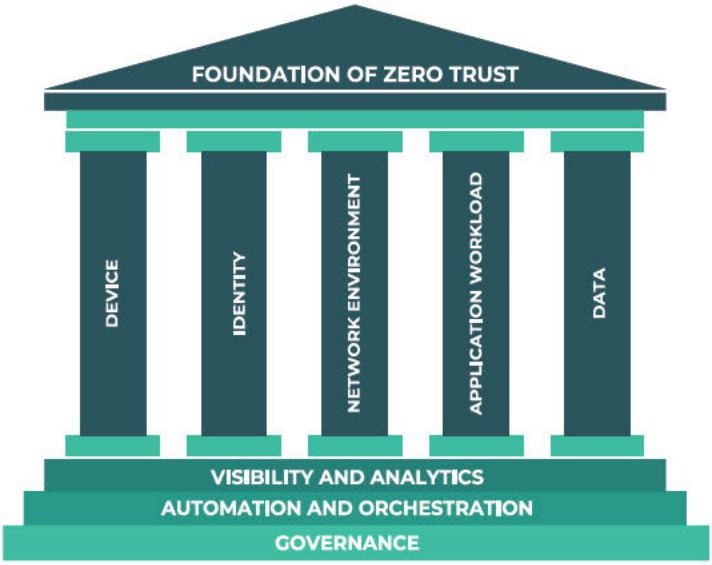
COLORTOKENS

SOLUTION BRIEF

Simplifying your journey to Zero-Trust Architecture

Why Zero Trust?

Traditional approaches to cyber security use a "perimeter defense" methodology, using firewalls and anti-virus signature detection to protect against attacks from the external internet. The problem with this approach is that the adversary only has to be lucky once; the defenders must be right every single time. In contrast, the Zero Trust security approach assumes the adversary is already inside your perimeter; internal users, programs and processes are not to be trusted by default



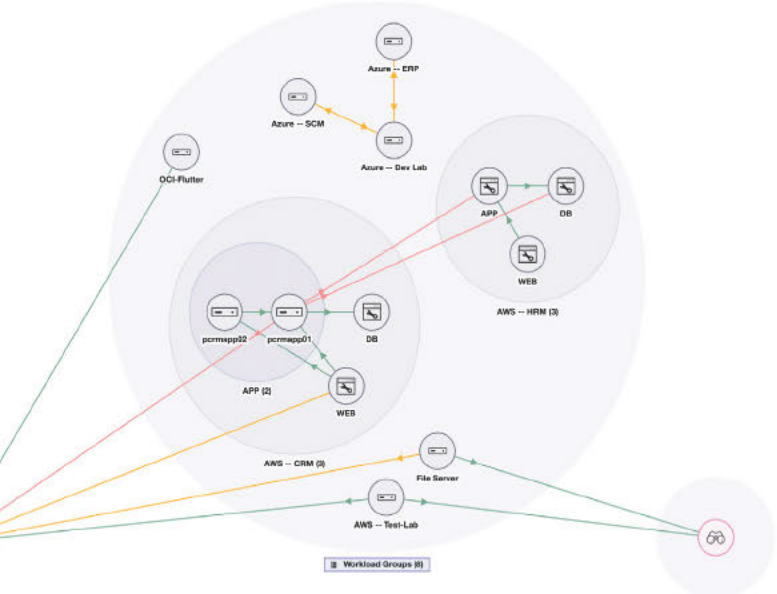
CISA Zero Trust Maturity Model

How do we get there?

Implementing Zero Trust architecture is a journey. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has defined the **Zero Trust Maturity Model** with five pillars supported by three foundational steps[1]. The ColorTokens platform is designed to help you move forward towards Zero Trust maturity in a way that is right for your organization, incrementally, **without disruption to your business processes.**

VISIBILITY AND ANALYTICS

Configuration Management Data Bases are often incomplete or inaccurate. To solve this, ColorTokens scans your environment to discover all your servers and devices, and automatically classifies and tags them based on network traffic. It lets you quickly discover, visualize, and model your assets, applications, and their interactions, for on-premise, containerized, and multi-cloud resources.



Automation and Orchestration

ColorTokens uses machine learning and heuristics automation to recommend the access policies which are defined by your business processes. Your team doesn't have to spend days or weeks trying to infer appropriate policies. In a very short time, you can begin blocking malicious lateral movement of data or programs by both external actors and insiders.

Governance

You can observe and analyze access policies with color-coded traffic lines. Progressive policy enforcement (observe/enforce modes) lets you implement access policy without disruption to your business—also known as "what-if" policy analysis. A unified user interface for managing both network device traffic policy and user access policy simplifies governance of your environment. Your workloads both in the cloud and on-premise can be governed to enforce software component integrity and security posture configuration.

*1 https://v/zero-trust-maturity-model

Device

ColorTokens gives you server/endpoint device **hardening** through whitelisting of applications and ***their child processes***. ColorTokens executes the Zero-Trust methodology by first observing the normal application usage in your business processes, and then only allowing those necessary processes to run. Therefore, it stops malicious processes and programs from running, by default, even if a novel malware has evaded the scanning of traditional anti-virus, EPP and EDR.

Identity

ColorTokens integrates with your existing LDAP/SAML Directory system and then goes beyond them to allow you to use the identity of your users **contextually**, for "enhanced identity governance", as described in the CISA maturity model. You can control users' access to applications and data depending on policy parameters beyond mere role. For example, you can have different access policies according to attributes such as the status of the device's OS updates, geo-location, subnet, and whether the user is logging on remotely.

Network Environment

ColorTokens automates the set-up and governance of **micro-segmentation** for your network environment. It lets you centrally control the configuration of the host-based firewall settings to define logical groups of applications, servers and users that are part of your normal business processes; other traffic is blocked by default. Micro-segmentation reduces the "attack surface"— the entry points into your environment — disrupts the propagation of malware or ransomware and blocks the lateral movement that often precedes the exfiltration of your data.

Application Workload

ColorTokens controls access to workloads in your on-premise network and cloud deployments based on the "least privilege needed to complete the task" tenant described in NIST SP 800-207. It also provides continuous monitoring through vulnerability and malware scanning of software components in your cloud application workloads, and deep scanning of your Operating System and cloud configuration. It does so without impacting your production system's performance, by scanning an image of your workloads.

Data

ColorTokens lets you control access to those assets that contain your "crown jewel" data, or High Value Assets (HVA) as described in the CISA maturity model. You can set rigorous access policies for your mission-critical files, applications, and servers, even in complex deployment environments. In addition, ColorTokens protects your data in-transit by leveraging AES GCM encryption.

Accelerate Time-to-Value through SaaS

Because it is delivered as Software-as-a-Service, the Colortokens platform eliminates the time and costs of capacity planning, hardware provisioning, installation, and configuration, as well as the on-going upgrades and maintenance effort needed by other solutions. Zero onboarding, zero maintenance..