COLORTOKENS

EDR-INTEGRATED MICROSEGMENTATION

Build Cyber Resilience Swiftly & At Scale

Microsegmentation Powered by the EDR You Already Trust

Lateral movement is how attackers get to their end goal — whether that is ransomware installation, exfiltration of data, or operational disruption. Microsegmentation is one of the most powerful controls for stopping lateral movement, and ColorTokens leverages your existing EDR footprint to ease implementation and deploy it at scale.

NO NEW AGENTS
Leverage the EDR footprint you already have

90 DAYS TO 90% RISK REDUCTION
Measured by blast radius and attack surface

AI-POWERED POLICY CREATION
Create, test, and maintain policies based on MITRE ATT&CK™

1 Deploy Microsegmentation Without Operational Disruption

Microsegmentation projects often fail due to complexity, resource constraints (including training gaps), operational disruption, scalability challenges, and lack of visibility. These failures can result in increased risks, wasted resources, and operational disruption. ColorTokens has a proven implementation methodology that leverages testing using real-time traffic and simulation using the last 100 days of traffic data accessed from the EDR system.
With ColorTokens, microsegmentation initial deployment is reliable, safe, and fast. Further, due to our lean installation footprint that relies on standard operating system APIs, ongoing maintenance effort is minimized.

2 Leverage AI For Better Policy Creation Without Breaking Applications

Manual creation of policies is time consuming, prone to policy conflicts, and requires learning multiple security layers. ColorTokens' AI creates and maintains policies for applications and workloads based on the latest MITRE ATT&CK TTPs. With AI, policies can be created, extensively tested with historical data, and tested with real-time data prior to implementation. With ColorTokens, practitioners minimize the risk of breaking or disrupting applications while maximizing responsiveness to emerging threats.

3 Extend Your EDR System To Lateral Protections Including Ransomware

EDR systems collect rich telemetry in real-time. ColorTokens collects this telemetry seamlessly via the EDR's APIs. When a breach Indicator of Compromise is detected by the EDR, ColorTokens creates the appropriate policies automatically with AI. For ransomware, ColorTokens policies immediately isolate the infected device to halt lateral spread. The policies are then sent to the enforcement method in real time. As a result, the blast radius is minimized, and the ransomware spread is restricted. ColorTokens fully leverages the EDR system's real-time capabilities to limit exposures before they snowball.

4 Maintain Consistent Policy Enforcement Across Different Environments

Policies are typically created on a standalone basis in each environment, such as network controls, endpoint controls, and more. With ColorTokens, intelligent, AI-driven policies are created and enforced consistently via the enforcement method in place. As a result, policy enforcement is consistent across all environments.

5 Protect OT, IoT, and Legacy Systems

Many organizations struggle in environments such as OT, IoT, and legacy systems, each typically with their own UI and inconsistent methodologies. ColorTokens provides a single UI, thereby minimizing training needs.
Our AI prevents disruptions due to policy conflicts and delays due to manual policy reconciliation. As a result, the entire environment including IT receives fast, accurate, and consistent policies that work together to maximize security.

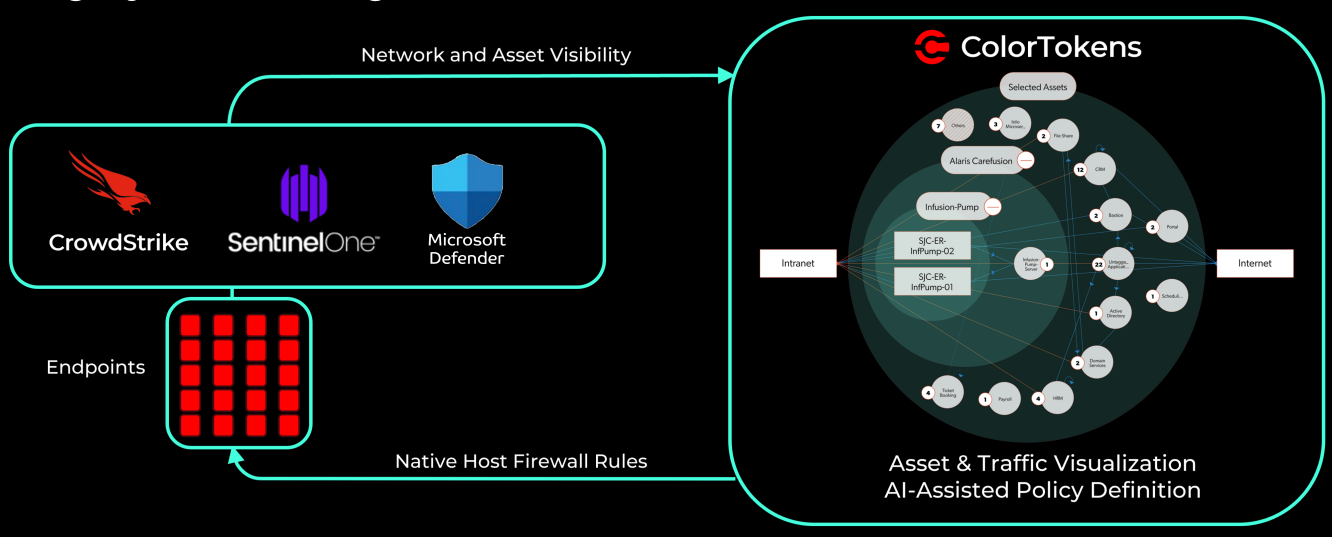
From Visibility to Enforcement in Days

IN MINUTES
Gain full asset & traffic visibility

IN HOURS
Segment your environment

IN DAYS
Enforce zero-trust policies

Leverage your Existing EDR for Real-Time Breach Containment



Learn more at
www.colortokens.com
Leverage your existing EDR. Stop lateral movement.
Reduce risk. Increase productivity.

LEARN MORE >

Visit our EDR-Intergrated Microsegmentation page