IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: ColorTokens

Digital transformation (DX) is creating a highly fragmented, expanding, and dynamic footprint of applications, data, devices, end users, and networks. Implicit trust, unfortunately, is a casualty. Micro-segmentation can operationalize the principles of zero trust and least privilege in balancing risk and business activity.

Micro-Segmentation Transforms Zero Trust and Least Privilege Principles to Reliable Practices

January 2021

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

Introduction

Digital transformation (DX), the act of transforming an organization into one that can scale all or part of its business and innovate at a pace that is an order of magnitude greater than that of traditional businesses, has been spurred by COVID-19 and is progressing rapidly. However, organizations are not progressing similarly. Some organizations undertake DX initiatives for near-term, tactical intent. Other, more DX-progressive organizations have a longer-term horizon, pursue DX enterprisewide, and have alignment between their DX initiatives and enterprise strategies.

Although differing in DX intent, organizations share common traits. For example, their attack surfaces are expanding as cloud adoption and work conducted from home and in the field become more prominent. According to IDC research, a majority of organizations across all stages of DX are increasing their spending on cloud services and anticipate that more of their workforces will permanently work from home or in the field.

AT A GLANCE

KEY TAKEAWAYS

- Zero trust and least privilege principles are critical as the risks of assumed trust are mounting.
- Transforming principles to reliable practices is difficult.
- Micro-segmentation eases the transformation of principles to reliable practices.
- Micro-segmentation solutions vary. IDC's recommendations can help organizations select an optimal solution.

The attack surface that accompanies cloud adoption not only is expanding but also is brimming with change. Organizations have pushed forward their cloud journeys to boost speed and agility in IT operations and software development through cloud-native modularity and automation. Yet, these cloud attributes do not align well with sound security practices if the means to define and enforce security policies are complex and manual. Vulnerabilities exposing strategic assets and sensitive information are sure to arise, with breaches following.

The principles of zero trust and least privilege provide a pathway to taming this expanding and dynamic surface area. In zero trust, all entities, whether inside or outside an organization's perimeter, are branded as untrusted. Before any access is granted, the entity's trust level is verified. Complementing zero trust is the principle of least privilege. In least privilege, end users, applications, and processes are allowed only the lowest level of privilege required to perform their legitimate functions. In combination, an entity's access permissions are capped to the level of verified trust. Micro-segmentation, the topic of this IDC Technology Spotlight, is a technology that actualizes the principles of zero trust

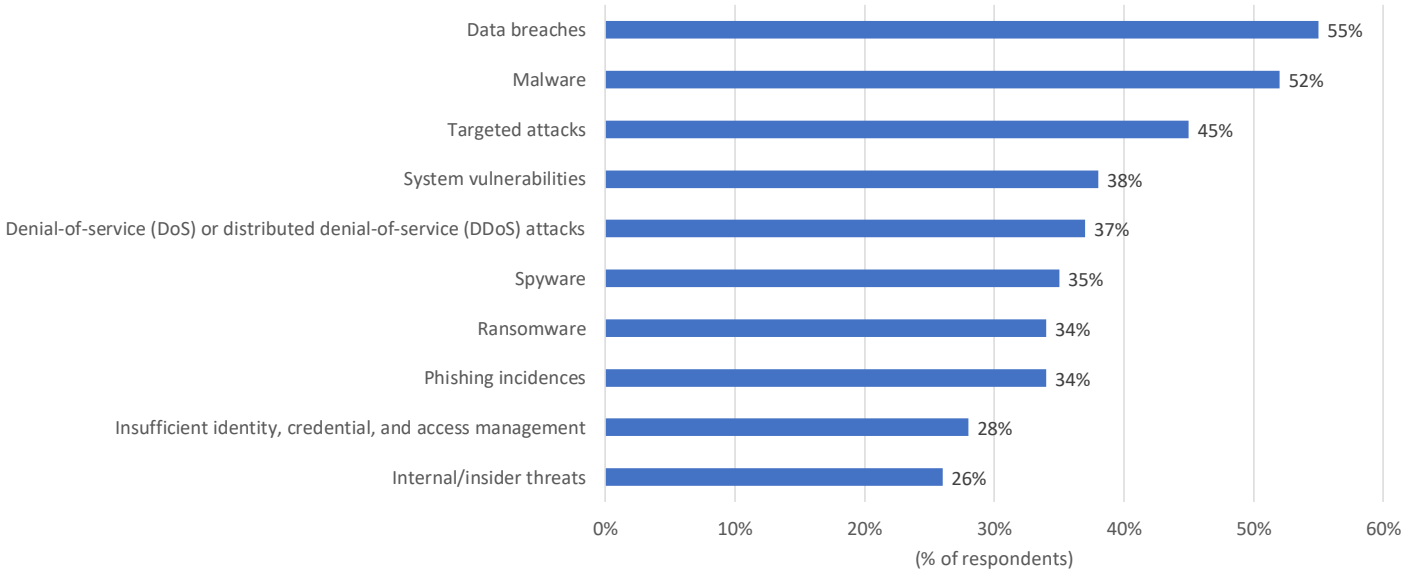
and least privilege. Through automated micro-segmentation policy creation and enforcement, the principles of zero trust and least privilege are applied across and among an organization's dynamic and diverse cloud instances (virtual machines [VMs], containers, and serverless architectures), datacenter servers, and end-user devices.

Security Concerns and Breaches Weigh on the Minds of Security Professionals

Security professionals are tasked with combatting threat adversaries that ceaselessly advance their tradecraft to identify and exploit the slightest of security gaps. In light of the rapidly expanding and highly dynamic surface area brought on by cloud adoption and remote working, plugging all potential security gaps becomes even more problematic. Not surprisingly, the variety of security concerns on the minds of security professionals is significant. IDC's 2020 *U.S. Managed Security Services/ Managed Detection and Response Survey* identified data breaches and malware as the top 2 concerns (see Figure 1).

FIGURE 1: ***Top Security Concerns***

Q *Which five factors are your organization's greatest concerns in securing business operations and IT environments?*



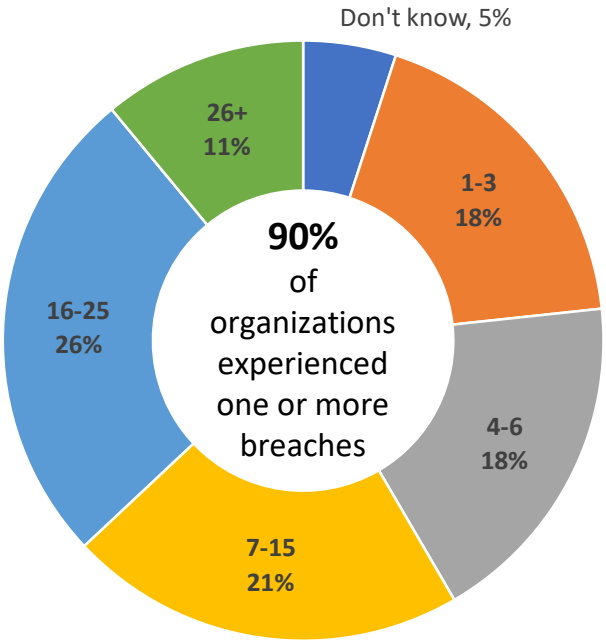
n = 410

Source: IDC's U.S. Managed Security Services/Managed Detection and Response Survey, May 2020

The high level of concern over breaches is warranted. According to the same IDC survey, 90% of organizations experienced at least one security breach in the past 24 months (see Figure 2). Nearly 60% of breached organizations encountered seven or more security breaches.

FIGURE 2: ***Security Breach Experience in the Past 24 Months***

Q ***How many security breaches/incidents has your entire company experienced in the past 12–24 months?***



n = 370

Base = respondents who experienced at least one security breach

Source: IDC's U.S. Managed Security Services/Managed Detection and Response Survey, May 2020

The Importance of Micro-Segmentation in Zero Trust and Least Privilege

Micro-segmentation, as previously noted, actualizes the principles of zero trust and least privilege. From an objective perspective, micro-segmentation equips organizations to mitigate the risks associated with an expanded and dynamic IT footprint that, by its very nature, lacks a firm foundation of trust. Contributors to this lack of trust are numerous and include the following:

- **Networks.** With cloud services and remote working, end users are originating access increasingly from unmanaged and therefore untrusted home networks and public hotspots and through the public internet.
- **Bring your own device (BYOD).** Breaking the bond between IT-provisioned user devices and corporate resources, cloud services have flung open the doors for access from BYOD. In addition, the pandemic-induced surge in laptop demand outstripped available inventory, forcing some organizations to resort to BYOD to conduct essential operations. End-user choice and convenience have also contributed to BYOD usage.

- **IT-provisioned end-user devices.** End-user devices are frequently the first point of entry for attackers to deliver their initial packets of malicious code and then move laterally. Despite advances in endpoint protection software, compromises still occur, and post-compromise detection takes time and security talent many organizations lack. In addition, device misconfigurations, excessive administrator permissions, and unpatched software add to exploitability. Thus even the most protected end-user devices can waiver in security posture.
- **End-user identities.** With high frequency, passwords remain a principle means of identification. And with the proliferation of passwords to access an increasing number of system and online resources, inconsistent and unsafe password practices ensue. As passwords can be collected from directory data breaches, phishing, and unprotected networks, the authenticity of a given individual entering a password is suspect.
- **Applications.** The business benefits of application componentization (e.g., via APIs and code repositories) and continuous integration/continuous deployment (CI/CD) practices are hard to pass up. Yet from a security standpoint, these factors also increase the risk of vulnerable applications going live and application drift degrading the application's security posture.
- **Application hosting environments.** The shared responsibility model of cloud services establishes a clear delineation in the roles of hosts and tenants. A sharp line of delineation, however, is not a guarantee that each party lives up to its responsibilities in ensuring appropriate security practices are followed consistently and comprehensively. Often, the fault lies with tenants in misconfigurations, lenient access permissions, outdated user directories, and neglected cloud instances.

Micro-Segmentation Solution Checklist

Given the many circumstances that contribute to trust uncertainty, organizations must assume that trust is not guaranteed but must be validated before access is granted and data movement is permitted (i.e., zero trust). Verification of trust, however, may not be binary or static. Rather, tiers and point-in-time verifications of trustworthiness are necessary. In addition, organizations are balancing business objectives and end-user productivity. Restricting access solely based on verified trustworthiness can be impractical. Least privilege complements zero trust by bounding access and activity to only what is necessary. In addition, least privilege boundaries can be adjusted based on the level of verified trust.

The pace of digital transformation and cloud adoption is accelerating. Cybersecurity risks are increasing, too. Organizations need a flexible framework to mitigate this risk without adding friction to their DX initiatives.

Micro-segmentation transforms zero trust and least privilege principles into a routinized discipline. In operation, micro-segmentation defines and enforces zones of least privilege in end users' application access and the communications among application resources. By implementing micro-segmentation, security teams can offset the broadening attack surface of modern applications and end-user access from untrusted devices and networks. While conceptually sound, attributes of the micro-segmentation solution are critical in ensuring operational effectiveness. IDC suggests that organizations choose a micro-segmentation solution with the capabilities described in the following checklist:

- **Facilitates identification of application resources.** Security teams cannot protect the unknown. They need a comprehensive inventory of all interconnected application resources to create least privilege application firewall policies.
- **Provides visualization.** Beyond the lines of software code, enterprise applications are an intricate web of interactions among users and resources. Visualization of these interactions serves multiple purposes: clarifies acceptable and intended patterns that follow the least privilege principle, guides the setting of allowable pattern variances, and creates a baseline from which to detect and document potentially malicious pattern deviations.
- **Incorporates business logic.** The business relevance and sensitivity of application resources vary. Automated guidance in policy creation and point-and-click functionality based on the application's business logic serves multiple objectives: adds meaningful context to application security policies and assists in identifying paths of potential lateral movement among applications that share common resources.
- **Supports uniform application protection across all hosting environments.** This feature assists enterprises in protecting each application uniformly and in migrating application and application resources among environments without sacrificing security.
- **Easily integrates into a security ecosystem.** As the security discipline is fueled by data, a broad security ecosystem facilitates access to additional sources of threat intelligence and telemetry used to strengthen security policies in defense against emerging threats.
- **Operates as a software as a service (SaaS) that leverages host-based firewall functionality.** As SaaS, the solution delivers the benefits of a cloud-based service (e.g., rapid enrollment, instant scalability, centralized management, and cloud economics) and has a light touch on host environments by utilizing the native firewall functionality of each host environment.
- **Simulates policies.** Before application firewall policies are applied, they can be simulated to confirm security effectiveness and to detect unanticipated outcomes such as blocking legitimate application functions.
- **Minimizes complexity.** Policies can be translated to firewall rules in the native language of each environment without the need for security administrators to be fluent in each environment's language.

Benefits of a Full-Featured Micro-Segmentation Solution

IDC believes that using a micro-segmentation solution that is aligned with the attributes in our checklist will help an organization realize the following benefits:

- **Improve security efficacy.** Allowing only authorized user application access and necessary application communication flows restricts the lateral movement of advanced persistent threats (APTs), prevents data exfiltration, and corrals malicious insiders.
- **Expand environment options.** With micro-segmentation operating independent of the hosting environment, an organization can select hosting environments primarily based on the business objectives of performance, cost, scalability, and adaptability.
- **Reduce administrative burden.** On the front end of applying security policies, security administrators are unburdened from having to become experts in the use of each environment's host firewall operations. On the back end, micro-segmentation based on the least privilege principle minimizes the number of security alerts to only alerts that deviate from the established baseline and have a high likelihood of being suspicious.
- **Accelerate security team's response speed.** Security administrators can create, test/simulate, and deploy micro-segmentation zones of least privilege rapidly. The solution abstracts away technical complexity so that administrators can focus on security objectives.

Considering ColorTokens

Based on NIST Zero Trust Architecture, ColorTokens Xshield delivers software-defined micro-segmentation for multicloud and hybrid data protection. Operating as a cloud-delivered service with lightweight agents, Xshield rapidly catalogs an organization's footprint of cloud instances, private datacenters, networks, and endpoints. From this viewpoint, administrators can group IT assets into logical business-oriented segments. Within each micro-segment, communication flows and dependencies are captured, displayed, and assessed for vulnerabilities and exposures.

With an actual depiction of communication flows and vulnerabilities, guided templates assist administrators in defining zero trust zones and multitier application use policies that are reusable to save configuration time. With policies created, simulation based on actual application and network traffic tests security efficacy and non-interference with legitimate business outcomes. Refined as needed, policies become enforceable using host-based firewalls. Integrated with the organization's existing identity provider and/or user directory, identity verification becomes an enforceable variable in micro-segmentation policies. Xshield's one-click segmentation supports a variety of automation tools, such as Microsoft GPO and Puppet, to enable deployment to be realized in minutes.

By continuously capturing and assessing network and application traffic, Xshield discovers new IT assets. Upon discovery, new assets can be added to an existing micro-segment and existing policies are automatically enforced. Alternatively, new assets can be grouped into a new micro-segment and new and distinctive policies can be created, simulated, and then deployed. This continuous collection of network and application traffic also supports incident response and forensics investigations.

ColorTokens Xshield aligns well with IDC's checklist of micro-segmentation solution attributes. Nevertheless, ColorTokens will be confronted with several challenges as described in the following section.

Challenges

- **Competition.** ColorTokens is not the only vendor in the security market. Addressing the increasing risks that organizations are encountering with their expanding and dynamic attack surfaces has attracted many vendors, existing and new. Rising above the clutter of vendor claims is one of the battles ColorTokens faces. In addition, organizations want to reduce their bloat of security technology stacks and vendor relationships that has grown over the years. Some organizations may view incumbent vendors and their new products more favorably than bringing in a new vendor. It should be noted, however, that micro-segmentation solutions offered by incumbent vendors and built on their legacy products were likely not designed with a zero trust architecture in mind. Therefore, organizations choosing to operationalize zero trust may well realize the benefits more quickly by choosing a vendor with a purpose-built zero trust solution.
- **Unfamiliarity and inexperience.** While zero trust and least privilege are generally understood principles, micro-segmentation is not extensively practiced as a mechanism to operationalize these principles. Overcoming this enterprise unfamiliarity and inexperience by educating the market is another challenge ColorTokens faces.
- **Future utilities and enhancements from cloud providers.** Cloud providers currently offer their own security capabilities and could expand on those capabilities in the future. Consequently, cloud providers represent a potential alternative to overlay solutions such as ColorTokens Xshield. However, with multicloud and hybrid environments being common and customers' reluctance to rely on cloud providers for both infrastructure and security, these two market conditions work in ColorTokens' favor.

Conclusion

Micro-segmentation adhering to zero trust and least privilege principles is a promising construct for protecting modern applications. Solutions based on micro-segmentation are well timed to address the increasing cybersecurity risks associated with rapid growth in cloud services and increased remote working arrangements. In addition, as most organizations will have and prefer to have a hybrid and multicloud footprint for their applications, a solution that eliminates the complexity while unifying protection is also well timed.

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.

MESSAGE FROM THE SPONSOR

About ColorTokens

For more information on ColorTokens Zero Trust security solutions, 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.
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com