SOLUTION BRIEF

COLORTOKENS

Tackling Cybersecurity Challenges of Mergers & Acquisitions

M&A allows organizations the opportunity to rapidly change or transform their business with new technology or quickly gain access to larger market segments. With the increase in M&A transactions, especially over the last few years, cybersecurity breaches have also increased.

These breaches stem from security gaps resulting from integrating two different networks, applications, and data. Some breaches are identified shortly after the integration, while others are not identified until years later. In either case, the liability and the economic consequences usually fall on the go-forward company.

Following an M&A transaction, organizations can reduce their cybersecurity exposures during IT integration by following due diligence processes developed by Gartner Research, for example. These industry analysts capture all the necessary details of the network and applications while also outlining all the security measures and tools available.

In 2022, Gartner estimates that 60% of organizations engaging in M&A will consider cybersecurity posture a critical factor in their due diligence process.

Despite these efforts, companies continue to experience increased breaches following M&A transactions, and they need additional tools and services to reduce their exposure.

Organizations cannot tackle the M&A cybersecurity challenges using point products due to the sheer scale and complexity of the challenge. Instead, they need to adopt a new strategy that includes a Zero Trust approach. The Zero Trust model assumes that attackers might already be present in the network requiring continuous authentication and authorization – an environment similar to M&A.

ColorTokens Xtended ZeroTrust™ Platform simplified, accelerates, and automates Zero Trust implementation for security teams and is ideally suited to tackle the complexity of M&A cybersecurity challenges.

> “
>
> Global mergers and acquisitions activity hit an all-time high in the first six months of 2021, with deals worth more than US$2.6t
>
> *Source: Ernst & Young*

M&A Specific Challenges

- Disparate IT infrastructure
- Inventory of assets
- Different technologies
- Integration of firewall rules
- Digital transactions
- Unknown user access
- Untrusted endpoints

M&A Specific Requirements

- Discover and map all systems
- Identify unauthorized users and applications
- Segment networks, services, and applications
- Create Zero Trust zones to ensure secure integration
- Identify vulnerable systems
- Harmonize security policies
- Lockdown endpoints

How ColorTokens Enables the M&A Cybersecurity Process

ColorTokens simplifies, accelerates, and automates Zero Trust Security for all enterprises, including data centers, multi-cloud, and hybrid environments.

Our SaaS-based, cloud-delivered approach ensures fast and easy visibility, segmentation, and lockdown of operating environments, effectively blocking the spread of ransomware and malware inside your on-prem networks and clouds.

ColorTokens Xtended™ Zero Trust Platform Secures at Every Deal Stage

The ColorTokens Xtended ZeroTrust™ Platform reduces operational costs by supplying required data to audit systems. It also generates reports and network maps showing how the organizations allow access to users – ending the need to compile and document thousands of access rules. **The platform provides an easy and fast way to segment various resources** while integrated into the overall go-forward IT environment. The platform can completely lockdown endpoints as desired, allowing access only to approved applications.

At ColorTokens, we understand that one-size-fits-all is no longer an effective cybersecurity solution. Each company is at a different stage of cybersecurity maturity based on its requirements. Enterprises need expert assessment, evaluation, and the right

Zero Trust security prescription to protect their environments effectively, now and especially in the future. From the start, ColorTokens works closely with your security teams to design the right solution, solve your security pain points and provide you with ongoing support throughout your Zero Trust journey.

Xtended ZeroTrust™ Platform
offers the combination of our multiple cybersecurity products to maximize enterprise protection. The ColorTokens platform is the industry's first unified solution for Zero Trust security in hybrid environments - across data centers, cloud, application workloads, users, and devices. With ColorTokens, enterprises can rapidly, affordably, and efficiently accelerate their Zero Trust journey, regardless of their current security posture.

ColorTokens Xshield - Zero Trust Micro-segmentation
Xshield deploys and delivers deep visibility into network assets, communication flows, and segments and protects assets with granular policies that progress from simple enforcement to complete Zero Trust.

ColorTokens Xprotect - Process Level Control and Enforcement
Xprotect locks down endpoints and servers with process control enforcement and quarantines suspected devices until remediation.

ColorTokens Xcloud - Comprehensive Cloud Security in a Single Platform
Instantly prioritize your risks and protect your cloud with just one platform. Xcloud delivers comprehensive cloud security for multi-cloud, including CSPM, vulnerability management, malware detection, and compliance.

ColorTokens Xassure - 24/7 Managed Zero Trust Service
The Xassure team of cybersecurity SOC experts accelerates customer adoption of micro-segmentation with Zero Trust services tailored to customer needs, from active breach containment to micro-segmentation and extending protection to users and devices.

Benefits for M&A Customers

- Discover systems in the entirety of the legacy on-premises and on cloud platforms
- Eliminate unnecessary network firewall segments and VLANs
- Achieve consistent security policies between both companies
- Reduce risks by identifying exposed workloads, misconfigured ports, and unauthorized connections
- Implement micro-segments consistent with the go-forward IT strategy
- Assign access policies that follow the workloads and users across both companies
- Enforce company policy to lockdown endpoints if they are unpatched
- Reduce the burden of compliance by narrowing the scope of audits

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 ZeroTrust™ 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 San Jose, California; New York; London; Copenhagen, Denmark; and Bengaluru, India. For more information, please visit www.colortokens.com.