CROWN JEWELS PROTECTION

Enterprises have sensitive assets distributed across different environments in their network, including critical applications running on bare-metal, traditional servers, cloud-hosted virtual machines, containerized workloads, and other host systems. Organizations lack visibility into what assets are in their network, where data exists in their distributed environment, who has access to data, and how the data is secured from malicious or unauthorized access. Regulatory requirements often enforce heavy penalties to underline the need to secure data. However, beyond compliance, organizations can have security weaknesses that put their most critical assets (crown jewels) at risk. The biggest risk to crown jewels security is from east-west communications of traffic flowing among devices and systems within the data center or cloud.

The consequences of a mission-critical application being compromised can be severe, including operational disruption, business continuity risks, legal consequences, possible breach of intellectual property, and reputational damage to name a few. Securing sensitive applications has thus become a top priority for organizations, both to ensure compliance and protect against breaches,

Gaining complete data visibility is essential to show data sensitivity across the organization and define critical (crown jewels) applications. Modern applications require integration with third-party suppliers, customers, and other market entities, increasing their risk exposure. The distributed nature of modern applications and the increasingly mobile workforce has created new and expanding attack surfaces. Visibility into the data sensitivity and application traffic flows helps to discover criticality for the enterprise, executives, or regulators. After mapping the data dependencies and the traffic flows, teams need to assign policies that enable identity-based access to the applications based on the sensitivity and business needs.

Enterprises need a platform-agnostic, easy-to-deploy solution that protects their crown jewels from unauthorized east-west communications and lateral movement. Xshield ensures that customers have complete visibility into their assets through a visual dashboard, gain insight into data-related business risk, and are continuously aware of the security posture of their crown jewels. The security policy is close to the data, and it moves with the assets as they shift from on-premises to the cloud.

Limitations of Existing Solutions for Delivering Flexible, Agile Micro-segmentation of Crown Jewels

- Perimeter firewalls and traditional hardware-based network segmentation tools do not provide the level of flexibility and agility needed for securing dynamic assets in today’s hybrid environments.
- These tools can be rigid, lacking east-west granularity, and manual policy creation can take weeks and months to implement, making them unsuitable for securing sensitive assets in distributed environments.
- Security policies need to scale up and down as workloads are added or removed, and need to be flexible and dynamic in nature, so sensitive workloads stay secure as they move from on-premises virtual machines to cloud

Key Customer Requirements for Proactively Securing Crown Jewels

Identify and Visualize Crown Jewels

Organizations need comprehensive visibility into their network, to visualize traffic flows and dependencies between assets, identify sensitive applications at risk of exposure, and accurately assess their attack surface.

Test Before Enforcing Policy

It is important to be able to simulate and observe the effects of micro-segmentation before enforcing. When defining granular security policies there may be un-intended consequences such as breaking the flow of communications for some applications, and this can be corrected in the simulation phase so that no harm is done in the deployment phase.

Security Policy Close to Data and Assets

Creating identity-based segmentation and control for sensitive assets ensures that policies are close to the application and more granularly enforced, and least-privilege access ensures that only the least amount of access needed for the job is allowed.

Automated Security Policy Definition

Identifying different asset groups, tagging them appropriately for policy enforcement, and maintaining policy updates when assets move can be a daunting and complex task, especially when you're dealing with hundreds or thousands of distributed assets. The use of AI/ML to automate these critical steps in micro-segmentation can reduce the burden on IT security teams by removing manual intervention as much as possible in the asset identification and policy definition phases. This considerably eases and accelerates deployment.

ColorTokens Xshield: Zero Trust Segmentation for Crown Jewels

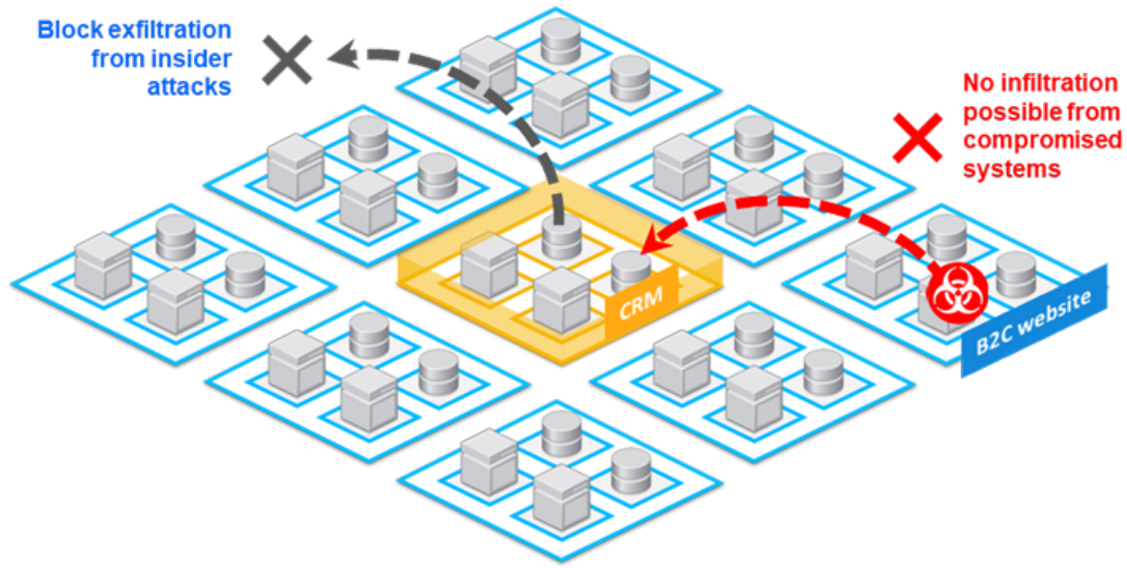

Figure 1. Xshield Identity-based Micro-segmentation.

Apply recommended policies, simulate, and enforce Zero Trust segmentation within days and weeks, not months.

ColorTokens provides a simplified, Zero Trust ("never trust, always verify") approach to securing an enterprise's most valuable crown jewels against cyberattack. ColorTokens Xshield is based on the NIST Zero Trust framework to address evolving new threats and compliance requirements. 100% cloud-delivered, SaaS-based for fast time-to-value, Xshield enables granular visibility, security, and control over applications and network assets to significantly reduce the attack surface and reduce the impact of breaches. Customers benefit from increased resilience to attacks, rapid containment, and minimal business disruption or downtime

ColorTokens Xshield is a vendor-agnostic micro-segmentation solution and provides comprehensive visibility into network traffic and deployed assets while preventing breaches and unauthorized east-west movement. The network flow analysis from its cloud-based console shows high-level and in-depth views into vulnerabilities and dependencies between applications, servers, and databases.

Built on an AI/ML-based policy engine, ColorTokens Xshield leverages automation for fast, easy implementation of Zero Trust segmentation and protection of crown jewels. Xshield's powerful policy engine automates the creation of Zero Trust secure zones (micro-perimeters) around critical assets. After simulation, least-privilege policies can be enforced with a single click, enabling Zero Trust segmentation. The identity-based micro-segmentation of crown jewels ensures that only authorized east-west communication is permitted, and the rule of least-privilege access is enforced. As a host-based solution, Xshield micro-segmentation is close to the application. This prevents any Command-Control (C2) communication from malware such as ransomware and limits malware propagation inside the network.

The Xshield Approach to Micro-Segmentation

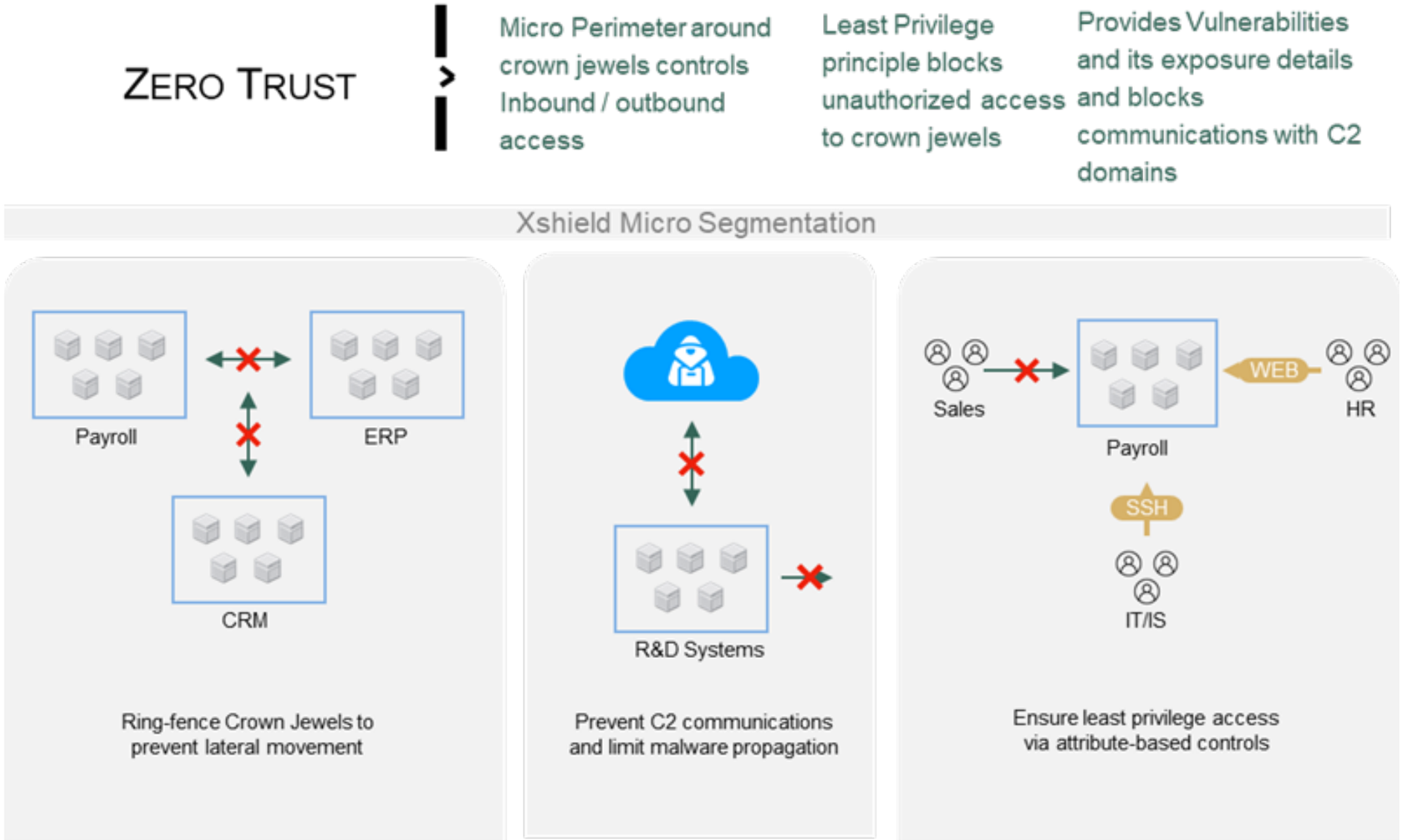

Figure 2. Xshield Zero Trust Micro-Segmentation

Business Benefits

Gain Complete Visibility

Xshield provides granular visibility into every communication between networks, applications, processes, and workloads. Its centralized dashboard collects telemetry data from all ColorTokens-managed resources. Security operators can thus achieve a comprehensive view of all traffic without using traditional technologies such as network taps or probes. The Skyview Visualizer provides summary views for CISO and security teams with high-level information, as well as deep filtering and drill -downs for detailed analysis to allow informed policy decisions and reduce business interruptions. We overlay security and Zero Trust data for impact analysis, reducing the risk of missed vulnerabilities.

Audit Network Traffic for Compliance

The traffic flows help administrators clarify how resources communicate amongst themselves, whether inside or outside the enterprise boundary. Attributes help to group resources for better cross-cloud visibility and to find compliance violations. Administrators can apply portable policy templates to resources and confirm compliance violations, such as misconfigured DNS servers or unauthorized access of production servers to the public internet.

Automate Policy Definition and Enforce with One Click

The automated policy tagging capabilities of Xshield define existing asset groups and boundaries effortlessly, providing automated policy recommendations with auto tagging and auto grouping of assets. Policy recommendations can be accepted or modified based on your business needs. With its powerful automated engine, Xshield can deploy, protect, isolate, and micro-segment sensitive assets in days, compared with traditional hardware-based segmentation that would take several months. Administrators can see the security policy changes in the asset environment reflected in the console and visualizer, with a dynamic policy graph showing real-time updates.

Detect Threats with Advanced Analytics

Xshield's built-in vulnerability assessment tool and integrations with threat intelligence feeds provide a multi-dimensional risk posture analysis for improved policy decisions. The robust threat analysis helps organizations stop zero-day attacks using telemetry data with powerful, filtered searches across more than 20 parameters. Customized notifications show where to focus on and reduce security vulnerabilities across a hybrid enterprise. Xshield's residual risk metrics help enterprises strategically assign resources to safeguard high-value, high-risk assets.

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.**