COLORTOKENS

SOLUTION BRIEF

Protect Your Digital Operations at Scale with EDR-Integrated Microsegmentation

No New Agents. No Complexity. Just Rapid Breach Readiness.

The Integration of Microsegmentation with Existing EDR Systems Quickly and Easily Improves your Security Posture

Microsegmentation is a foundational capability for a Zero Trust architecture. It creates isolated segments that are more granular than traditional VLAN network segments. This prevents attackers from moving laterally within the environment to access critical resources, degrade operations, exfiltrate data or encrypt systems for ransom. By stopping lateral movement, microsegmentation substantially minimizes the potential damage from a breach and lets you quickly return to normal operations.

ColorTokens delivers instant visibility and granular microsegmentation with no additional agents

ColorTokens Xshield leverages your existing EDR system to visualize assets, monitor traffic and enforce policies. No additional software needs to be tested, qualified and installed on endpoints and servers to gain the benefits of Zero Trust microsegmentation. The Xshield SaaS policy engine connects to the EDR platform already deployed in your organization's environment like **CrowdStrike Falcon®, SentinelOne Singularity**™, or **Microsoft Defender**, providing the ability to quickly and seamlessly develop and deploy policies to stop the lateral spread of malware or ransomware. In less than one hour, you can connect the Xshield SaaS policy management system to your existing EDR implementation and have complete visibility into all assets and traffic in your landscape.

Using the telemetry and asset data from the existing EDR platforms, ColorTokens' network map visualization interface enables admins to view endpoints and traffic in the environment using over 20 drill-down dimensions, such as assets, applications, dependencies, physical location, custom attribute tags, and others (as shown in Fig 1.).

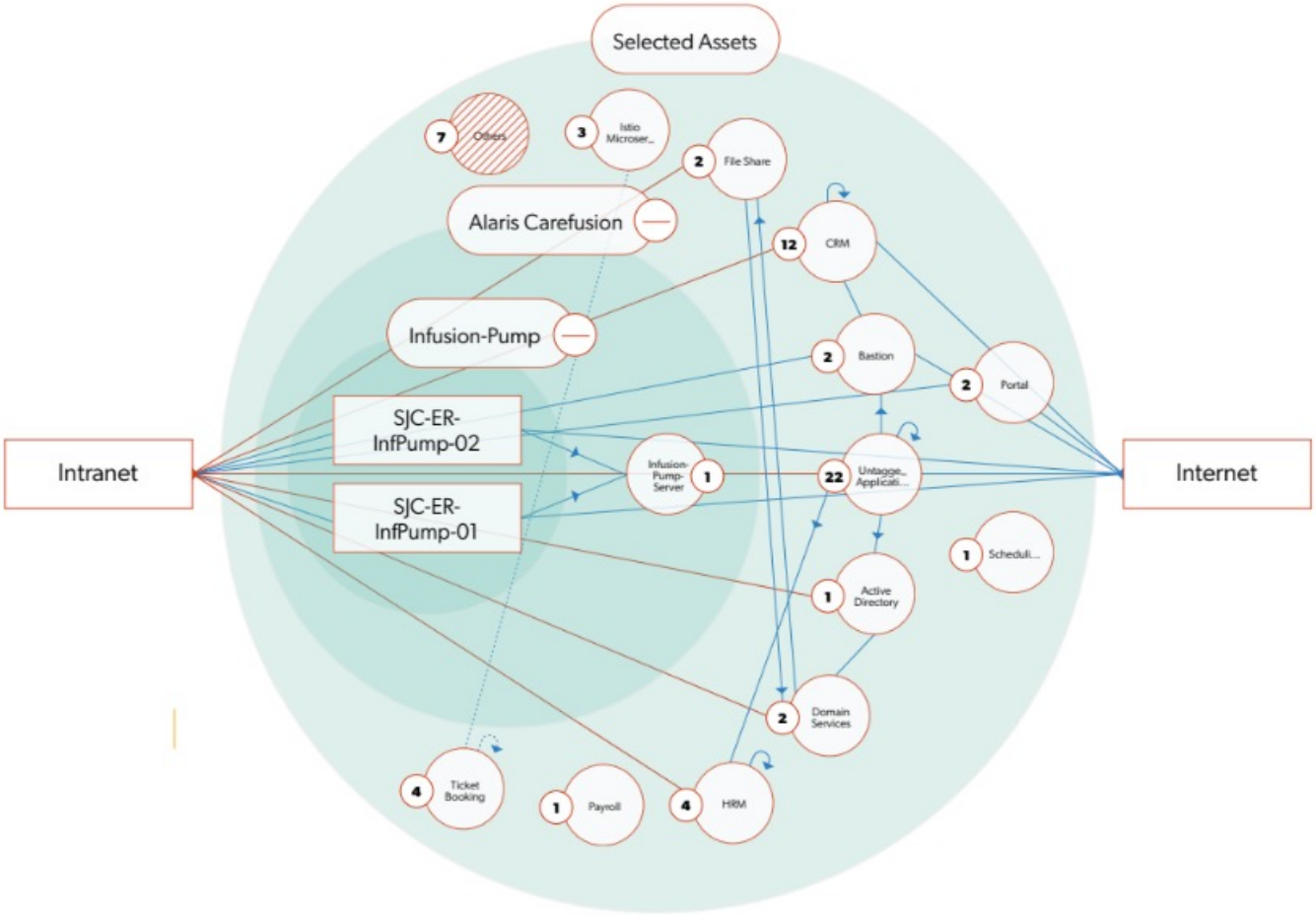

Fig 1. ColorTokens Xshield Network Asset and Traffic Visualization

This means that different user personas, such as the security, application, and infrastructure teams, each have their own view of the environment that best fits their needs. The Xshield mapping user interface provides visibility into the whole enterprise. It provides a focal point for traffic analysis and Zero Trust policy design.

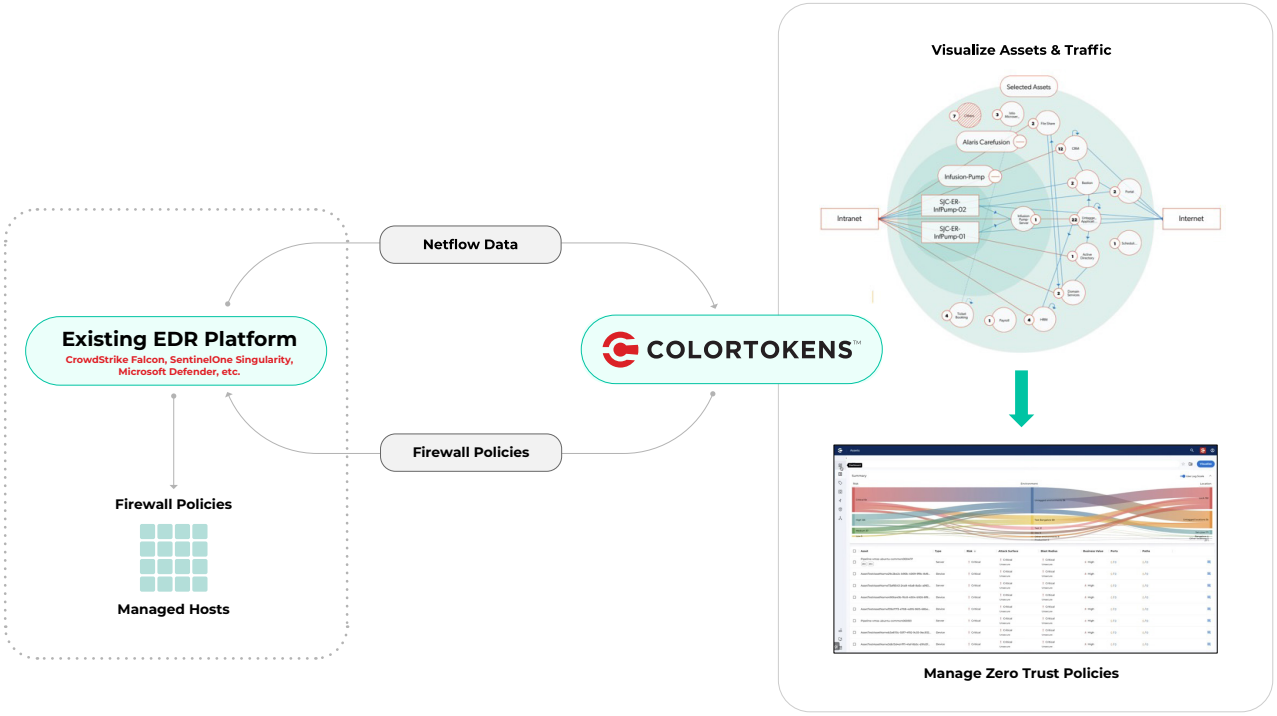

Fig 2. EDR and Microsegmentation: Integrated Architecture

Zero Trust communications policies are configured in the Xshield console, which programs the enforcement rules on the hosts using the existing EDR platform, as shown in Fig. 2 above. These Zero Trust policies allow authorized traffic to proceed and stop out-of-policy traffic, preventing an attacker from spreading malware and ransomware throughout the enterprise.

Top Use Cases

Ransomware Containment: If ransomware infects an endpoint, the existing EDR platform detects malicious activity while Xshield isolates the affected device, preventing the spread to other systems. This containment strategy minimizes damage and reduces recovery time.

Lateral Movement Prevention: EDR platform identifies unauthorized credential use or network scans, and Xshield blocks communication between unauthorized devices, stopping attackers from pivoting across the network.

Zero Trust Network Traffic Control: The integration ensures that users and devices can only access authorized resources, reducing the attack surface and enforcing least-privilege policies.

Automated Incident Response: Security teams can automate containment actions based on EDR platform alerts, instantly restricting network access for compromised endpoints without manual intervention.

Benefits of the Integrated Solution

Enhanced Security Posture and Risk Reduction

The integration of already deployed endpoint protection with Xshield microsegmentation significantly strengthens an enterprise's cybersecurity. While EDR platform detects and prevents threats at the endpoint level, Xshield ensures containment by restricting lateral movement within the network. This layered defense reduces the likelihood of attackers escalating privileges or spreading malware across systems. If an endpoint is compromised, microsegmentation policies isolate it, preventing further damage. This proactive approach limits breach impact and enhances resilience against ransomware, insider threats, and other advanced attacks.

Simplicity and Speed of Implementation

One of the standout advantages of this combined solution is how quickly and easily it can be deployed. Because Xshield integrates directly with existing EDR platforms —leveraging the already-installed agent—there's no need to qualify additional software or undergo lengthy deployment cycles. Organizations can begin enforcing microsegmentation policies within minutes rather than weeks, dramatically shortening time-to-value. The setup is straightforward, requiring minimal configuration and no disruption to existing security tools or workflows. This streamlined integration accelerates enforcement, enhances visibility, and enables security teams to focus on policy design and threat response instead of tool management.

Cost Efficiency and ROI

By combining existing EDR capabilities with Xshield microsegmentation, organizations benefit from reduced security breaches, lower downtime, and simplified security operations. Preventing lateral movement significantly reduces the financial impact of cyber incidents, minimizing breach-related expenses.

Organizations deploying this integration also experience cost savings through optimized security infrastructure—ColorTokens leverages existing agents for enforcement, so that no additional software needs to be installed to begin gaining the benefits of microsegmentation. The integration also enhances operational efficiency, as security teams gain better visibility and control without increasing their workload.

Compliance and Regulatory Benefits

Organizations must meet stringent regulations like PCI-DSS, HIPAA, the EU's GDPR, DORA, and the UK's Cyber Essentials which demand strong data protection, access control, and monitoring. The combined power of EDR and Zero Trust microsegmentation supports compliance by securing endpoints and enforcing network segmentation. While microsegmentation isolates sensitive environments to reduce audit scope, EDR delivers real-time monitoring and detailed logs for audit readiness. Together, they simplify reporting and align with Zero Trust models increasingly endorsed by regulators.

Achieve Operational Resilience by Bringing Breach Readiness Instantly to Your Enterprise

The integration of EDR with microsegmentation delivers significant business and technical benefits by providing breach readiness, improving compliance, reducing costs, and enhancing operational resiliency. The ability to dynamically enforce network segmentation based on real-time endpoint intelligence makes this solution a strong fit for organizations adopting a Zero Trust security model. With minimal deployment complexity and high scalability, this integration offers a practical and effective way to strengthen enterprise security posture while simplifying security management.

Using Xshield and existing EDR platform together brings you an improved rapid breach readiness with quicker time-to-value, reduced ongoing maintenance, and improved security in a cost-effective way.

For more information on how you can add ColorTokens Xshield to your existing EDR implementation, contact our expert solution team at www.ColorTokens.com/contact-us

About ColorTokens:

ColorTokens is a leading provider of enterprise microsegmentation and breach containment solutions, dedicated to making organizations “breach ready.” By preventing the lateral spread of ransomware and advanced malware, ColorTokens protects complex network infrastructures through its innovative Xshield™ platform. The platform visualizes traffic between workloads, OT/IoT/IoMT devices, and users, enabling the enforcement of granular micro-perimeters, swift isolation of critical assets, and effective breach response. Xshield is recognized as a **Leader** in the Forrester Wave™: Microsegmentation Solutions (Q3 2024).