



DEFENDING AGAINST ADVANCED ATTACKS WITH A ZERO TRUST ARCHITECTURE

WHITEPAPER

Overview


Enterprises across the globe have undergone a fundamental change in the way they conduct business and operate their networks. Corporate applications and data are no longer contained solely within the corporate network or on-site, instead distributed across various types of public and private networks including: on-premise, multi-cloud, hybrid-cloud, and through third-party SaaS applications. This has resulted in the blurring of the traditional corporate network perimeter and opened up a growing attack surface for internal networks.

The potential for financial damage as a result of internal breaches has only increased over the past year. Ill-prepared for the impact that digital transformation is having on their network security and risk posture, and alarmed by highly visible and damaging breaches such as the SolarWinds, Colonial Pipeline and Microsoft hack, CISOs, CIOs and C level executives are focused on incorporating Zero Trust into their network security architecture to reduce the attack surface and proactively defend against threats.

Challenge: Balancing Productivity and Security Risk


There are numerous security challenges for organizations as they digitize their business for enhanced productivity. From an IT security perspective, with the network perimeter blurred it is virtually impossible to get full visibility into the entire network traffic using traditional security tools. The traditional security model of using firewall perimeter-based security to protect user traffic at the data center edge has become outdated as most traffic is now east-west between servers, and invisible to firewalls. The lack of holistic visibility leaves organizations vulnerable to unknown threats and with greatly increased security risks. It is impossible for an organization to have a true understanding of their exposure to risk without a clear picture of the traffic and communication flows (north-south and east-west) between all users, devices and assets on their network. Obtaining continuous 360° visibility into their networks has become a key concern for organizations.

Another major IT challenge is the increase in a distributed workforce using a multitude of devices to access distributed applications, creating many more attack surfaces for bad actors to exploit. While “anywhere, anytime access” boosts worker productivity with more ready access to applications and location independent operation, the distributed nature of assets and users also significantly increases the inherent security risks. To defend against attacks, organizations must put defenses in place that assume nothing and no one is trusted, where each connection is verified regardless of whether they are inside or outside the network.



...the average time to identify (a data breach) was 207 days and the average time to contain was 73 days, for a combined 280 days. In 2019, the combined data breach lifecycle was 279 days.

IBM - Cost of a Data Breach Report 2020



47% of organizations report an increase in cyberattacks since the COVID-19 pandemic and related work from home started

ESG Master Survey¹

1. ESG Master Survey Results: Technology Impact of COVID-19: IT Decision Maker (ITDM), Report Published: May 28, 2020

Ransomware and other advanced attacks are causing greater damage than ever before and are happening at a higher frequency than in past years. Many of the successful breaches today are the result of lateral movement inside the network after a successful penetration of firewall defenses by hackers. Advanced persistent threats (APT) and ransomware often work their way through a network laterally, sometimes lying dormant for months, to reach high value assets. Traditional security tools are not well equipped to detect a bad actor who has gained access to the internal network, often leading to malware remaining undetected inside the network for long periods of time. The longer a threat remains undetected, the greater the costs to repair the potential damage and recover from the loss of crown jewels. Organizations must assume that it is relatively easy for bad actors to circumvent traditional firewall defenses and gain access to crown jewels inside the network.

Most security tools are siloed point products that address only a part of the problem. They create security gaps and obscure visibility into the network, often making the problem worse by creating unnecessary complexity. This has created a huge operational and security challenge for resource-strapped IT departments already dealing with a work-from-home reality and the growing need to support remote access and business continuity. Operations and security teams are searching for solutions to the same set of challenges. Adopting a Zero Trust approach to security is the only way to stop attacks such as ransomware in their tracks, and prevent future intrusions.



As of 2020, the average total cost of a data breach is \$3.86 million.

IBM - Cost of a Data Breach Report 2020



76% of organizations find that threat detection and response is more difficult today than it was two years ago.

ESG Master Survey²

2. ESG Master Survey Results: The Threat Detection and Response Landscape. Published: April 12, 2019

Expert Recommendations

Major organizations like the DoD (Department of Defense) and NIST (National Institute for Standards and Technology), and now the White House, along with prominent industry analysts such as Gartner, Forrester and IDC, agree that organizations must implement a proactive Zero Trust approach to security, based on a principle of “**Never Trust, Always Verify**,” to reduce their digital attack surface and prevent against attacks, while also reducing the impact of breaches.

NIST Zero Trust Framework

- All data sources and computing services are considered resources.
- All communication must be secured regardless of network location. Network location alone does not imply trust.
- Policy is the set of access rules based on attributes that an organization assigns to a subject, data asset, or application.
- Access to individual enterprise resources is granted on a per-session basis. Trust in the requester is evaluated before the access is granted. Access should also be granted with the least privileges needed to complete the task.
- Access to resources is determined by dynamic policy.

(Source: NIST SP 800-207, Section 2.1)

Gartner describes Zero Trust as “a paradigm where implicit trust is removed from all of our computing infrastructure. Implicit trust is replaced with explicitly calculated, real-time adaptive trust levels for just in time, just enough access to enterprise resources.”³

A Zero Trust principle is based on an identity-aware security model that allows verified users to access only those resources that they need to do their work, also known as least privilege access. This principle holds true for end users, third parties, contractors and other entities seeking access to corporate resources and crown jewels. Similarly, east-west communications between crown jewels and network assets are restricted to least privilege verified access, ensuring that secure zones exist to prevent lateral movement between assets.

A Zero Trust framework can reduce the attack surface and make digital networks more resilient to attacks, without disrupting digital transformation initiatives or negatively impacting user experience.

Converting a traditional flat network to a more segmented Zero Trust architecture significantly restricts east-west movement inside the network. This prevents lateral movement of malware and reduces the likelihood and severity of any breach, including persistent targeted attacks and ransomware.

Organizations looking to move to practical implementation should focus on two primary projects: user-to-application segmentation (ZTNA) and workload-to-workload segmentation (identity-based segmentation).

*Gartner*⁴

^{3,4}. Gartner Research Report “What are Practical Projects for Implementing Zero Trust?” by Analysts John Watts, Neil MacDonald. Published: March 17, 2021

A Practical Approach to Achieving Zero Trust

To build a successful Zero Trust implementation, organizations need an end to end, contextual, identity aware system that allows users to be identified across different systems as well as adaptive access controls to ensure access to secure resources is given to the proper users, before beginning their move to Zero Trust. Once the foundational identity and access control functionality is in place, organizations can focus on these projects, taking an incremental approach to achieving Zero Trust.

According to Gartner Inc.:

Most zero trust strategies start with networking-related initiatives due to the excessive implicit trust in traditional network security models.

Zero trust networking initiatives break into two areas:

1. Front-end network access focused on user-to-application segmentation (ZTNA)
2. Back-end network access focused on workload-to-workload segmentation (identity-based segmentation)


ZTNA reduces excessive implicit trust for access to resources, primarily from remote locations, by employees, contractors and other third parties. Start with a pilot of a ZTNA product. Plan rollouts to the organization by prioritizing contractor and third-party access. Then conduct a proof of concept (POC) to test applications with the ZTNA product, and use observation mode to learn patterns of access by user and role to build policies from there.

Identity-based segmentation reduces excessive implicit trust by allowing organizations to move individual workloads to a default deny model for communication, rather than an implicit allow model. Implement network segmentation to reduce excessive trust zones, starting with high level segmentation of campus and server networks. Like ZTNA, observation mode will be necessary to learn the patterns of communications by workloads and applications in order to build policies. Then, evaluate machine identity management techniques such as SPIFFE, OpenID Connect and SAML across workloads to support granular segmentation. When starting an identity-based strategy, start with a small collection of critical assets to build initial implementations and expand from there.

Security and risk management leaders should:

- *Develop a strategy to address heterogeneous workloads spanning on-premises, hybrid, virtual and container environments.*
- *Identify workloads that require segmentation using means other than agents, such as network-based or API-based orchestration.*⁵

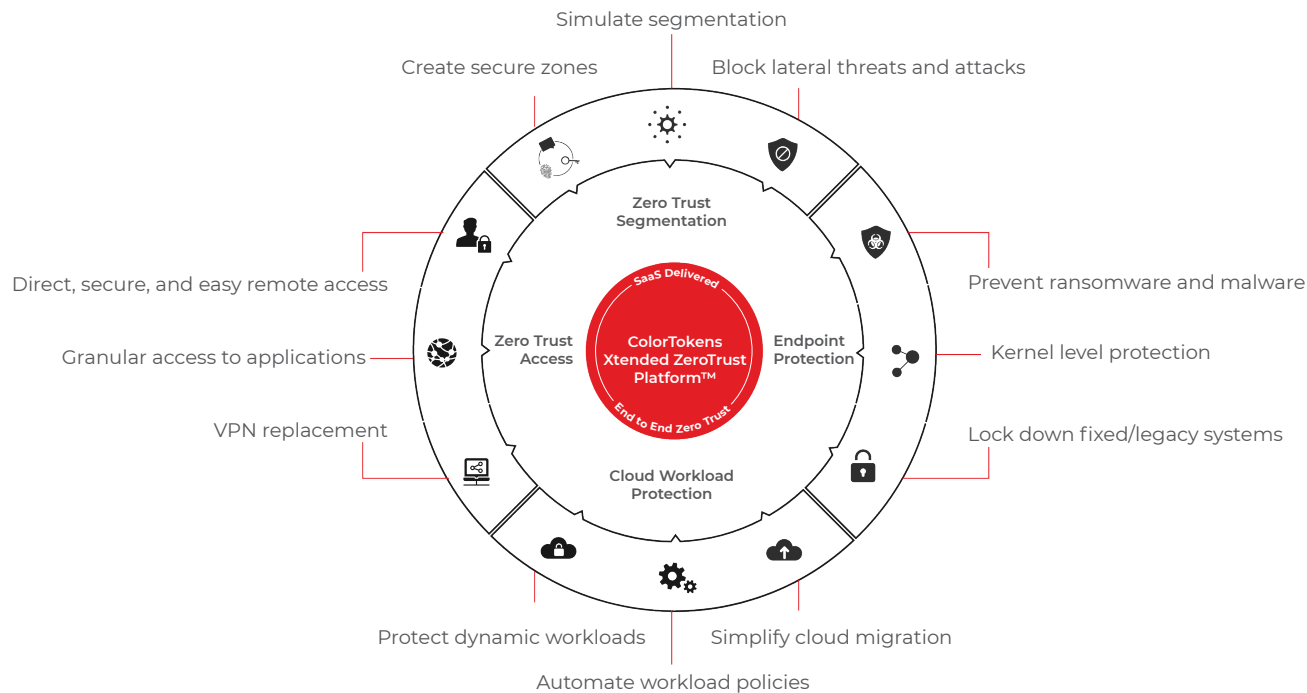
5. Gartner Research Report "What are Practical Projects for Implementing Zero Trust?" by Analysts John Watts, Neil MacDonald. Published: March 17, 2021



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 a secure perimeter as they can.

ColorTokens: A dynamic, intelligent platform for practical Zero Trust implementations

ColorTokens delivers a comprehensive, software-defined and cloud-delivered SaaS security platform, based on Zero Trust architecture, that protects users, devices, apps, and data across hybrid clouds and on-premises. ColorTokens Xtended Zero Trust™ Platform for cloud workload security and secure remote access consists of a suite of solutions designed from the ground up with Zero Trust as the foundation. ColorTokens' Platform addresses all pillars of Zero Trust out of the box.



ColorTokens Xtended Zero Trust™ Platform - End to End Zero Trust

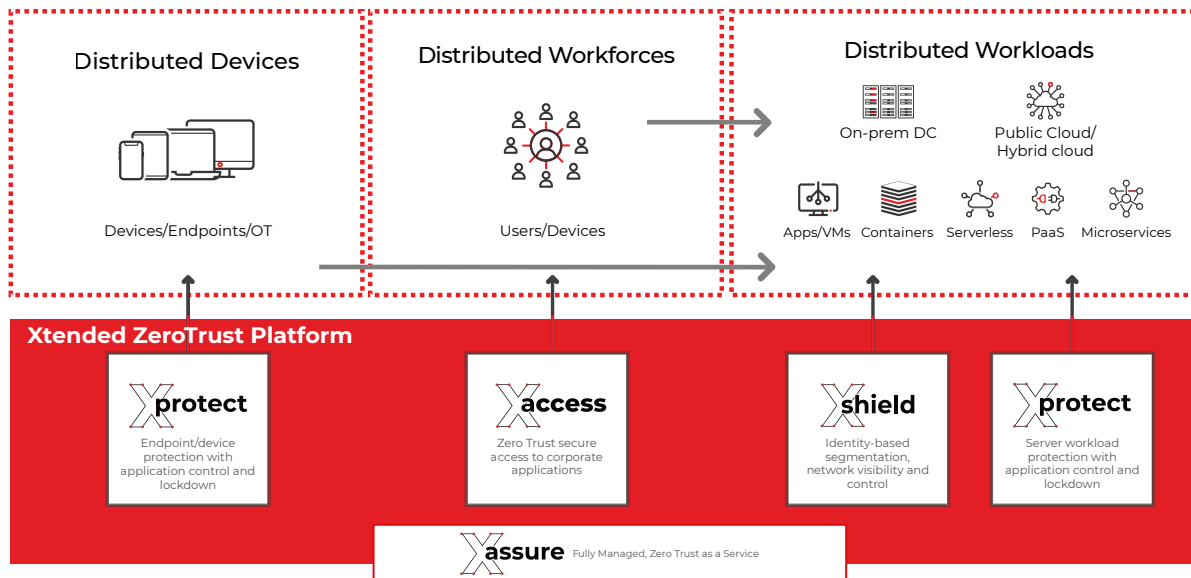
ColorTokens' platform consists of the following infrastructure agnostic and cloud delivered software components that operationalize the principles of Zero Trust in a common platform:

Xaccess is ColorTokens' ZTNA solution for remote user application-level access. Xaccess supports remote end-users as well as advanced functionality for IT administrators. Based on a SaaS model, Xaccess supports scalable access control regardless of resource and end-user location.

Xshield delivers workload-to-workload, identity-based segmentation (micro-segmentation), allowing least privilege access only to legitimate communication flows between workloads, based on user, device, and application context.

Xprotect provides lockdown and process control capability to enforce application and process whitelisting policies on servers and endpoint devices in the network. It contains threats to the first compromised device preventing outward movement and ensuring business continuity in the event of a breach.

Xassure delivers the platform components as a fully managed Zero Trust service, for organizations wanting 24x7 security services support for deploying and operationalizing Zero Trust in their network.



ColorTokens' Platform – A Contextual, Intelligent, Dynamic Security Control Platform for Hybrid Environments

Zero Trust Capability	Xtended Platform	Xaccess	Xprotect	Xshield
SaaS/Cloud delivered	✓	✓	✓	✓
Infrastructure agnostic	✓	✓	✓	✓
Single management console	✓	✓	✓	✓
Deep visibility into assets and communication flows	✓	✓	✓	✓
Least privilege access	✓	✓	✓	✓
User to application secure access (ZTNA)	✓	✓		
Workload-to-workload segmentation (identity-based segmentation)	✓			✓
User access to micro-segments	✓	✓		✓
Server lockdown/process control	✓		✓	
Whitelisting/allowlisting	✓		✓	
Endpoint protection	✓		✓	
Identity governance	✓			✓

ColorTokens' Platform – A Single Zero Trust Platform for Hybrid Environments

Conclusion

Digital transformation has become a strategic necessity forcing organizations to rethink their cybersecurity strategies. Zero Trust has emerged as a growing solution that eases this transformation. The challenge for enterprises comes in operationalizing Zero Trust, as it is a complex undertaking that requires a new way of thinking about cybersecurity. Zero Trust requires a platform solution supporting all of the basic tenets out-of-the-box, and compatible with existing hardware and systems. Traditional point products stitched together by modifying outdated architectures or by acquiring disparate point products from third party vendors can never be as secure as a platform purpose-built using Zero Trust as the basis for every design decision from day one. ColorTokens has built their Xtended Zero Trust™ Platform from the ground up to enable enterprises to protect their business with the latest Zero Trust technology, while leveraging current hardware and software investments for future-proofing.



About ColorTokens

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 Zero Trust™ 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.

© 2021 ColorTokens. All rights reserved. ColorTokens, ColorTokens logo and other trademarks and service marks are registered marks of ColorTokens and/or its affiliates in the U.S. and other countries.

Third-party trademarks mentioned are the property of their respective owners.



Winner in 4 categories of 2021 Global InfoSec Awards



Winner in 4 categories of 2021 GLOBEE Awards



Winner in 5 categories of 2020 Cyber Excellence Awards



Most Awarded at RSAC in 2019 in 6 Categories

Gartner

Market Guide for Cloud Workload Protection Platforms
April 2020

Third-party Microsegmentation Products
June 2019

Emerging Technologies and Trends Impact Radar - Security



Featured on the Solution Checklist for Transforming Zero Trust Principles to Reliable Practices

FORRESTER

Zero Trust Solution Providers
Q2, 2020