White Paper

Trustgrid Remote Access for Banking

Quick, Secure, Access to Sensitive Applications

Banks and credit unions must secure some of the most important data in the world. As financial institution employees have begun connecting to their work applications from a variety of locations and devices, the need to evolve security around these environments has grown. And while security is the top priority, it is closely followed by the need to ensure business continuity and productivity.

The applications serving a typical banking organization live in both the cloud and bank controlled data centers. The network is now borderless and while tools such as VPN have served as the primary way to access applications in the data center, they no longer serve the purpose of modern IT architectures that mix in public and private cloud applications.

With more than 80% of web traffic now consisting of cloud services, a new connectivity approach is needed. Trustgrid's Remote Access delivers Zero Trust network access to users that need to access applications in hybrid cloud environments quickly and securely.

Zero Trust Network Access

As the security paradigm has shifted from a static network perimeter to one focused on the resource or device requiring access, Zero Trust network access (ZTNA) has emerged as the most secure and future proof way to do this.

ZTNA solves the challenges of remote user connectivity by creating identity-centric micro-perimeters around each user and device. These perimeters are created according to the individual user and application and governed by a bank or credit union's security policy.

ZTNA applies the concept of least-privileged access to all applications to ensure that users get exactly the access they need, and no more.

Trustgrid Remote Access applies the principles of Zero Trust through an elegant agentless deployment that gives access to private applications without the need for an agent on an employee's device.

Trustgrid Remote Access

Trustgrid's Agentless Remote Access is the easiest way to deliver Zero Trust network access to any application, user or device.

As either a replacement or supplement to existing VPNs, it allows for any user to connect to private applications (hosted in the cloud or data center) without requiring layers of security appliances, device agents and weeks of configuration.

Remote Access Is The Easiest Way To:

- Allow banking employees to securely work from home
- Enable any device to access private applications
- Provide a single interface to connect to anything
- Monitor and log all application access
- Integrate network access to security solutions
- Eliminate the need for expensive VPN hardware

Users connect directly to applications through a single web-based portal that authenticates and authorizes sessions based on a user's identity and associated policies. Deployments can be done quickly and complex configurations are virtually eliminated.

As a cloud-delivered service it is continuously improving without the need for manual updates, making it easy for networking teams to manage.

For More Information Visit **www.trustgrid.io**

Trustgrid Remote Access versus VPN

Trustgrid Remote Access can be used as either a supplement or replacement to legacy VPN deployments. While there are many similarities, the differences between these two technologies are numerous.

Apply Least Privileged Access to Applications

Zero Trust network access spins up a new connection between a user and application for each session. Compared to VPN's perimeter-based access that can enable lateral movement inside of a corporate network, this direct connection limits the access to a single application and nothing more. This micro-segmentation limits the blast radius of a breach should a compromised user gain access to an application.

Increased Security and Compliance

VPNs have limited visibility into what users are able to access. From a security perspective, this lack of logging results in potential compliance gaps and presents a big security gap. From the Trustgrid management portal user sessions can be monitored in real-time, activity is centrally logged for reporting and metadata from sessions can be streamed to a 3rd party security solution. When suspicious activity is detected all active sessions can be terminated with the touch of a button.

Hide the Corporate Network

VPNs rely on the public IP addresses of applications and networks. The exposure of these IP addresses provides a target for malicious actors to attack. Trustgrid Remote Access removes the need for public facing IP addresses by only revealing addresses upon a user's authentication. With IP addresses hidden, there is one less attack vector exposed.

Align Access to Identity and Device Context

Everyone knows that identity is key to IT security. But when it comes to applying this to the network, VPNs only loosely leverage this tool. Trustgrid Remote Access applies a Zero Trust methodology by tightly integrating with an identity provider. This alignment allows for groups, roles and individual access policies to be applied at a granular level.

Increase the Speed and Reliability of Connections

VPNs can be slow due to hardware limitations or when they are tunnelling traffic through a centralized data center that does not house the resource a user needs to access. They don't enable continuous connectivity and create connections that aren't always stable, hindering employee productivity. Disconnects, which force timeouts, cause employee frustration and cost organizations both time and money. Trustgrid Remote Access provides a single, user-tailored portal that abstracts all of these problems from the user and makes access smooth, secure and speedy.

Eliminate Configuration and Deployment Complexity

Deploying and managing VPN clients on end user devices can be difficult when administrators don't have access to end user devices. With the rise of remote hiring and BYOD, access to remote devices can add days or weeks to deployment times. Trustgrid Remote Access eliminates this by using an agentless approach. By eliminating device agents, users are able to securely access private applications from any device without administrators first having access to the device.

For More Information Visit **www.trustgrid.io**

The Benefits of Trustgrid Remote Access

Quickly Add and Remove Access	Provision access to new applications in hours or users in minutes with SaaS-like connectivity that is handled through a centralized cloud control panel.
Ensure Access to All Environments	Trustgrid Remote Access supports applications across the data center, private clouds or public clouds (AWS, Azure, Google and Oracle) with intelligent routing that removes the need for backhauling traffic to the data center before reaching cloud applications.
Increase Security and Compliance	Automate and simplify the FFIEC compliance process. The cloud-delivered management portal logs all activity and controls exactly which users and locations can access applications and monitors activity in real time.
Define and Enforce Granular Policies	Through its tight integration with popular identity providers such as Azure AD, Google and Okta, policy-based network segments are built to align with corporate security controls.
Deliver A Cloud-Like User Experience	Give on-premise employees, remote employees and contractors a consistent user experience when accessing any application.
Eliminate Device Agent Hassles	Patches, updates and device configurations become a thing of the past as the cloud-delivered portal provides simplicity from the administrator to the end user.
Accelerate and Simplify M&As	Support multiple identity providers concurrently without the need to integrate legacy equipment such as firewalls and routers.

888.308.8995
info@trustgrid.io

For More Information Visit **www.trustgrid.io**