IDC ANALYZE THE FUTURE

IDC VENDOR SPOTLIGHT

Sponsored by: ColorTokens

Organizations must have a plan to tame the challenges of zero trust. Granular visibility of assets and communication flows powered by AI/ML automation in an extensible, cloud-based platform brings zero trust into focus.

Accelerating Zero Trust Through Policy and Workflow Automation

May 2021

Written by: Michael Suby, Research Vice President, Security and Trust

Introduction

Cloud services and remote working have redefined the IT environment. Sensitive data and business applications are no longer solely hosted within a private datacenter, and end users are just as likely to access these resources remotely as they do locally. Moreover, with modular and open designs, applications are changing at an accelerating pace. Use of cloud services continues to multiply, further adding to the environmental change.

What follow are communication and application flows that are more diverse and dynamic than ever before. For CISOs and their teams, establishing and enforcing security policies for resource segmentation and access permissions are increasingly complex responsibilities. While they want to embrace a zero trust architecture built on identity-based segmentation and least privilege, operationalizing may seem beyond their technical reach, budget, and timeline.

If organizations don't make progress in implementing zero trust, then threat actors gain ground. Lacking clear and narrow definitions of legitimate communication and application flows, threat actors conduct their clandestine operations under the covers of a broad range of permissible flows. Triggering alerts provides a ray of hope that the trail left by threat actors will be uncovered. Yet, there are no guarantees that detection will occur or occur soon enough to contain the threat before organizations suffer tangible damage (e.g., data exfiltration, disrupted operations, and regulatory violations).

Fortunately, there is a path forward. IDC contends that a centralized platform approach that embodies the attributes of deep visibility into assets and traffic flows (north-south and east-west), policy automation, low impact on protected resources, and use case extensibility can operationalize a zero trust architecture rapidly, affordably, and efficiently. That platform approach is described in this paper.

AT A GLANCE

WHAT'S IMPORTANT

Organizations' digital footprints are evolving rapidly, in part accelerated by the pandemic but foundationally by digital transformation. How organizations secure their assets and limit cyberexposure is an ongoing challenge, and implementing zero trust is a leading solution candidate.

KEY TAKEAWAYS

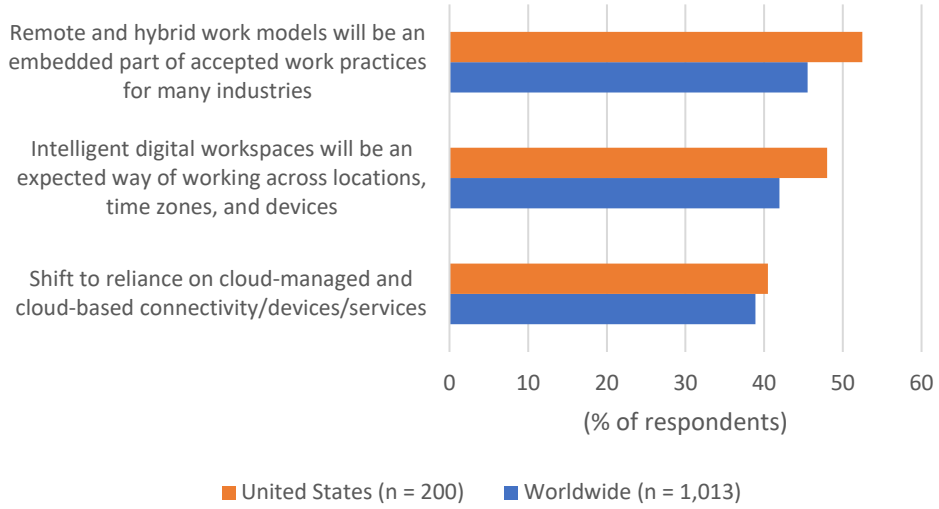
Operationalizing zero trust approaches will take center stage as organizations move from concept to implementation. Of prime consideration will be solutions that have a light touch, supplement rather than compete with business objectives, and are infrastructure agnostic.

Security Challenges

Security challenges continue to mount. Foremost is the diversification of the IT footprint and, as a consequence, a broadening attack surface. Case in point: The pandemic forced IT organizations to rapidly react to a sudden burst in full-time remote work arrangements. In addition, IT organizations have been saddled with an IT infrastructure designed for a mostly onsite workforce, which accelerated the shift from on-premises applications to cloud services. As Figure 1 shows, these pandemic reactions will endure post-pandemic.

FIGURE 1: ***Remote and Hybrid Work Models and Cloud Services Will Endure Post-Pandemic***

Q In your opinion, which work practices and technology advances emerging from the pandemic are most likely to endure?



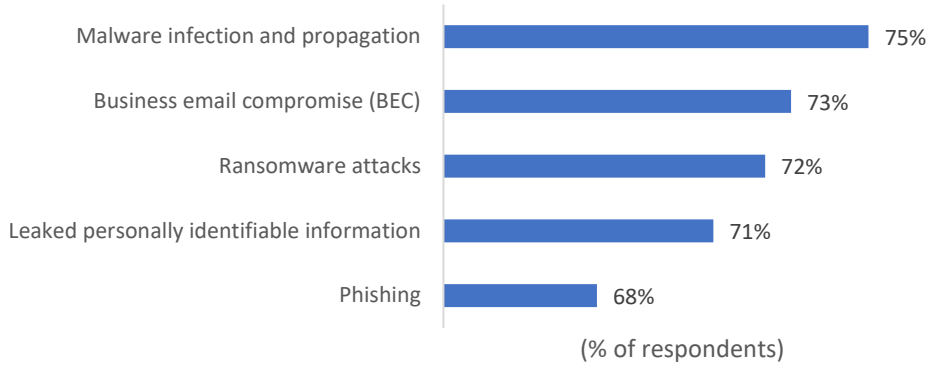
Source: IDC's Future Enterprise Resiliency and Spending Survey, February 2021

The broadening of the attack surface is measured not only by where end users are located and applications are hosted but also by the application source, which is diversifying. According to IDC's *Future Enterprise Resiliency and Spending Survey,* CIOs and line-of-business (LOB) leaders expect half of their new applications in 2021 will be developed by or purchased from a third party. As the recent SolarWinds hack illustrated, third-party applications can be a highly effective attack vector into victims' IT environments.

Organizations have many options to mitigate their widening exposure to cyber-risk. Endpoint security is a prominent option. As Figure 2 illustrates, organizations indicated that endpoint security has a high level of relevance in mitigating numerous forms of cyber-risks.

FIGURE 2: ***Malware Infection and Propagation Tops the List of Cyber-Risks***

Q ***Rate the relevance of endpoint security products in mitigating the following risks, (where 1 is "not relevant" and 5 is "very relevant").***



n = 308

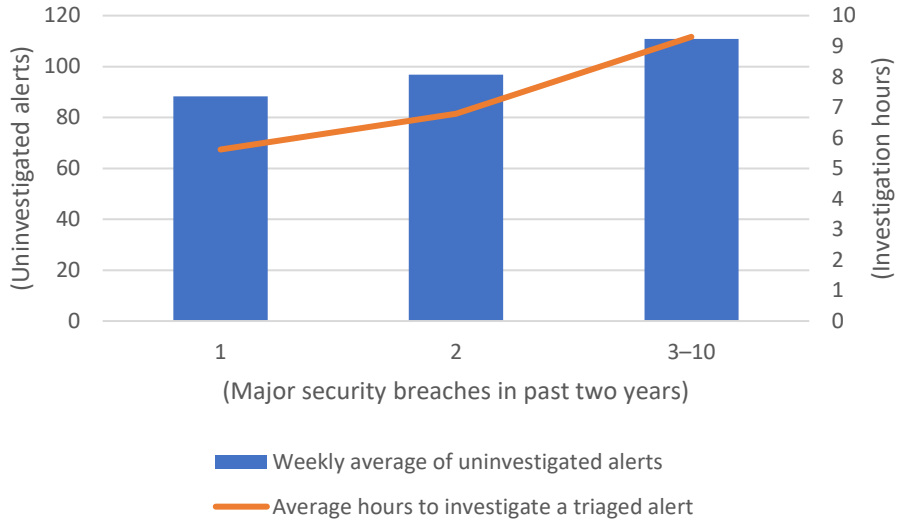
Note: The data is from survey respondents choosing 4 or 5.

Source: IDC's North America SMB Security Survey, April 2020

But security technology is not enough and can even be counterproductive when a complex and growing stack of security products from multiple vendors force security personnel to spend precious time working across products rather than the products working together. This inefficiency is reflected in the correlation between the number of security breaches with uninvestigated security alerts and the elapsed time to investigate a triaged alert (see Figure 3).

FIGURE 3: ***Number of Security Breaches Is Positively Correlated with Number of Uninvestigated Alerts and Investigation Time***

- Q ***Approximately how many major security breaches has your organization had in the past two years that involved spending significantly extra resources to rectify?***
- Q ***On average, how many suspicious alerts are uninvestigated, regardless of severity, each week?***
- Q ***After an alert has been triaged and deemed worthy of investigation, how quickly, on average, can your organization investigate suspicious threat activity?***



n = 342

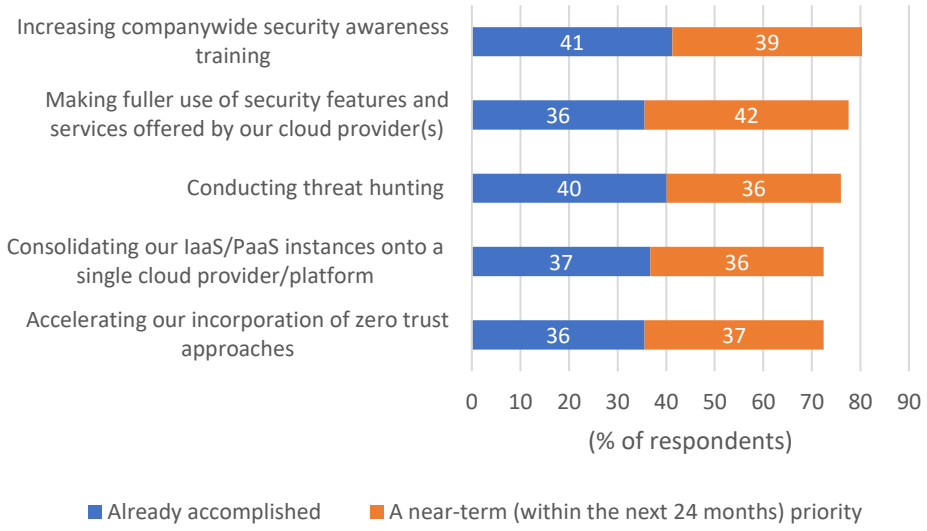
Source: IDC's EDR and XDR 2020 Survey, December 2020

Security leaders are acutely aware of the heightened cyber-risks they must address. While many potential remedies exist, organizations are constrained by budget, resources, and complexity, so prioritization is essential. To gain perspective on priorities, IDC presented security leaders with 12 actions to strengthen their organizations' IT and security resiliency and asked them to rate each based on status: already underway, near- or long-term planned initiatives, or no plans.

Figure 4 lists the top 5 actions that either are already underway or are near-term priorities. Two of the five actions relate to cloud strategies, which is consistent with the accelerating shift to cloud services. Threat hunting reflects the realistic and prevailing point of view that hackers will evade even the best cyberdefenses and bore into the organization's IT environment. Incorporating zero trust approaches adds a preemptive dimension to strengthening IT and security resiliency. Rather than identify and circumvent a continuously evolving and deepening pool of malicious activities, zero trust defines and enforces policies that only permit activities that have been defined as allowable.

FIGURE 4: ***Threat Hunting and Implementing Zero Trust Approaches Among Top 5 Actions to Strengthen IT and Security Resiliency***

Q Which of the following actions has your organization taken or will your organization take to strengthen IT and security resiliency?



n = 504

Source: IDC's EDR and XDR Survey, December 2020

While the concept of zero trust is intuitive, operationalizing zero trust across an IT environment that spans public cloud workloads, containers, and microservices; SaaS applications; dedicated servers; internally and third-party-developed applications; and remote and hybrid workforces is a daunting endeavor. The next section discusses a centralized platform approach that provides a path forward to operationalizing zero trust.

Attributes of Zero Trust Solutions

As workforces, workloads, and data became increasingly dispersed and dynamic, organizations soon discovered that security policy management tied to the location of IT assets is no longer optimal. For example, synchronizing a policy management system for on-premises workloads with a policy management system for cloud workloads is inherently challenging when applications are intertwined across workload locations. Similarly, security policy management for end-user devices that rely on devices being onsite is no longer viable for end-user devices that are seldom onsite. A more viable approach is a centralized security policy management platform that operates across IT assets and locations. This is the rationale for a centralized platform for zero trust.

A centralized platform is only one of many important attributes of zero trust solutions. IDC recommends that organizations consider the following solution attributes as they evaluate prospective vendors and their zero trust solutions:

- **Deep visibility into assets and communication flows (north-south and east-west).** Defining "allow only and deny all else" policies (the foundation of micro-segmentation) requires a current, comprehensive, and accurate inventory of connected assets, including knowing the business value or sensitivity of each asset. It also requires granular visibility into past and current communication flows (network, application, user, process) among users and assets and among assets. In addition, organizations should consider not only what communication is visible but also the intuitiveness with which this information is organized and presented.
- **Policy and workflow automation.** Security personnel are burdened with too many menial tasks and crushed by an excessive volume of decision points. Automation is an unburdening attribute. Collectively based on visibility (assets and flows), threat intelligence, and artificial intelligence (AI)/machine learning (ML) modeling built into the platform, priority-tiered zero trust policy recommendations are presented for review, customization, monitoring, and enforcement (i.e., set to block). Security personnel concentrate more on deciding among policy options than the nuts and bolts of designing policy options. In addition, the workflow steps to implement policy are condensed and automated, which relieves security staff from manual input and assists in ensuring policies are implemented confidently, comprehensively, and rapidly.
- **Low impact on protected resources.** Although visibility is critical, gaining visibility should not come at the expense of costly overhead and high-touch installations. Instead, agents installed on IT assets should be lightweight in resource consumption and easy to deploy, configure, and update. End-user transparency is important.
- **Cloud-based management.** Because the platform is cloud based, there is no infrastructure to acquire, deploy, and maintain. Management operates out of band, avoiding interference with critical business operations, and comprehensively across all zero trust policy implementations (e.g., end-user devices, cloud workloads, remote access).
- **Use case and IT environment extensibility.** With an objective of operationalizing zero trust broadly, the solution needs to be extensible across a range of security use cases (e.g., reduce incidents of lateral movement and privilege escalation, protect sensitive data, strengthen ability to thwart ransomware attacks and malware propagation, contain malicious insiders, and narrow end-user remote access permissions) and environments (e.g., end-user personal computing devices and application and database environments: physical servers, virtual servers, workloads, containers, and serverless functions in private datacenters and private and public clouds). In practice, policies are automatically rendered into the language that is pertinent for each native traffic flow control point (e.g., host firewalls, APIs). Because of policy automation, security personnel can concentrate on policy objective rather than mechanics.

Benefits

The benefits of a centralized and comprehensive approach to a zero trust policy management platform can be summarized in the following categories. Naturally, the degree of the following benefits depends on the organization's current circumstances and the extent to which the organization implements zero trust:

- **Risk reduction.** Enforced zero trust policies narrow the range of motion for both internal users and threat actors who have established a foothold in the IT environment (e.g., an end-user device). The risk of internal users and systems intentionally or unintentionally executing a program, conducting an operation, or accessing resources inconsistent with their defined roles, responsibilities, or purpose is prevented. Similarly, threat actors are equally restrained. Their movements are confined to what allow-list policies permit. In turn, this restriction also alters the economics (increases the cost) for threat actors as higher levels of skills are required to overcome these restrictions. In addition, the more precise allow-list policies become, the greater the risk of detection for threat actors as their attempted actions blocked by allow-list policies are also identified and flagged as high-confidence alerts.
- **Strengthened compliance assurance.** Compliance assurance is bolstered as zero trust policies can be defined based on what regulations allow and only what regulations allow. Zero trust policies can become the ultimate in proving restricted access to sensitive data. For example, rather than validating that each access instance to sensitive data is compliant, a zero trust approach guides organizations to a state of "compliant by design."
- **Improved staff optimization.** A centralized zero trust policy management solution that meets the attributes defined previously presents many avenues for improving staff optimization. Those avenues include the following:
  - **Singularity.** Security teams will need to engage in fewer time-robbing, inefficient practices because they are using a single viewing portal for all IT assets and all communication flows and a single interface to define, monitor, and apply zero trust policies. Those practices include but are not limited to oscillating between multiple administrative interfaces; spending extra time to become proficient in each interface; and building compensating, cross-platform workflows that eventually become obsolete as each platform is on its own unique update cycle. Moreover, the accumulated complexity of multiple interfaces and platforms increases the risk of error and oversight.
  - **Policy confidence.** A reservation frequently associated with allow-only policies is the risk that these policies will break or interfere with legitimate business operations. As a result, security teams hesitate to enact more granular and restrictive policies. Thus, there is greater reliance on other compensating security controls, which also need to be managed by policy. Policy management coordination efforts increase and so too does the potential for conflicting policies and errors. The unified and comprehensive visibility of a centralized zero trust management platform that is also automatically updated for changes in assets and communication flows helps offset breakage concerns, elevates policy confidence, and accelerates implementation of zero trust principles that are adaptable to changing conditions.

- **Alert reduction.** What does not happen does not create an alert. Allow-only policies prevent the creation of alerts that need to be triaged, investigated, and resolved. All of this takes staff time and, as illustrated in Figure 3, is positively correlated with security breaches. Instead, alerts emanating from zero trust policies are affirmations of prevention. Equally important, these alerts are quite likely smaller in number and less urgent to address because the threat actor is corralled within the compromised IT asset.
- **Focus on broad policy rather than policy mechanics.** Built-in policy translation relieves security teams from spending time learning and applying rules to all policy control points where zero trust policies are enforced.

» **Favorable economics.** Because the platform is cloud based, there is no additional IT infrastructure to procure, deploy, and manage, and scalability is an inherent feature. In addition, use case extensibility presents potential opportunities to avoid expenditures on other security technologies and retire pre–zero trust technologies.

Considering ColorTokens

When ColorTokens launched in 2015, the company had a mission of enabling enterprise digital transformation with an extensible zero trust security platform. That mission is bearing fruit. An expanding customer base is demonstrating that ColorTokens has designed its platform to solve customers' correlated cybersecurity and business challenges rapidly, confidently, and continuously and with a light touch that is the company's true differentiator.

Design tenets to the ColorTokens Xtended Zero Trust platform include the following:

» **Granular and dynamic visibility.** In zero trust, the foundational ingredient is understanding IT assets and communication flows. ColorTokens gains this visibility through its lightweight agents. From telemetry streamed from these agents and combined with vulnerability and threat intelligence and powered by AI/ML, zero trust policies unique to each customer are formulated. Continuously adapting policy recommendations are updated as new telemetry is digested.

» **Single-click policy deployment.** From the same administrative dashboard, zero trust policies are deployed on protected assets. With policies translated into rules enforced through native controls on protected resources, the time from policy decision to enforcement across all protected resources is trimmed to minutes.

» **Cloud delivered.** Because the platform is designed as a cloud service, customers can avoid infrastructure investments and gain scalability and autonomy from their protected resources (i.e., operates across the infrastructure containing the protected resources).

» **Cloud and hybrid workloads.** Cloud-native workloads (virtual machine or PaaS or containers or serverless or microservices APIs) are protected across multiple cloud platforms, as are hybrid (private cloud datacenter) workloads.

» **Easy implementation and extensibility.** ColorTokens, in its short existence, has brought to market three products that operationalize the principles of zero trust in a common Zero Trust Platform:

- Xshield delivers infrastructure and cloud-agnostic security as well as identity-based segmentation of business traffic so that only legitimate and allowable communication flows are permitted based on user, device, and application context.

- Xprotect enforces policies on servers and endpoint devices using lockdown capability to prevent lateral moment; that is, it contains the threat to the first compromised device, preventing outward movement and allowing resilience and business continuity in the event of a breach.
- Xaccess is ColorTokens' solution for remote user application-level access control, including users with advanced requirements such as remote IT administrators. Like Xshield and Xprotect, Xaccess is infrastructure agnostic and cloud delivered to support unlimited and scalable access control regardless of resource and end-user location.

Challenges

Gaining market attention is the principal challenge for ColorTokens. Implementing zero trust approaches is top of mind among CIOs, CISOs, and business leaders. This interest is driving development and marketing spending by a wide assortment of solution providers, including incumbent IT, networking, and security vendors. ColorTokens, as any new market entrant, will be battling for attention and the opportunity to participate in proofs of concept (POCs) within a crowded field. One factor that favors ColorTokens is that its platform design and product delivery greatly minimize the time and effort that organizations need to dedicate to conducting POCs.

Deep visibility and policy and workflow automation powered by AI/ML modeling in a cloud platform ease the practical burdens of implementing zero trust.

Conclusion

The strategic necessity of digital transformation is forcing organizations to reevaluate their cybersecurity strategies. As they do, the appeal of zero trust has grown. At the same time, the practical considerations and challenges of operationalizing zero trust will become increasingly apparent. IDC believes the cloud-delivered, infrastructure-agnostic platform design followed by ColorTokens provides a worthy blueprint for organizations to marry their digital transformation journeys with zero trust.

About the Analyst

Michael Suby, *Research Vice President, Security and Trust*

Michael Suby is a Research Vice President in IDC's Security and Trust research discipline. In this role, Mr. Suby concentrates on endpoint security and, in collaboration with IDC team members, engages in research spanning a wide and evolving spectrum of security and trust topics. In the broad endpoint security landscape, Mr. Suby's focuses on impactful developments in solutions, markets, cyberthreats, and end-user requirements in the following endpoint security categories: modern endpoint security, server security, and consumer digital life protection.

MESSAGE FROM THE SPONSOR

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 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.

For more information, please visit www.colortokens.com.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com