netskope

White Paper

How to Apply Zero Trust Principles the Right Way

Zero Trust

Phase 0

Before You Begin

- Devise personas and assign access requirements
- Inventory all SaaS and private applications
- Inventory all data assets

Phase 1

Zero Trust Access

- Define sources of truth for identity
- Construct a mapping of users to applications
- Remove stale or unused entitlements
- Steer all access through a policy enforcement point to remove risks of direct access

Establish this zero trust access baseline

Phase 2

Adaptive Access

- Add context to access policies
- Allow context to signal whether to require strong authentication
- Incorporate context into coaching
- Continuously adjust access policies

Enrich the trust baseline for authorization within app activities.

Phase 3

On-demand Isolation

- Insert remote browser isolation for access to risky and low-reputation web sites
- Monitor for command-and-control attempts and other anomalous behavior

Apply explicit trust controls to destinations

Phase 4

Continuous Data Protection

- Differentiate access by managed and unmanaged devices
- Adapt access policies based on context
- Ensure correct configuration of cloud resources
- Identify sensitive information and control its spread
- Continuously assess sharing permissions and app-to-app integrations

Continuously investigate and remove excess trust. Adopt and enforce a least-privilege model everywhere.

Phase 5

Inform & Refine With Real-time Analytics

- Maintain visibility over applications and risk
- Inspect cloud and web activity for best assessments of and adjustments to policies
- Create visualizations tailored to various stakeholders
- Implement closed-loop policy refinement

Strengthen security and trust posture with closed loop refinement of policy

WHY SO MUCH EMPHASIS ON "ZERO TRUST," AND WHY NOW?

The past few years have demonstrated that companies can adapt to massive change when much of the world's workforce suddenly transitioned to remote work. The change was initially disruptive, and not all industries can or should sustain a mostly-remote work style. But for many companies, remote work is already the new normal. Employees and their business partners require access to applications wherever they reside (on-premises, SaaS, public cloud) from whatever kind of device (managed or unmanaged), and they expect that access to be steady, fast, and efficient.

The zero trust model is ideally suited to accommodate such a requirement. Broadly, two categories of products implementing this model have emerged since "zero trust" was first coined more than a decade ago: zero trust network access (ZTNA) and identity-based segmentation (microsegmentation). And, these days, there's more marketing around the "zero trust" term than for all but a handful of security-centric concepts and buzz phrases.

But it's in the use of *context* where cloud security architectures that apply zero trust principles distinguish themselves from the many so-called products marketed as "zero trust." A context-driven approach to zero trust might best be described as achieving continuous adaptive trust—in which the technology can not only manage entitlements (e.g. who has access to what data or applications) but also define the attributes and contextual elements that together determine the level of confidence required for interacting with resources. In environments where traditional access and authorization models can't be well defined, the addition of context enables a more accurate assessment of trust.

CONTINUOUS ADAPTIVE ZERO TRUST

A Secure Access Service Edge (SASE) or hybrid security-networking environment consists of the ability to establish continuous adaptive trust across users, devices, networks, applications, and data to increase confidence in policy enforcement everywhere.

The primary goal of a zero trust approach is to shift from trust but verify to verify then trust. Resources no longer place implicit trust (IP address, for example) in any entity that wants to connect. But evaluating the confidence level at the start of any interaction is insufficient. During the interaction, context should be continuously evaluated. Alterations to the context can result in an adaptation (an increase or a decrease) in the level of trust, which is likely in turn to alter the type of access to the resource.

Continuous adaptive trust overcomes the limits of binary decision-making so often seen in security architectures. Binary decisions such as "full access" vs. "no access" lack the flexibility required by contemporary and emerging work styles — for example, a higher-risk SaaS application necessary for employee productivity but unmanageable with simple "all" or "nothing" access.

The crucial ingredient is that access should be context-aware, balancing trust against risk. The continuous adaptive trust model increases the requirements for the level of confidence in parallel with the value of the asset being accessed. Based on signals such as application or activity risk, user risk, data sensitivity, device posture, user location, and other attributes, adaptive access provides the ability to make real-time decisions to permit, deny, restrict, redirect, and even coach the user. Adaptive access aligns policies with risk appetite, which may include revocation of access, if required at a point in time.

BUSINESS OUTCOMES

Companies can achieve their business goals without making security tradeoffs by building continuous adaptive trust into their security and risk programs and into their digital transformation plans from the outset. This yields several key benefits.

Agility in the business

Agility in business requires elasticity in infrastructure and services both in scale of volume and location and in breadth of new services and applications. Outcomes that can and should be achieved based on zero trust principles in a SASE and hybrid architecture include:

- Harmonized user experience — access is the same regardless of where a user is; access is predictable regardless of the user's device type.
- Location independence — application access is decoupled from the underlying network design; applications can be moved (say from on-premises to the public cloud) without forcing users to change their habits.
- More opportunities to provide some degree of access — to reorient the majority of security decisions away from "no" toward "yes, with conditions."
- Increased collaboration with suppliers and partners without provisioning local user accounts for them and without placing demands on their computing environment.
- Proactive security operations built to support the growth of applications and to eliminate the fire drills of hunting down and retroactively securing access to applications after they're already deployed.

Reduction of risk

Cyber risk is a priority for most boards of directors, especially with the potential costs of a security incident so onerous. Every company must determine its own risk appetite and tolerance, though these tend to be roughly the same for most companies in any given industry. Managing risk is complicated by dependency on increasingly lengthy and opaque supply chains, the proliferation of cloud services and applications, and an ambiguous regulatory environment.

Risk reduction in this new environment will involve a zero trust approach in which:

- Resources are moved from public to private access and thus shielded from the internet, invisible to those who lack strong access credentials or the ability to demonstrate confidence.
- Inappropriate access is constrained, reducing the blast radius of compromised accounts.
- Visibility into sensitive data types, locations, and movements is improved and constant.
- Analytics offer the whole picture of acceptable policy and behavior, thereby more rapidly surfacing risks and threats (both anomalous and malicious activity) for quick containment and neutralization.
- Overall security posture is improved, making companies less attractive to attackers.

> According to Gartner, "sensitive-data visibility and control is a critical capability of SASE" and if that inspection point non-negotiably needs to follow the data, that means the inspection point needs to be in the cloud so that its benefits can be delivered to users and delivered to the apps.

Streamlined product deployment and maintenance process

Business agility and risk reduction require the right architecture, including:

- A cloud-native security service that scales as the business requires, eliminating the deployment complexities and capacity constraints commonly associated with hardware security appliances.
- A single cloud platform, single-pass inspection, and policy enforcement point, driven by a single console and policy engine that is applied to ensure a consistent security policy across all channels.
- A single vendor relationship that eliminates delays commonly accompanying troubleshooting and repairing products with untested or unknown interoperability characteristics

A state of continuous adaptive trust, in which the principles of zero trust are judiciously applied across the security architecture favoring context for what governs trust, is achievable today.

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply Zero Trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements. Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.

©2022 Netskope, Inc. All rights reserved. Netskope is a registered trademark and Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks are trademarks of their respective owners. 06/22 WP-552-1