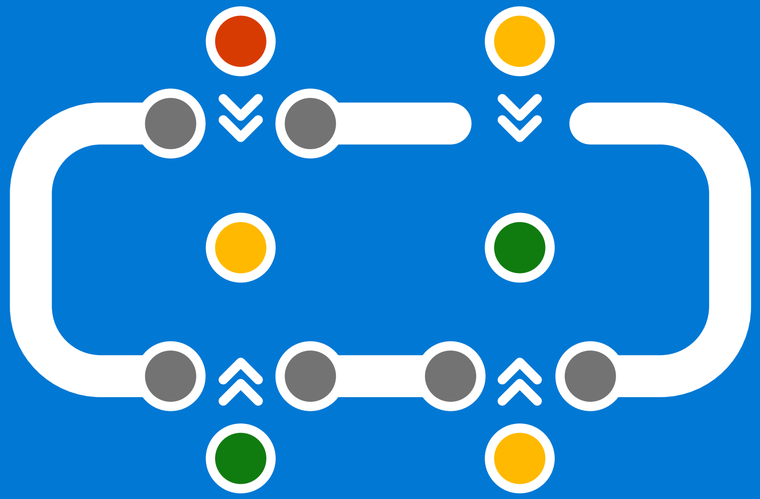
Microsoft Security

10 Tips for Enabling Zero Trust Security

The widespread adoption of public cloud services and the growth of the mobile workforce have rendered perimeter-based security models obsolete.



An organization's applications and data are likely to exist both inside the traditional firewall and beyond it. Security and IT teams can no longer assume that users and their devices (both personal and corporate) on the network are any safer than those on the outside. Perimeter controls do little to prevent an attacker from moving laterally on the network after gaining initial access to it.

What's needed is a pivot to "boundaryless" security, known more commonly as Zero Trust. In a Zero Trust model, all users and devices—both inside and outside the corporate network—are deemed untrustworthy. Access is granted based on a dynamic evaluation of the risk associated with each request. The same security checks are applied to all users, devices, applications, and data every time.

Zero Trust is gaining traction

Interest in Zero Trust is strong. A new IDG survey finds that 21% of organizations have already adopted a Zero Trust model and 63% plan to do so over the next 12 months[1]. In a separate 2018 Security Priorities survey from IDG, 35% said they planned to increase spending on Zero Trust or create a new spending category for it. Another 30% viewed Zero Trust as a potential new investment area[2].

Although Zero Trust has been gaining momentum, the approach is not new. In 2004, a security consortium known as the Jericho Forum was formed to promote the idea of "de-perimeterization" – focusing on finding ways to protect data across new platforms[3]. Analyst firm Forrester coined the "Zero Trust" term in 2010[4]. Interest in Zero Trust has been growing recently, especially among organizations looking for a way to prevent attackers from moving laterally on the network.

Getting to a Zero Trust model can take years of effort and require collaboration across the enterprise. If you are committed to deploying a Zero Trust model, or even if you're just considering it, here are 10 tips to help make your journey a bit smoother.

[1] IDG Explorer survey, May 2019.
[2] IDG Security Priorities study, https://www.idg.com/tools-for-marketers/2018-security-priorities-study/, 2018.
[3] Wikipedia, https://en.wikipedia.org/wiki/Jericho_Forum, undated.
[4] CSO, https://www.csoonline.com/article/3287057/what-it-takes-to-build-a-zero-trust-network.html, July 2018.

Tip 1

Realign around identity

Identity is the best starting point for Zero Trust.

Users can have multiple devices and access enterprise resources from a variety of networks and apps. Almost all of these resources require authentication, making identity a common denominator across all access requests, whether from a personal device on a public Wi-Fi network or a corporate device inside the network perimeter. Using identity as the control plane lets companies treat every single access request as untrusted until the user, device, and other factors are fully vetted.

Many organizations focus on micro-segmentation as an approach to enabling Zero Trust, but this approach has significant limitations.

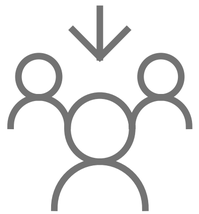
Micro-segmentation can be useful in reducing attack surfaces and for breach containment within on-premises, legacy application environments.

However, this approach is less effective in cloud environments where the networks between enterprise assets are often not owned or managed by IT.

Zero Trust represents a cultural shift from network-based controls to identity-based policies and processes. Teams across specialization silos should align around identity-based protection to lay the groundwork for a Zero Trust model. “Building the identity foundation is the best starting point,” says Mark Simos, lead architect with Microsoft’s Cybersecurity Solutions Group. “It sets you up with a good access gateway between your assets and potential threats to them.”

Tip 2

Implement conditional access controls



Hackers routinely compromise identity credentials and use them to access systems and move laterally in the network.

Trust cannot, therefore, be inferred solely from whether a particular user or their device is inside or outside the corporate network.

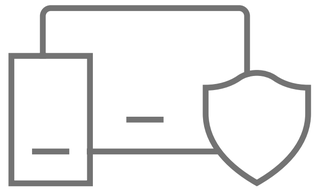
Instead, **adopt an "assume breach" mindset and trust no request until it is fully vetted.** For Zero Trust, access control decisions should be dynamic and granted conditionally based on an evaluation and contextual understanding of the risk associated with every single resource request across multiple dimensions.

This conditional access approach considers user identity and access rights, device health, application and network safety, and the sensitivity of the data being accessed.

An enforcement engine, guided by a set of granular policies, is then used to decide whether to allow, restrict, or block access to the requested resource. A Zero Trust network with the right conditional access policies for users and devices can prevent hackers from using stolen credentials to move laterally in the network.

Tip 3

Strengthen your credentials



Weak passwords undermine the security of your identity system and make it easy for hackers to compromise your network via, for example, password spraying or credential-stuffing attacks.

Making multifactor authentication a part of conditional access restrictions can help enable better user verification and limit the ability of hackers to misuse stolen credentials.

It provides an additional layer of user validation, especially for gating access to critical applications and data.

Tip 4

Plan for a dual-perimeter strategy

To prevent business disruption and re-introducing old risks, maintain existing network-based protections while adding new identity-based controls to your environment.

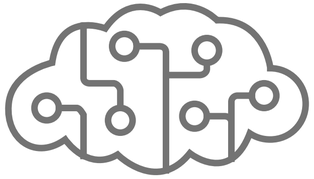
"In a Zero Trust context, you really have to start looking at your applications as either cloud or legacy," Simos says. Cloud-native applications support identity-based controls and allow for conditional access rules to be layered on relatively easily.

The other category consists of applications that were designed to sit behind network firewalls in legacy environments.

These applications require modernization to support identity-based conditional access. One option to do this at scale is enable access via a secure authentication gateway or application proxy, which also may allow you to eliminate VPNs (which can lower your risk).

Tip 5

Integrate intelligence and behavior analytics



Support for identity-based access control in cloud applications is not the only reason to accelerate cloud migration.

The cloud also generates richer telemetry to enable better access control decisions. For example, such telemetry can augment conditional access controls by making it easier to infer abnormal user or entity behavior to identify threats.

Your ability to make good access control decisions depends on the quality, quantity, and diversity of signals you integrate into those decisions.

Integrating threat intelligence sources like IP addresses for bots or malware, for example, will force adversaries to constantly acquire new resources. Integrating more detail about the log-on (time, location, etc.) and seeing if it matches the user's normal routine will be harder for attackers to mimic, while minimizing user inconvenience.

Tip 6

Reduce your attack surface

To bolster the security of your identity infrastructure, it's important to minimize your attack surface. (That's good security practice in general, of course.)

For example, implementing privileged identity management will minimize the likelihood of a compromised account being used in an administrator or other privileged role.

It's also a good idea to block apps using legacy authentication protocols.

This is critical because these protocols don't support conditional access or multifactor authentication, allowing attackers to bypass them.

In addition, limit authentication access entry points to control how users access apps and resources. This will also help to reduce the impact of compromised credentials.

Tip 7

Increase security awareness

Your identity and endpoint infrastructure can generate a high volume of security events and alerts.

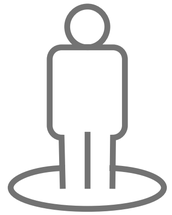
Use a Security Information and Event Management (SIEM) system to aggregate and correlate the data to better detect suspicious activities and patterns that indicate potential network intrusions and events, such as leaked credentials, bad IP addresses, and access from infected devices.

A SIEM system can be used to audit user activity, document compliance with regulatory requirements, and help with forensic analysis.

It can also improve monitoring of least privileged access and ensure that users only have access to resources they really need.

Tip 8

Enable end-user self-help



Users are likely to be far less resistant to Zero Trust than they are to many other security initiatives.

That's because they're already familiar with identity-based access on their personal devices and apps and want the same experience at work. Zero Trust enables security organizations to secure (and say "yes" to) modern productivity scenarios like mobile devices, BYOD, and SaaS applications, keeping users happy without compromising security.

IT teams can reduce friction by empowering users to carry out certain security tasks, such as self-service password resets.

Allowing users to reset or unlock their account passwords without administrator involvement—while monitoring for abuse or misuse—ensures a good balance between security and productivity.

Similarly, implementing self-service group management allows owners to create and manage groups without needing an administrator to do the job.

Tip 9

Don’t overpromise

Zero Trust is not a single “big bang” initiative like implementing multifactor authentication.

It really is about a long-term end stage with a new generation of security controls that are built entirely differently from traditional network-based access models.

Achieving the vision takes time, via a continuing set of smaller projects.

Along the way, it’s important to set and manage expectations appropriately. Garner support from key stakeholders and have a plan for communicating effectively with them through the project lifecycle. Prepare to take steps to overcome cultural resistance and other challenges from groups long used to doing things very differently.

Tip 10

Show value along the way

One of the most effective ways to build long-term support for a Zero Trust initiative is to demonstrate incremental value with each investment.

In IDG's security survey, more than half of the respondents (51%) said a Zero Trust access model would help improve their ability to protect customer data and 46% said it would help enable a superior and more secure end-user experience.

Quantifying such benefits can be difficult, however. Another way to measure success is to focus on the cost to the attacker. Are your Zero Trust investments making it more expensive for the threat actor to attack you? Is it getting harder to break into your network?

"The key is to make it continually harder, so that each individual investment changes the attacker's view of your network," Simos says.

A model for the future

There's no way to predict which new exploits will appear in the wild on any given day or how they might gain entry into your environment. Because one can never assume that any particular user or the device, app, or network they're using is completely safe, the only reasonable approach to security is to trust nothing and verify everything.

A Zero Trust model is not easy to achieve, but it's a key element of any long-term modernization objective for the digital enterprise.

Assess your Zero Trust maturity stage (Traditional, Advanced or Optimal) to determine where your organization currently stands.

Zero Trust maturity model assessment tool

Microsoft