WAN DYNAMICS

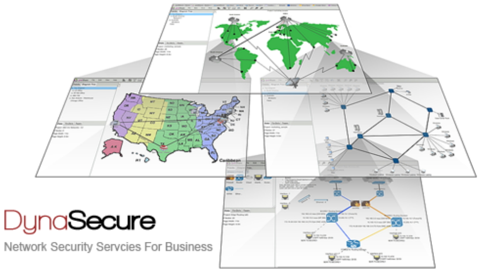
Delivering The Now Generation

Contact Us For More Information Today:
(877) 400-9490

DynaSecure

DynaSecure At-A-Glance:

- Cloud-based next-generation security infrastructure helps minimize the operational burden associated with protecting remote networks and mobile users.
- A shared ownership model lets you focus on managing your next-generation security policies for remote networks and mobile users while WAN Dynamics manages the security infrastructure.
- Based on our entire suite of security features, DynaSecure cloud security service provides an alternative approach for protecting your distributed network from advanced cyberattacks.
- Reduced operational burden enables you to move your remote location and mobile user security expenditures to a more predictable and cost saving OPEX model.



WAN DYNAMICS

WAN Dynamics is an industry leader in helping businesses navigate & effectively leverage now-generation enterprise networking technologies, including SD-WAN, SDN, SaaS and cloud-first voice and data communications. Visit us online today at www.wandynamics.com or give us a call for more information!

DynaSecure utilizes fully managed network based firewalls that are capable of providing network security protection for large or complex deployments.

DynaSecure from WAN Dynamics allows you to extend the prevention philosophy for your corporate network to your remote networks, safely enabling commonly used applications and web access.

Remote networks are connected to trusted services such as Palo Alto GlobalProtect and Zscaler Internet Security via an industry-standard IPsec VPN-capable device or SD-WAN fabric.

DynaSecure cloud security services, fully engineered, deplored and managed by WAN Dynamics, takes advantage of these full suites of next-generation security platform features.

Safely Enable Network Activity

Knowledge combined with enforcement is a powerful security tool. DynaSecure cloud security service gives you complete visibility into all applications in use at remote networks and by mobile users, as well as the content within and the user. Armed with this knowledge, you can globally deploy a more consistent security policy to protect your network from known and unknown attacks.

Reduce the Attack Surface

Using the application identity as a means of enforcing a positive security model reduces the attack surface by enabling only allowed applications and denying all else. You can align application usage to business needs, control application functions, and stop threats from accessing and moving laterally within your network.

Prevent Known Threats

Applying application-specific threat prevention policies to allowed application flows represents a key step in adhering to a prevention philosophy. Application-specific threat prevention policies can block known threats, including vulnerability exploits, malware and malware-generated command-and-control traffic.

Prevent Unknown Threats

Unknown and potentially malicious files are analyzed based on hundreds of behaviors. If a file is deemed malicious, a prevention mechanism is delivered in as little as five minutes. Once the prevention technique has been delivered, the information gained from file analysis is used to