Barracuda
Your journey, secured.

Barracuda CloudGen Access

How Barracuda CloudGen Access can protect you from ransomware.

There is a ransomware victim every 11 seconds. Today's ransomware attacks often start with credential harvesting whether through phishing or acquiring it from the dark web. Once the attacker has fraudulent credentials, they often have access to everything on your network - unless you have granular network and application access controls in place. The next step is usually achieved by scanning and accessing the network using technologies like Virtual Private Network (VPN), Remote Desktop Protocol (RDP) and Secure Socket Shell (SSH). It is critically important to protect against these remote access infiltrations.

Exploiting Remote Access

With stolen or illegally purchased credentials, an attacker can virtually become an authorized individual with access to everything that person has rights to. They can easily access your network and find relevant data to steal and then encrypt important data to demand a ransom. If such an attack occurs, your organization can lose access to their business-critical data and may be forced to pay the ransom and pay even more money to prevent stolen data from being publicly exposed.

Protecting your organization from ransomware.

Barracuda CloudGen Access disrupts the attacker's pathway to the internal network by removing easily discoverable VPN concentrators from the organizational attack surface as well as hardening other remote access tooling such as SSH and RDP by making them invisible to unauthorized users. This strategy effectively eliminates the attacker's ability to run a reconnaissance campaign to discover remote access endpoints which can greatly reduce or even remove the possibility of using compromised credentials to access your internal servers, workloads and data.

Ensure conditional, application-specific access

With CloudGen Access, even authenticated users won't be able to scan or sweep the internal network since they will only be able to observe apps and servers that are explicitly granted access to. Even in the scenario where the attacker physically compromises the endpoint and has access to the user's credentials, they won't be able to laterally move within the network and their access will be limited to what that particular user is able to access.

Prevent access from rogue devices

CloudGen Access requires a valid and cryptographically secure device certificate to identify a valid device before the user is able to authenticate on your network. These certificates enable the concept of device identity and require the combination of user and device identity to be paired for remote users or even machines to be able to access your internal resources. A rogue attacker with just the user credentials will not be able to be authorized by CloudGen Access, and attempts to authenticate as the compromised user will be denied. The secure device certificates are stored in the devices' TPM or SEP modules to make it near impossible to extract, copy or clone them.

Gain full visibility

CloudGen Access can help you gain valuable insights and full visibility into your enterprise resource access flows to mitigate security and compliance risks. It's easy to create a clear system of record, delivering reports of system access across your organization. You can manage, track, and verify the who, what, and when of privileged access in just one product.

Prevent lateral movement

CloudGen Access connects users and devices to specific applications they are explicitly authorized to use without giving them full access to the entire network. This blocks a potential attacker from gaining access to their target data sources and other assets.

Conclusion

Ransomware attacks continue to evolve, becoming more complex every day. No organization can ever be fully protected from ransomware by a single layer of security. That's why a defense-in-depth strategy is best for protecting against ransomware attacks. Barracuda can help you build a winning strategy against ransomware, providing solutions that help your organization detect, prevent, and recover from ransomware attacks.

Barracuda
Your journey, secured.

SOLUTION BRIEF • US 1.0 • Copyright 2021 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com