YISDA

You can’t hack what you can’t find.

Problem Statement

In today's rapidly evolving digital landscape, both traditional and hybrid networks confront a spectrum of cyber threats. The attack surface, driven by the widespread adoption of digital technologies and the proliferation of internet-connected devices, opens up numerous entry points for malicious actors. In addition to current cyber solutions, a proactive and advanced solution is needed to safeguard our most valuable digital assets, data, and vulnerable systems while still providing the remote access demanded by today’s workforce.

The Yisda Cloaking Technology (YCT)

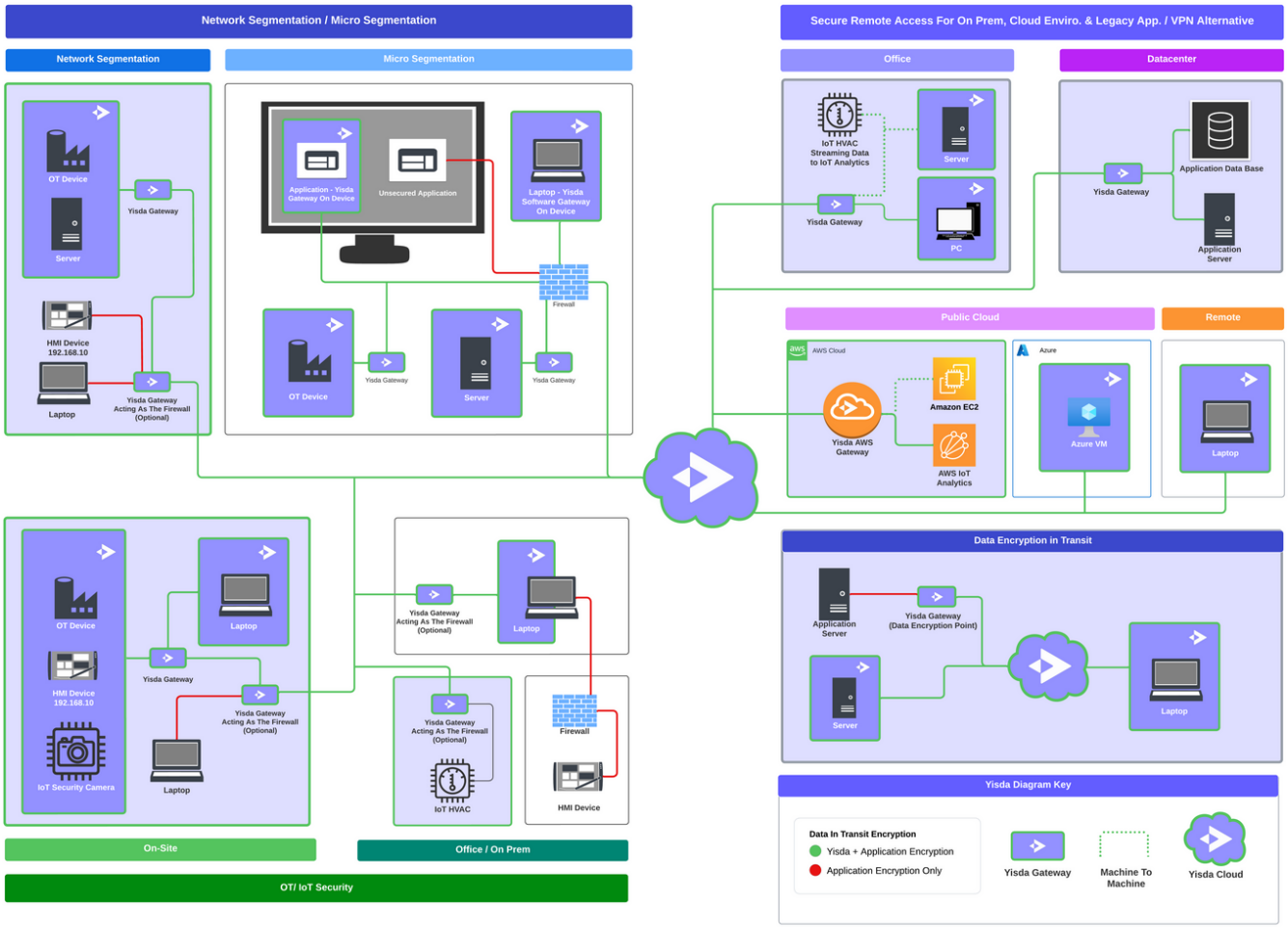
The Yisda Cloaking Technology provides flexible protection to the digital assets you deem most critical.

We understand you have data with strict compliance requirements, legacy systems requiring segmentation, and valuable digital assets protecting sensitive data. These examples and many others ultimately increase your attack surface and make you vulnerable. Prevention is a key strategy that can be achieved through an implementation of the Yisda Cloaking Technology.

- Yisda Host Agent can be installed directly on a server hosting critical applications.
- You can place the physical or virtual Yisda Gateway on your network inline or adjacent to other assets creating a cloaked network segment.
- The Yisda Agent maps a local service address and port to a Cryptographic Yisda Address.
- The Yisda Overlay Network does not use DNS servers or IP addresses, rather cryptographic addresses are used for connections.

- The Yisda Overlay Network is built to allow private, zero-trust access to the assets on your network.
- The Yisda Client provides you access to the Yisda Overlay Network or locally hosted Yisda Network, and your secured digital assets.

Yisda Network Map



Next Generation Secure Access

Most organizations use VPNs to allow remote employees access to applications and services hosted in their corporate data centers. With increasingly remote and hybrid workforces; organizations are looking for alternatives to VPNs because:

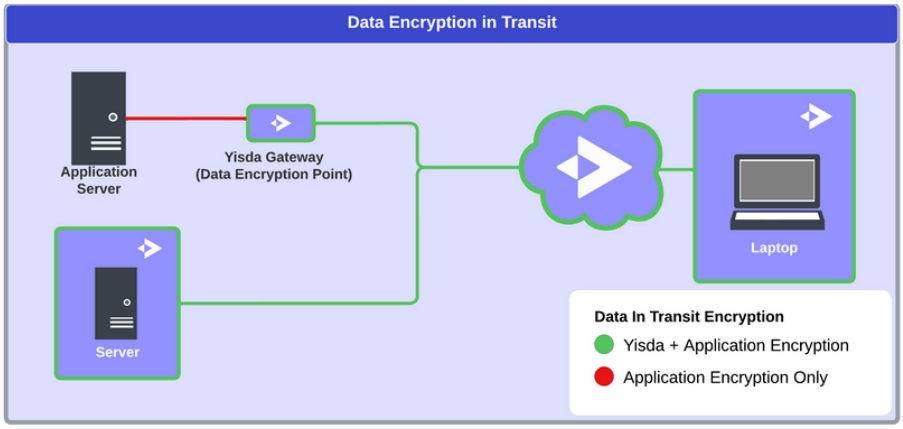
- VPNs require open listening ports and are visible on the public internet and susceptible to attacks
- Users connected to a VPN are able to scan and discover all applications and services hosted on the network
- Because most VPNs rely on a single appliance, increasing network capacity is cumbersome and difficult. This creates a single point of compromise or failure.

Yisda solves many of the challenges faced by VPNs and Jump Servers while still allowing secure access.

- Yisda does not require open ports on your network devices, thus removing their visibility from the internet or internal networks..
- Yisda prevents lateral network movement. Users are only able to access and discover the specific services and applications for which they have permission.
- The Yisda Overlay Network consists of multiple redundant servers and does not have a single point of attack or failure.

End-to-End Encrypted Data In-Transit

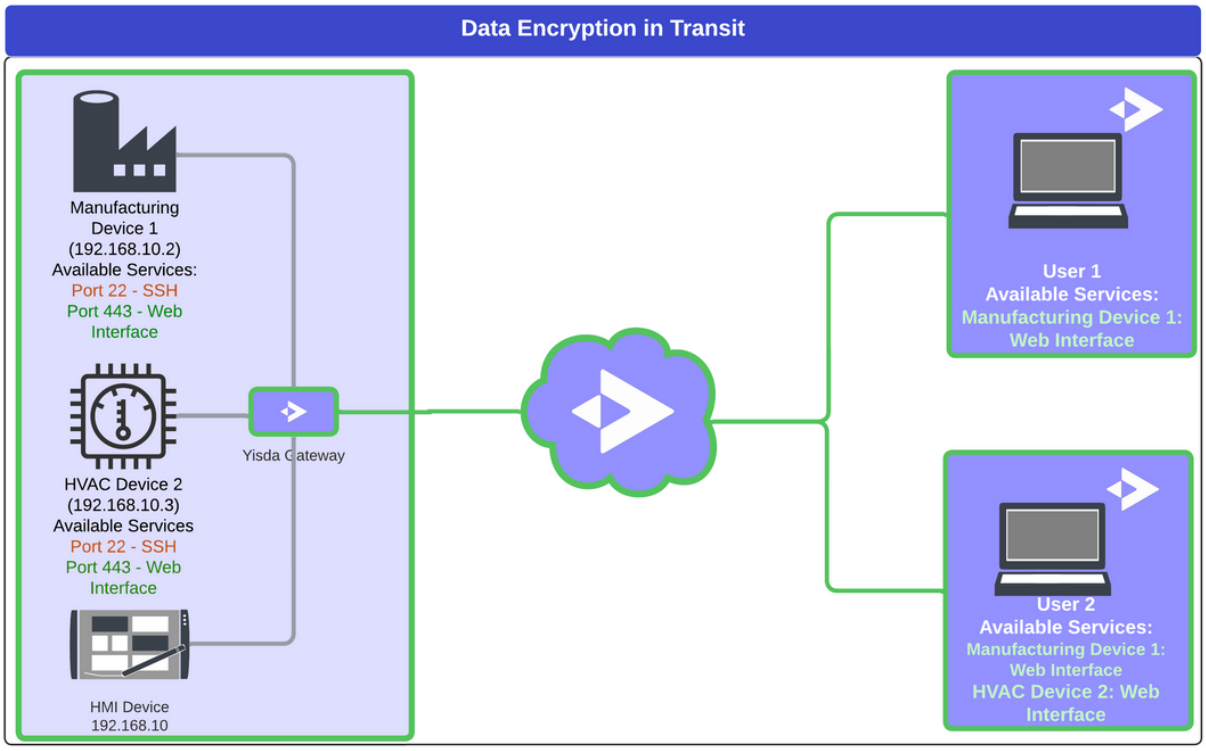
Traffic to and from clients and Yisda gateways uses multiple layers of encryption. Yisda uses AES and Diffie-Hellman Key Exchanges to protect your data while in transit. Yisda is crypto-agile and able to support different cryptography/key exchange methods and standards.



Targeted Access Policies Prevent Lateral Network Movement

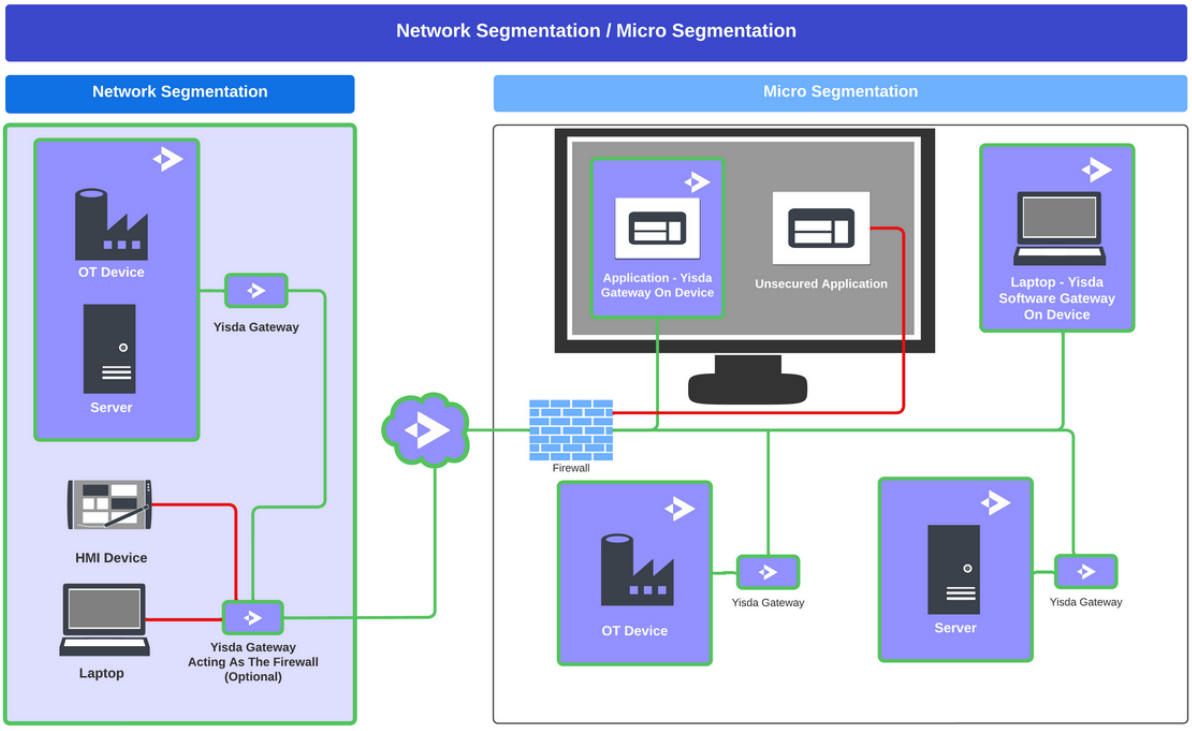
Yisda Cloaking Technology allows you to grant access to specific services and ports within a network segment rather than granting access and visibility to all assets within a network. A client that has been granted access to a specific Secured Asset is only able to connect to and discover that asset.

In the example below 'User 1' has permissions for Manufacturing Device 1 Web Interface. User 2 has permissions for the web interface of both Manufacturing Device 1 and HVAC Device 2. Neither user has been granted access to the SSH services or the HMI device. Because access is targeted to the specific asset and service (IP:port) the users are not able to move laterally to discover other services or devices within the network. Each destination on a network is uniquely designated. Users are only able to connect to and discover the services to which they've been given access.



Micro or Macro Segmentation

A single Yisda Gateway is capable of cloaking and securing access to multiple secured assets. This allows the Yisda Cloaking Technology to enable both Micro and Macro network segmentation. This flexibility allows Yisda to work with your current network infrastructure to protect targeted critical servers and applications without replacing existing firewalls. Yisda gateways can also be used to protect whole network segments. When an asset or network segment is secured by Yisda, it is cloaked from discoverability from other users on the network. Only those who have the Yisda client installed and have been granted access will be able to connect to or discover the assets secured via Yisda.



If you would like more information, a demo, or a deep-dive on the Yisda technology please contact lrichardson@yisda.com

You can't hack what you can't find.