COLORTOKENS

Zero Trust Through a Business Lens

Let's face it: The cybersecurity industry hasn't always served its customers well. Despite spending millions on security solutions, organizations worldwide are still left with enormous gaps: in protection against breaches, but also in their understanding of risk. As a result, they're vulnerable to internal as well as external cyberthreats.

Traditional security solutions have only one purpose: to keep attackers out. This approach assumes that threats come from outside the network, and that every user and device insider the perimeter can be trusted.

But today's threat landscape, not to mention today's business requirements around remote work, cloud workloads, and third-party applications, demands a new approach to cybersecurity. Faced with persistent, sophisticated attackers, organizations need to ensure business continuity and maintain data integrity.

> It's time for a change.

Zero Trust: The way forward

In cybersecurity, you don't get results simply from throwing money at a problem. You achieve results when you combine your security investment with a strategy congruent with these modern business needs.

> Zero Trust is that strategy.

Built on the principle of "Never trust, always verify," a Zero Trust security approach seals the gaps in your security infrastructure and empowers you to prevent and neutralize threats faster and more effectively than before.

With a conventional, perimeter-based security architecture, the primary goal is to protect the network location. In a Zero Trust architecture (ZTA), the focus is on securing resources like applications, workflows, and accounts. Authentication and authorization of both subject and device are separate functions performed before each session.

By putting Zero Trust principles into practice, organizations can maintain a strong, resilient security posture that limits both an attacker's ability to penetrate the network and their potential to wreak havoc once inside.

Business advantages of implementing Zero Trust

Implementing Zero Trust security makes you more secure, reduces costs, and improves business agility. With Zero Trust, organizations can:

Protect your data and your customers': Zero Trust architecture ensures least-privilege access (meaning users or systems have only the access they need, and no more) to protect against unintentional exposure or malicious attacks both inside and outside your organization.

Reduce compliance costs: Zero Trust-based infrastructure is inherently segmented, which reduces the scope of regulations and compliance audits.

Empower security teams to do more: Adopting a Zero Trust model improves your security posture, drastically reduces false alerts, and delivers a better experience for your users. Instead of spending their time on maintenance and urgent fixes, security teams can focus on business enablement.

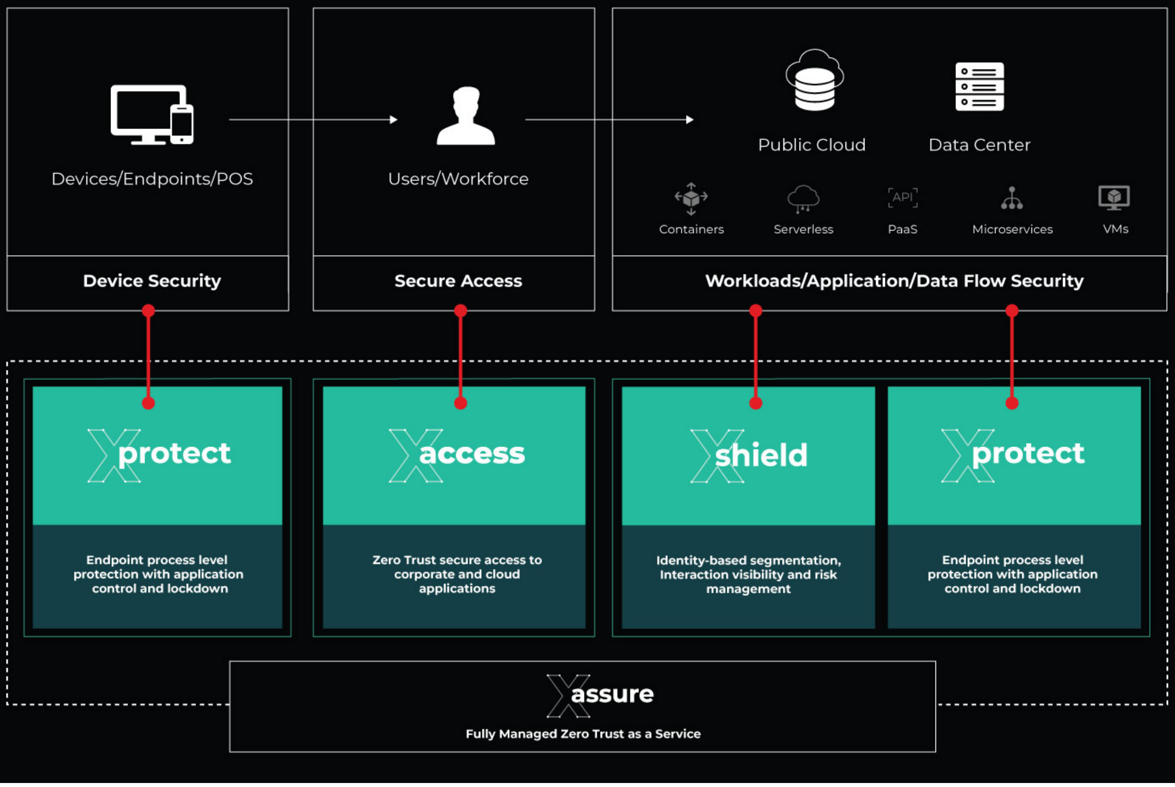
Enable digital transformation: Segmented Zero Trust networks empower security teams to support new services without hindering existing business operations.

It comes as no surprise that in 2020, 60% of organizations globally reported that they were accelerating Zero Trust implementation.

The ColorTokens’ Difference

ColorTokens Xtended ZeroTrust^{TM} Platform delivers unparalleled protection to enterprises from sophisticated attacks such as ransomware, unauthorized lateral movement, and zero-day attacks. The unified platform is a cloud-delivered, software-defined solution that secures critical assets, including applications, endpoints, workloads, and user access. The platform both simplifies and accelerates the enterprise journey to hybrid environments and full cloud adoption.

ColorTokens Xtended ZeroTrust™ Platform



Devices/Endpoints/POS
Users/Workforce
Public Cloud
Data Center
Containers
Serverless
API
PaaS
Microservices
VMs
Device Security
Secure Access
Workloads/Application/Data Flow Security
Xprotect
Endpoint process level protection with application control and lockdown
Xaccess
Zero Trust secure access to corporate and cloud applications
Xshield
Identity-based segmentation, Interaction visibility and risk management
Xprotect
Endpoint process level protection with application control and lockdown
Xassure
Fully Managed Zero Trust as a Service

Platform modules

Xshield delivers workload protection through granular visibility and software-defined micro-segmentation.

Xaccess enables organizations to offer secure remote access to employees, partners, and third parties.

Xprotect locks down endpoints to prevent breaches, malware, ransomware, and zero-day attacks.

Xassure provides breach prevention, detection, response, and containment services using advanced XDR and AI/ML capabilities.

Add-on Services

Xquantify takes the guesswork out of cyber investment and helps organizations develop and implement a risk-based cybersecurity framework.

Schedule a demo or visit our website to know more.

About ColorTokens
ColorTokens Inc., a leader in proactive security, provides a modern and new generation of security that empowers global enterprises to singlehandedly secure cloud workloads, dynamic applications, endpoints, and users. Through its award-winning cloud-delivered solution, ColorTokens enables security and compliance professionals to leverage real-time visibility, workload protection, endpoint protection, application security, and Zero Trust network access—all while seamlessly integrating with existing security tools. For more information, please visit **www.colortokens.com.**