BlackBerry. Intelligent Security. Everywhere.

The New Concept of Zero Trust

As organizations look to implement Zero Trust technologies, it's critical to keep in mind that no single technology platform or service can wholly deliver Zero Trust. To achieve a Zero Trust access control posture, organizations need to think through the following aspects of how their environment operates.

Here's a list of steps to take in order to conduct a proper assessment:

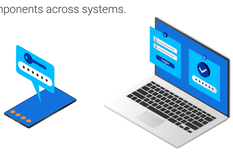
1 Define Trusted Users and Trusted Devices

To get started, a discovery effort is critical. Most micro-segmentation and Zero Trust technologies include some form of scanning and discovery tools to find identity use and privilege allocation, application components in use, traffic sent between systems, device types, and behavioral trends and patterns in the environment.

Security teams should work with Identity Access Management (IAM) teams or those responsible for key IT operations functions to understand the different groups and users within the environment, as well as the types of access they need to perform job functions. The same should be done for all types of user devices, primarily laptops and desktops, in use by privileged users.

2 Integrate Identity (User/Device) and Network

After some basic discovery has been conducted, any mature access control (micro-segmentation) policy engine should be able to start linking detected and stated identities (user, groups, devices, and privilege sets) with network traffic generated by specific services and application components across systems.



To get the most benefit from a Zero Trust strategy, this stage of planning and project implementation needs to carefully accommodate business and application centric use cases.

Security teams should plan to evaluate what types of behaviors are actually needed and necessary in the environment, versus those that may be simply allowed or "not denied" explicitly.

3 Determine Where Remote Access Fits

A very critical element of Zero Trust planning and implementation is increasingly common remote access and remote work arrangements for a wide variety of employees. Zero Trust technologies that also focus on remote access may include some of the following capabilities:

Endpoint Protection – Anti-malware and exploit protection monitoring is becoming more common in remote access agents associated with Zero Trust tools.

Endpoint Detection and Response – Endpoint monitoring for both signature-based and malicious behaviors can significantly improve the security posture of trusted endpoints, with automated quarantine and elimination of detected threats adding even more value.

Data Loss Prevention – Monitoring and protection of specific data patterns and types is not a common feature for Zero Trust and micro-segmentation technologies but adds significant value to help align granular policies with application and service use cases.

Mobile Protection – Mobile device sandboxing and protection is also a valuable feature for any enterprise Zero Trust technologies.

4 Review Zero Trust Best Practices

Organizations should keep the following general best practices in mind for implementing Zero Trust tools and controls:

Start with passive application discovery, usually implemented with network traffic monitoring. Allow for several weeks of discovery to find the relationships in place and coordinate with stakeholders who are knowledgeable about normal traffic patterns and intersystem communications.

Design Zero Trust architecture based on how data moves across the network and how users and apps access sensitive information. This will assist in determining how the network should be segmented and where protection and access controls should be positioned.

Take the time to categorize systems and applications. More advanced Zero Trust tools integrate with asset identities, which may be part of an application architecture, aligned with a business unit or group, or representative of a specific system type.

Look for products that work in both internal and public cloud environments where possible. This will almost always require an agent-based solution.

Conclusion

A Zero Trust architecture should include authentication and authorization controls, network access and inspection controls, and monitoring/enforcement controls for both the network and endpoints.

No single technology currently will provide a full Zero Trust design and implementation – a combination of tools and services is necessary to provide the full degree of coverage needed.

For most, a hybrid approach of both Zero Trust and existing infrastructure will need to coexist for some period of time, with emphasis on the common components and control categories that could suitably enable both, such as identity and access management through directory service integration, endpoint security and policy enforcement, and network monitoring and traffic inspection.

As Zero Trust frameworks mature and evolve, so will standards and platform interoperability, likely facilitating more streamlined and effective approaches overall.

For more information about how to build and execute a successful Zero Trust approach, including a look at where Zero Trust security frameworks are headed, *access a full white paper here.*