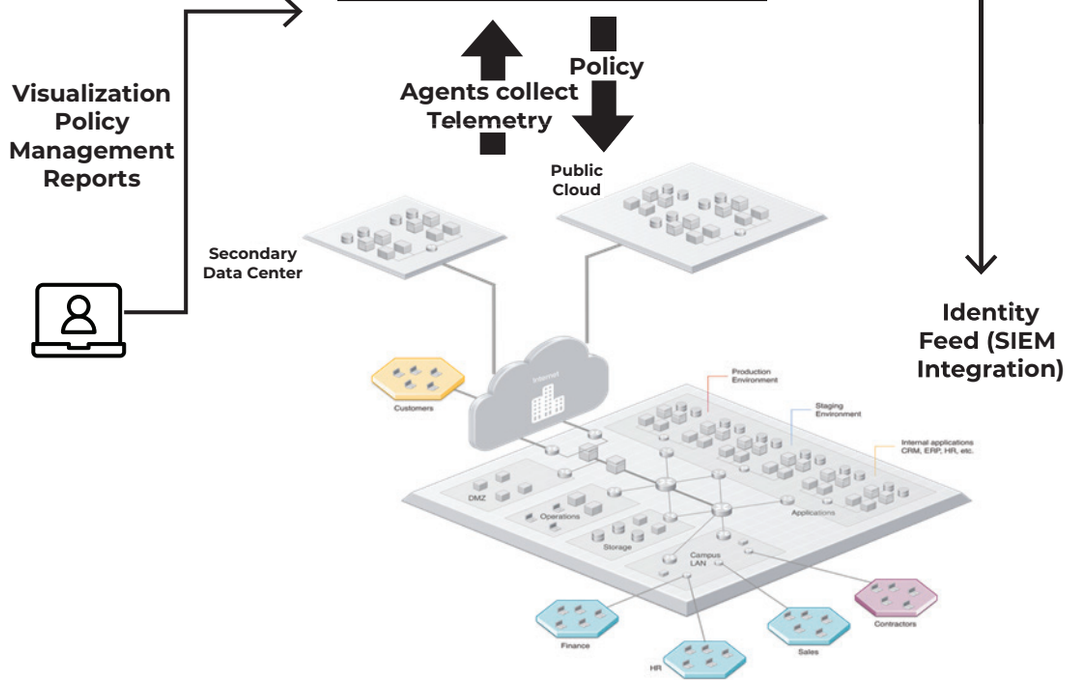

Figure 1: Xshield Dashboard/Architecture

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, migrate them confidently, and secure your data center and cloud applications with a single comprehensive platform.

- **Breach containment and futureproofing**

  Stop breaches from spreading laterally and proactively protect your business from future attacks.

The Xshield Advantage

Xshield introduces several innovations that enable even small teams to secure large-scale environments.

Operational Excellence

No hardware or infrastructure dependencies and rapid deployment by creating Zero Trust Zones™ with a few clicks.

Policy recommendations reduce deployment effort and time for security teams from months to weeks.

The cloud-powered platform scales as your needs grow across multi-cloud or hybrid environments.

Turnkey and 24x7 managed service eases initial operational and maintenance effort and reduces the burden on IT security staff.

Enterprise Capabilities

Both agent-based and agentless solution provides native support for cloud workloads using cloud APIs.

The unified platform integrates existing workflows with APIs and out-of-the-box connectors for popular enterprise tools.

Infrastructure-agnostic across all workloads and legacy operating systems eases installation and reduces the need for multiple point solutions.

Meet the needs of auditors, InfoSec team, and executives with visual reports and streamline compliance for PCI, HIPAA, and other audits.

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.

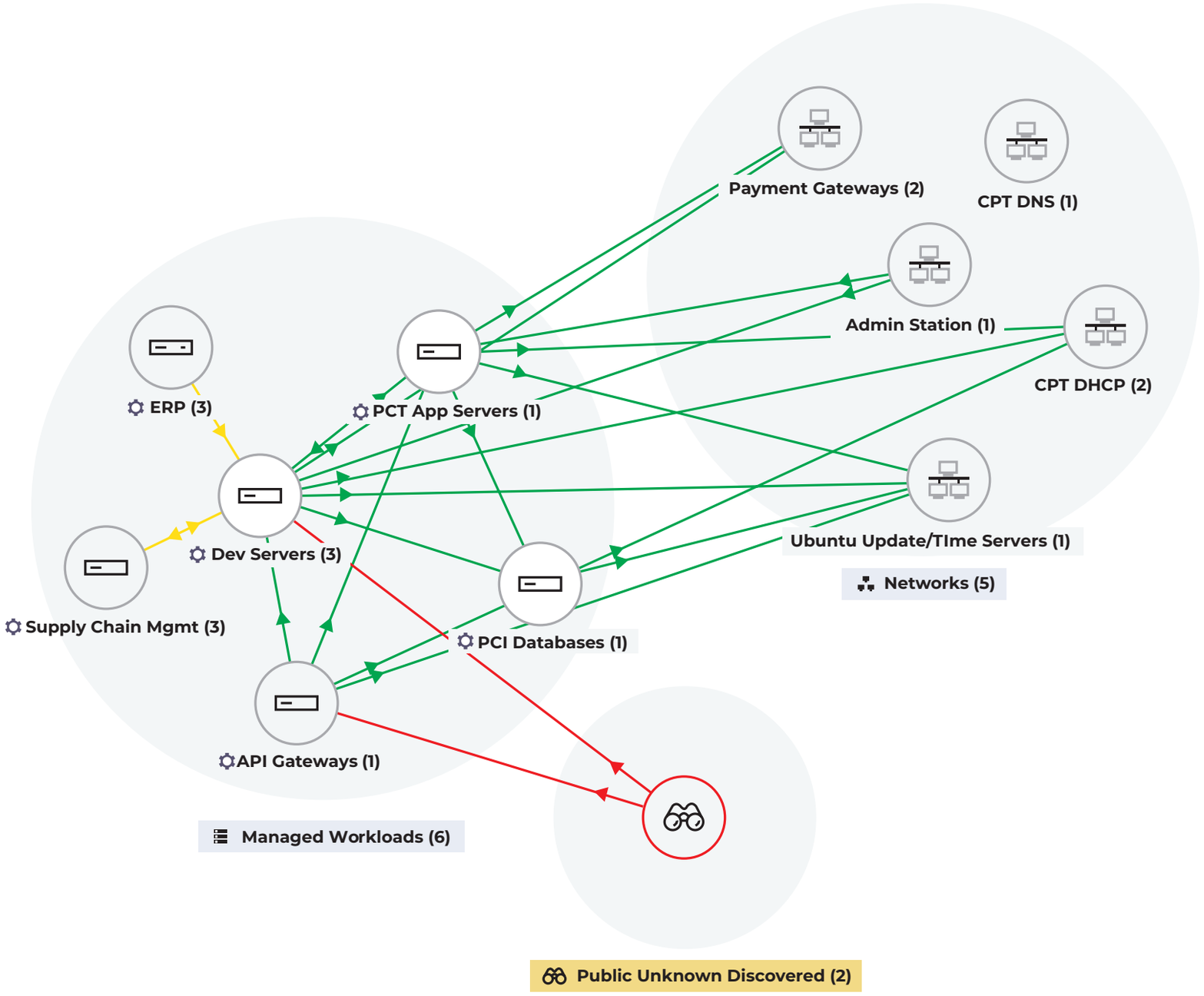

Figure 2: Top-down visibility to your environments, applications, and users

Conclusion

In closing, organizations must 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 within their data center or across clouds.

Our business value

Discover, visualize, and classify with tags in minutes

- Discover assets in real-time
- Visualize application access and communications
- Understand security gaps and vulnerabilities
- Automatically identify and classify assets with automated tags
- Tag rule and integration with cloud workloads
- Use intuitive FQL based rules to tag current and future assets

Define, simulate, enforce and protect in days

- Granular service level segmentation within application with auto-grouping
- Customize and automate policy recommendations using ML engine
- Block suspicious communication before enforcing zero trust mode
- Secure workloads instantly by replicating policy templates
- Protect with one click policy enforcement and monitor policy violations
- Secure unsafe communications with out-of-box encryption

Integrate with open APIs into your enterprise environment

- Instantly integrate into your existing environment
- Gain comprehensive view of security vulnerabilities in a single SIEM dashboard
- Proactively plan and refine the security posture of the organization.
- Deep dive into security logs with Public APIs and native integration.
- Consume audit logs with public APIs
- Filter specific assets with FQL keywords

Schedule a Demo

or send your query to info@colortokens.com

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 **www.colortokens.com.**