Zero-Trust Cybersecurity

Add Value to your Business with your Cybersecurity Network Strategy

Over the past two years cyber-threats have increased due to a variety of circumstances, leaving companies vulnerable and directly affecting their reputation and performance. Therefore, effective cybersecurity must now be considered as a competitive advantage for any business. Showing that you care for your business protection, means that you care about your customers and their data security while using your products and services.

To stay ahead of cyber-crime your network security strategy needs to be a concentrated, multi-directional, multi-layered effort that encompasses all endpoints. Despite increased user-awareness and training, over 80% of ransomware attacks are a consequence of human error (1), as organised attackers are using more sophisticated techniques to deceive users. So even though training is an essential part of protecting against a cybersecurity breach, companies can't rely only on that alone. Other measures must be put in place to prevent cyber-crime from happening. That is where Zero-Trust Security comes in.

What is Zero-Trust Security?

Zero-Trust Security is based on the concept 'Trust No-one' requiring the organization to validate all users, applications and devices, whether they are inside or outside of the organization's network, before providing access. By configuring a series of security policies these approaches will grant or deny access to the data within your network, preventing an attacker from having lateral access, minimising the risks of vulnerabilities and cyber-threats.

Traditional network security, often known as perimeter security, focuses on keeping external attackers from entering the network but is vulnerable to threats from users, applications and devices inside the network. What happens when internal elements are already compromised with malware?

Network Critical
The Window to your Network™

The new approach of Zero-Trust Security assumes that internal sources are unsafe, and enforces multi-layered policies that apply the same controls to internal as well as external sources. This ensures that any attempt to access network services will face the same audit controls regardless of their source. Hence Zero-Trust is the new approach network security administrators are adopting to stay secure from the inside.

VPNs & Zero-Trust - A combined approach

There have been many discussions about which approach is the most effective at providing secure access to corporate data in a networked environment, and two most commonly mentioned approaches are Zero-Trust Network (ZTN) and Virtual Private Network (VPN).

ZTN is based on clearly defined access control policies, whereas VPN establishes a private and encrypted tunnel between a remote end-point and the organization's network. While these approaches are conceptually very different in how they provide security, the key difference is that VPN grants implicit access to all services from the remote site across the entire network, whereas ZTN grants explicit access only to specific service sockets between specific end-points.

Therefore, while VPNs provide an excellent solution to the problem of securely connecting remote sites across public networks, they don't limit the services that the 'trusted' remote site has access to. With a Zero-Trust security approach, services from the remote site are assumed to be unsafe, so ZTN access control policies are enforced to provide access only to the verified services.

However, as the National Institute of Standards and Technology (NIST) Cybersecurity Framework recommends, all network security strategies should take a multi-layered approach. Layered network security is a method that uses a combination of security controls to defend the most vulnerable portions of your technological environment from a breach or cyberattack. As a result, combining VPN with ZTN ensures that your network is secure from both the inside and out, guaranteeing that each component of your cybersecurity plan has a backup in case of defects or holes. These layers work together to strengthen the defences and form a solid foundation for a robust network security strategy.

Building a Zero-Trust Architecture

Usually, Zero-Trust is linked to securing the network from users, however, a complete Zero-Trust solution includes not only users but the whole infrastructure. From routers, switches, cloud services, and IoT,

everything in your network infrastructure must be addressed with the 'Trust No-one' approach. Zero-Trust architecture, when implemented appropriately, not only improves overall security but also reduces security complexity and operational overhead.

The **four core tenets** of IBM Security's zero trust governance model (2) include:

- **Define Context** – Discover and classify resources based on risk. Coordinate actions across the ecosystem for consistency and context.
- **Verify and Enforce** – Protect the organization by quickly and consistently validating, enforcing and implementing zero trust policies and controls.
- **Rapid Response** – Resolve and remediate security incidents with minimal impact to the business by taking targeted actions based on context.
- **Analyze and Improve** – Continually improve security posture by adjusting policies and practices to make faster, more informed decisions to tighten security around each resource.

Boost your Security with Zero-Trust Technology

There are key benefits of a Zero-Trust Architecture, for example, having Real-Time Authentication ensures your employees' access is verified by policies based on parameters such as location in real-time. Also, it helps keep the corporate networks and digital landscape safe in remote-work environments. Finally, restricting access across your corporate network is another way to minimize the exposed attack surface, and is vital to ensuring you are continuously safeguarded from advanced cyber threats, data breaches, and other network vulnerabilities.

Adding Value your Business

Leaking sensitive customer data to the public domain, bringing down the production environment, or requesting a ransom for selling your customer's personal information to other bad actors; All these events can harm a company's reputation, make a company legally liable, or have significant financial and business repercussions that put a company at risk. With Zero-Trust Security in place these disastrous situations could be prevented.

Network Critical's INVIKTUSTM cybersecurity system is the strongest low-level security for your critical network, ensures data and resources are securely connected through a deny-by-default policy and authorization. This additional internal security layer has been designed from the ground up with the security and network managers in mind. Network Critical knows that users of this device need a low-cost, easy-to-use, and highly reliable device to secure the network, reach objectives, and stay within budget.

This new solution is completely invisible to the network it protects, as it makes security devices undetectable to any intruder. Hackers can't attack what they can't see, so having INVIKTUSTM in place gives the customer the reassurance that your company is highly protected and cares about protecting their data as well. With the 'Lock & Leave' functionality, INVIKTUSTM is easy-to-use and requires little to no maintenance. While protecting your corporate network, this Zero-Trust Security solution does not compromise its performance, keeping your company at its best.

For more information, visit
www.networkcritical.com

Network Critical
The Window to your Network™

www.networkcritical.com