CGI Netherlands
Zero Trust security concept

In todays world workloads are being moved to the cloud and employees expect productivity everywhere. With all the benefits this brings it also increases security challenges.

The world of business is undergoing a major shift as more organizations are embracing the cloud and adopting a remote work culture. While this transition has brought many benefits, such as increased flexibility, cost savings, and access to innovative technology, it has also introduced new security challenges.

Your company data and applications move to the cloud and are accessed from multiple devices and locations. This requires a proactive approach to security, with measures such as data encryption, access controls, and monitoring in place to protect against cyber threats. In this fast-paced and ever-evolving business landscape, addressing these challenges is crucial for organizations to stay competitive and secure in the long run.

Zero Trust security concept

Zero Trust is a security framework that emphasizes the principle of "never trust, always verify." In a traditional security model, the assumption is that everything inside the network is trustworthy and secure, and security is focused on protecting the perimeter. However, modern security risks have evolved to be more sophisticated, and attacks can come from both inside and outside the network.

Zero Trust takes a different approach, assuming that no user or device should be trusted by default, regardless of their location or origin. This means that every request for access to resources, whether from within the network or outside it, must be authenticated, authorized, and validated before access is granted.

Zero Trust mitigates modern security risks in several ways:

Reduces the attack surface: Zero Trust minimizes the number of resources that are exposed to potential threats. By implementing strict access controls and segmentation policies, Zero Trust limits the scope of any attack that manages to breach the network perimeter.

Managed Security

CGI NCE GTO delivers a full set of managed security services to manage your security risks.

- Security Operation Center Global threat intelligence
- Managed SIEM
- Threat prevention EDR/XDR
- Vulnerability management
- Penetration testing
- Security awareness training

Improves visibility and control: With Zero Trust, organizations have greater visibility and control over user access and behaviour. By enforcing strict access controls, organizations can track user activity and detect anomalies in real-time, which enables them to respond quickly to potential security threats.

Protects against insider threats: Zero Trust assumes that no user or device is inherently trustworthy, which means that even insiders are subject to strict access controls and monitoring. This helps prevent insider threats from compromising sensitive data or systems.

Facilitates secure remote access: With the rise of remote work, many organizations have had to implement new security measures to protect against remote access threats. Zero Trust provides a framework for secure remote access, ensuring that users can only access the resources they need, and only after being authenticated and authorized.

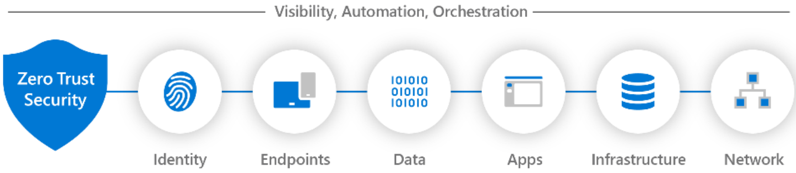
Overall, Zero Trust is a more holistic and proactive approach to security that can help organizations mitigate modern security risks and protect their critical assets.

Our solution

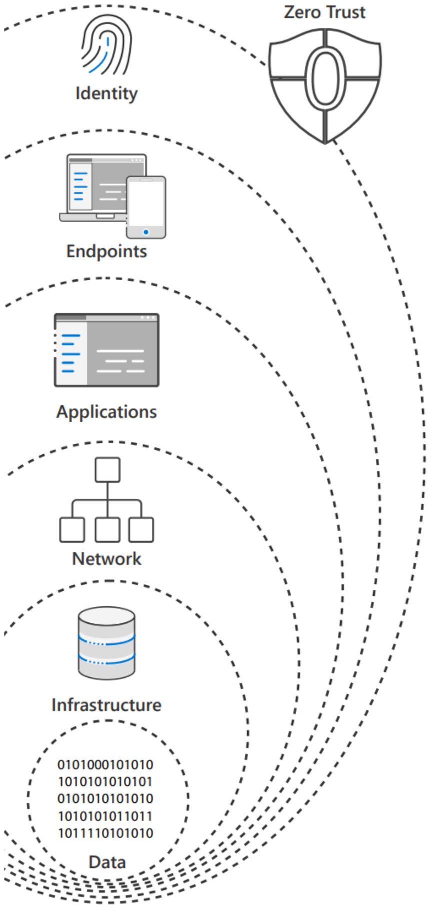
CGI can help your organization to adopt the Zero Trust security concept. With our expertise and experience we can guide you through the process of implementing a Zero Trust framework, from assessing the current security posture to designing and deploying a tailored solution. This will enable your company to implement best practices in security and mitigate modern security risks effectively.

We offer you:

- Best practices for implementing Microsoft Zero Trust security framework which offers great integration with Microsoft 365 modern workplaces while protecting all your cloud workloads.



- Zero Trust impact analysis to help identify the potential impact of implementing a Zero Trust security model on your existing infrastructure, operations, and user experience.
- Zero Trust roll-out for the gradual implementation of a Zero Trust security model across your organization's systems and applications, ensuring that access controls, segmentation policies, and other security measures are deployed in a phased and controlled manner.
- Seamless integration with cloud and modern workplace services.



Insights you can act On

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across 21 industry sectors in 400 locations worldwide, our 90,250 professionals provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit cgi.com/nl/

Email us at info@cgi.com