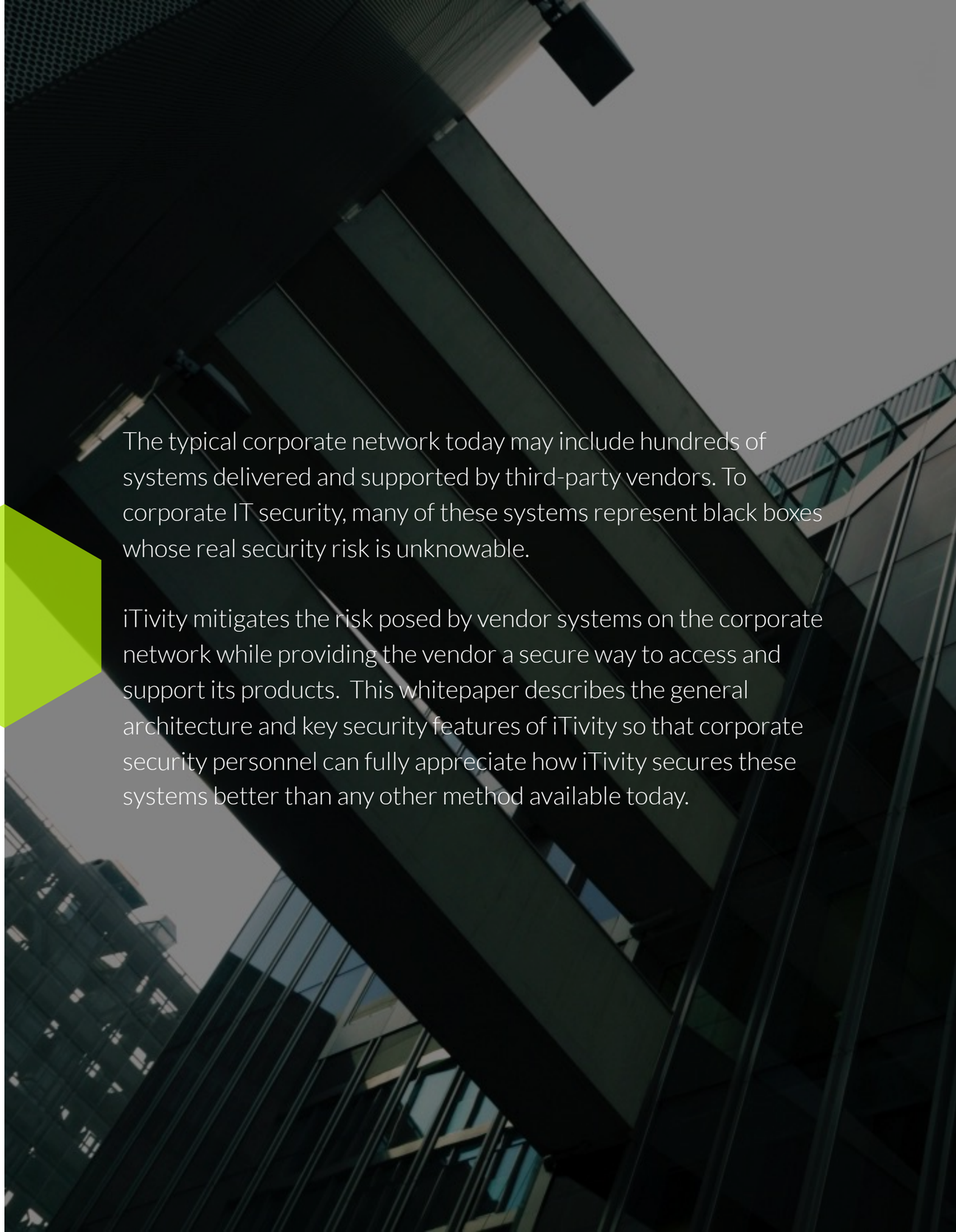
iTivity™

Serious security simplified.

Quarantined:

How iTivity Secures Vendor Systems



The typical corporate network today may include hundreds of systems delivered and supported by third-party vendors. To corporate IT security, many of these systems represent black boxes whose real security risk is unknowable.

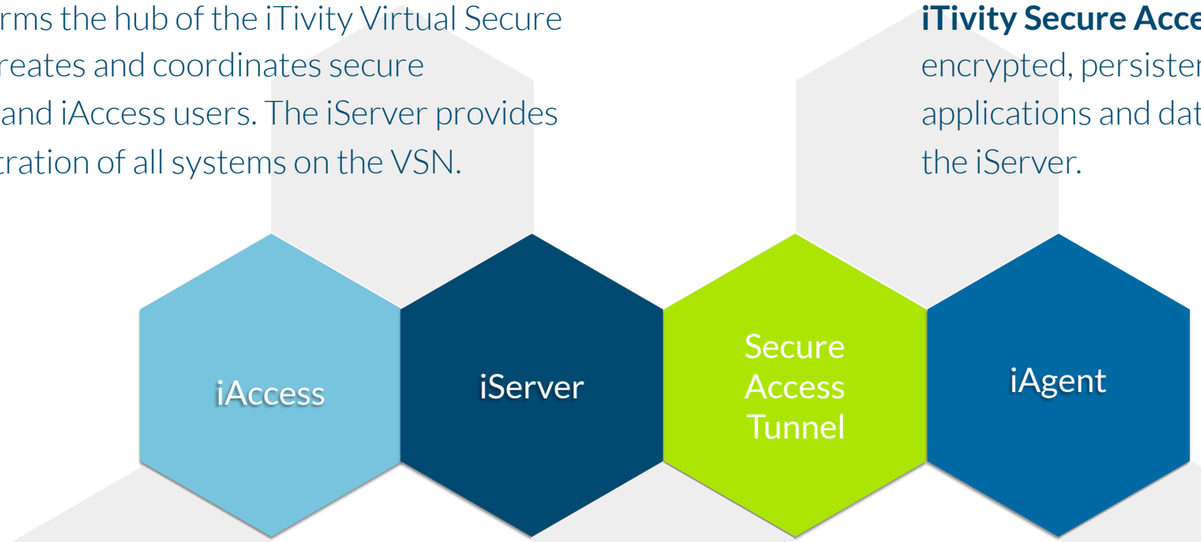
iTivity mitigates the risk posed by vendor systems on the corporate network while providing the vendor a secure way to access and support its products. This whitepaper describes the general architecture and key security features of iTivity so that corporate security personnel can fully appreciate how iTivity secures these systems better than any other method available today.

Architecture:

Primary components of the iTivity Virtual Secure Network

iServer: The iServer forms the hub of the iTivity Virtual Secure Network. The iServer creates and coordinates secure connections to iAgents and iAccess users. The iServer provides for centralized administration of all systems on the VSN.

iTivity Secure Access Tunnel (iSAT): The iSAT is an encrypted, persistent tunnel for the transport of all applications and data into and out of a given system and the iServer.



iAccess: iAccess connects authorized users to the iServer and provides a single of point of access to all systems available to the user.

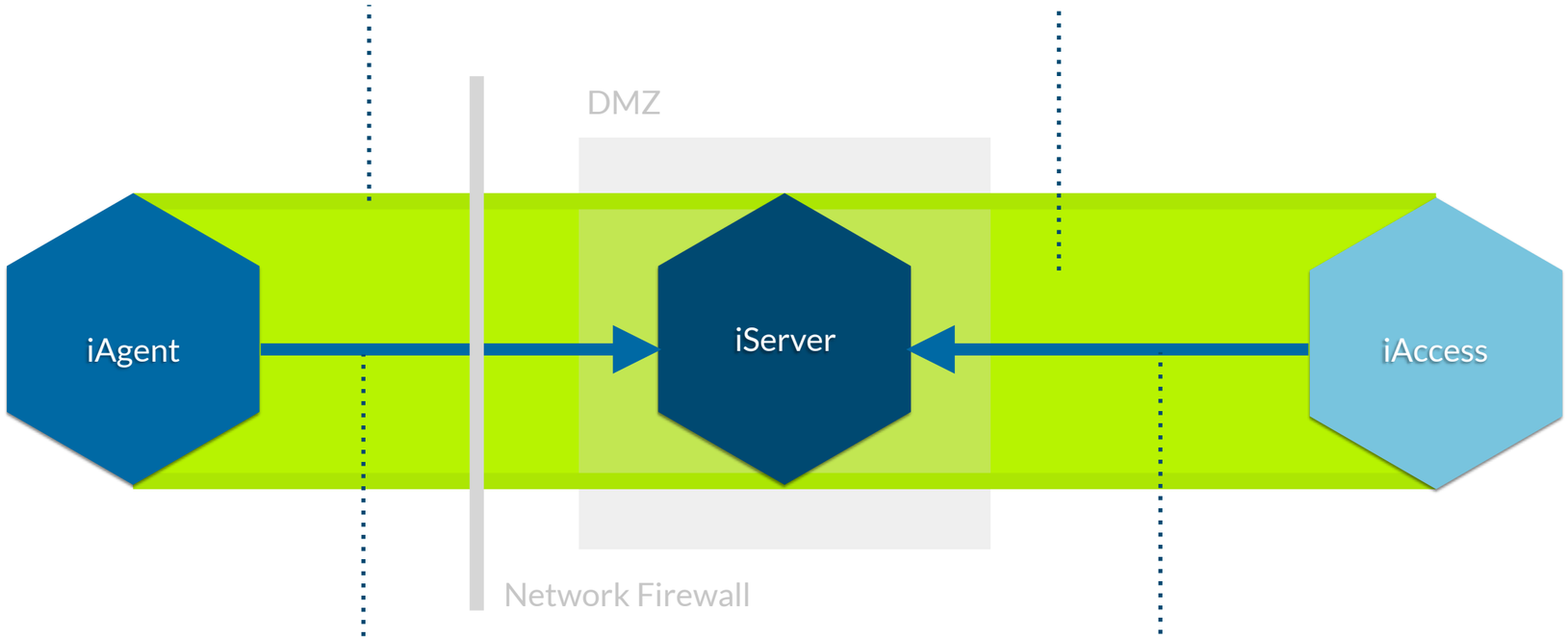
iAgent: The iAgent is a lightweight software agent that installs on the targeted system. The iAgent initiates the iSAT connection by making a request to the iServer.

iTivity Secure Access Tunnel:

An encrypted, persistent tunnel for transporting all data and applications

Encryption: All connections between iTivity components are encrypted at all times, beginning with the iAgent's initial request to the iServer. iTivity uses 2048 bit RSA asymmetric key exchange and AES encryption with 256 bit bulk/session/symmetric keys.

Proprietary protocol: The iTivity Secure Access Tunnel (iSAT) is established using a proprietary protocol. The iSAT originates with the iAgent's outbound connection to the iServer. The iServer then extends the iSAT to users working in iAccess.



HTTPS: By default, iTivity sends data utilizing secure HTTP over outbound port 23800. All inbound ports remain closed rendering the system invisible to hackers.

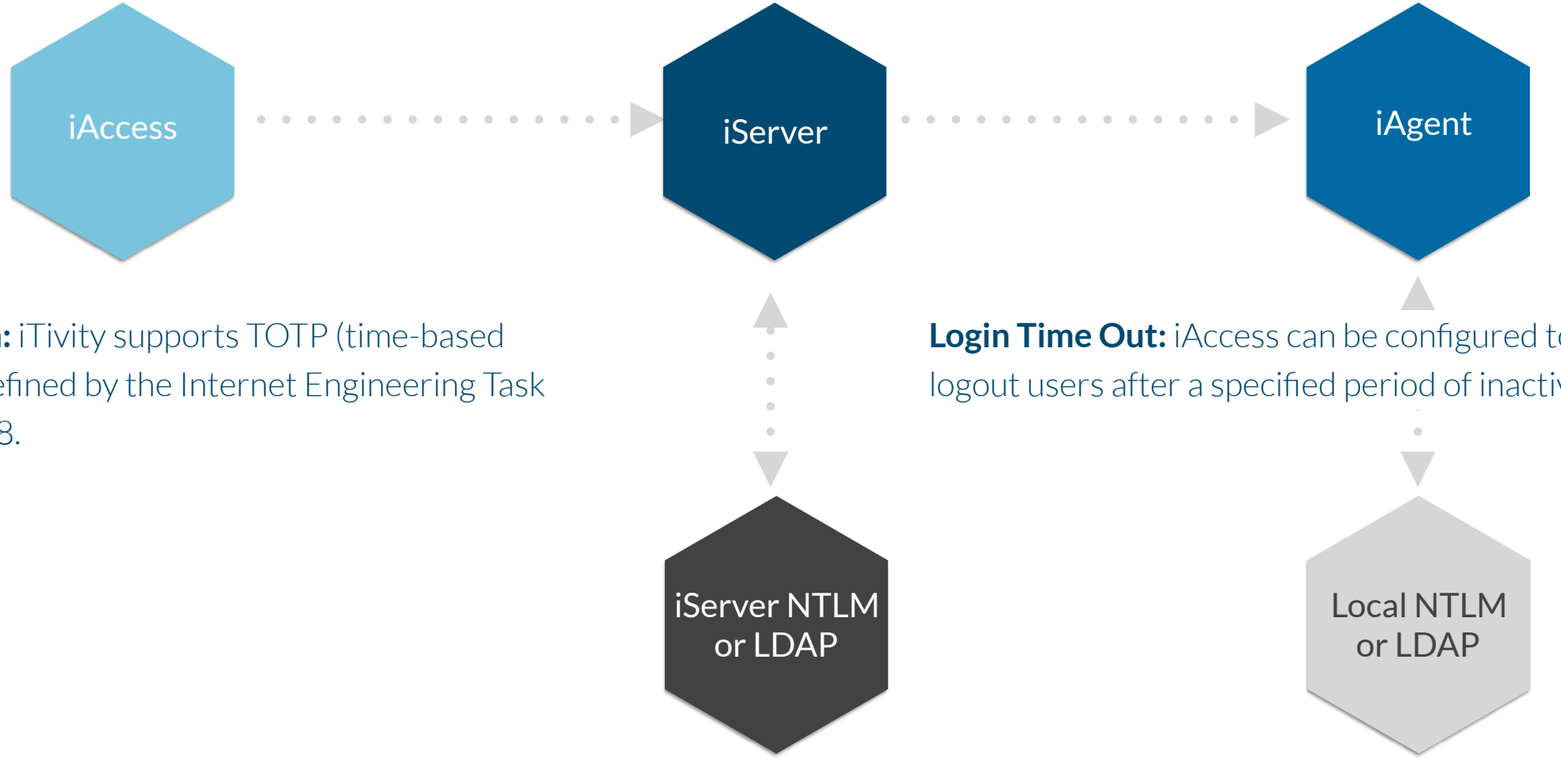
Tunneled applications: iTivity redirects all applications (including RDP, SSH, FTP, Webmin, etc.) through the iSAT. Once redirected, applications are only accessible from the iServer.

Access Management:

Centralized control of privileged user access

iServer Authentication: iAccess users must authenticate against an iServer in order to reach any iAgent. The iServer integrates with both LDAP authentication systems (including Microsoft Active Directory) and NTLM authentication systems.

Local System Authentication: By default, iTivity requires users to authenticate to the local system. iTivity recommends using a centralized LDAP or NTLM server, although any method employed by the local system will work.



2 Factor Authentication: iTivity supports TOTP (time-based one-time password) as defined by the Internet Engineering Task Force standard RFC 6238.

Login Time Out: iAccess can be configured to automatically logout users after a specified period of inactivity.

Security Monitoring:

Pipe relevant security data to your SEIM or SOC.

Activity Monitoring: The iAgent can be set to monitor system and user activity such as login attempts, application start-up, copying files, installing files, CPU utilization and more — making iTivity an effective defense against ransomeware attacks and other malware attacks as well as direct, brute-force attacks.

iTivity Logging: iTivity logs all iAgent activity on the iServer. By storing activity logs off the end-point system, they cannot be altered by the hacker to hide an attack.

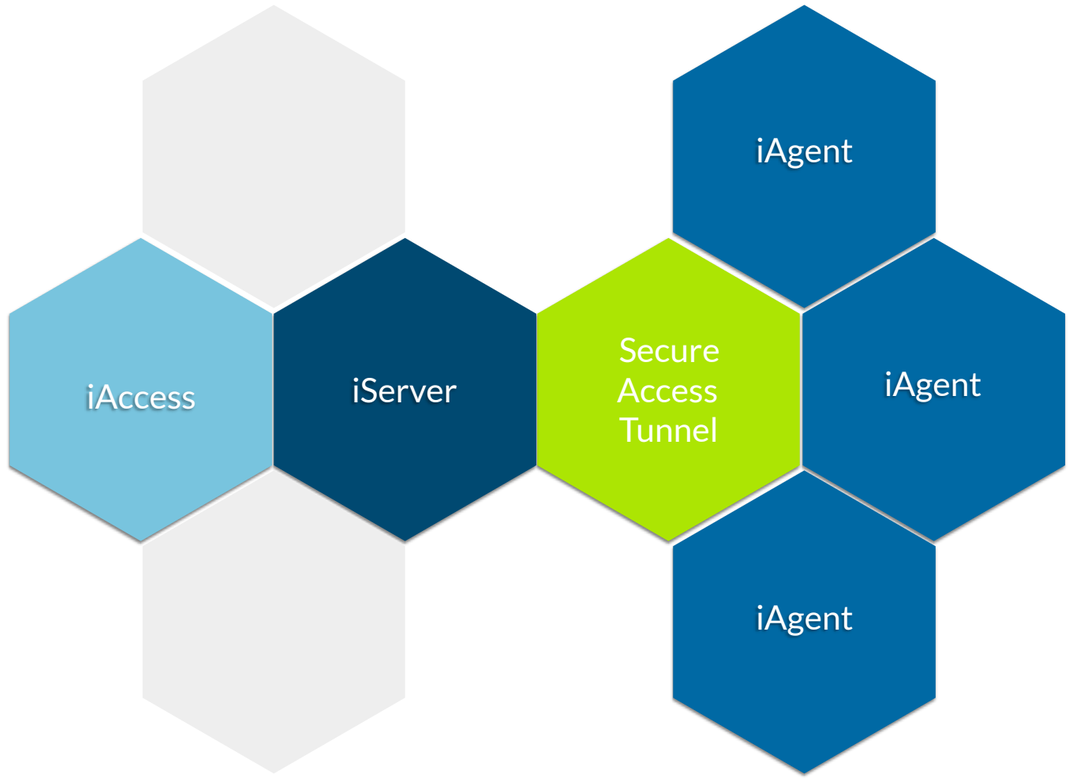
SEIM Integration: iServer log files can be mapped to leading Security Event Information Management Systems from Splunk, McFee, IBM etc as well as Security Operations Centers. Integrating security systems with iTivity allows the organization to capture data on all of its vendor systems with a single point of integration.

Virtual Secure Network:

Connect thousands of devices to create a secure, parallel network.

Simplified Network Segmentation: The iServer allows for iAgents to be grouped into logical network segments. Similarly, iAccess users can be grouped into logical workgroups. By assigning segments to workgroups, organizations can easily control internal and third-party access to specific virtual network segments.

More secure than any VPN: Unlike SSL VPNs, iTivity requires no inbound ports to be open and listening which can be scanned and attacked from outside.



iTivity Corporation
3060 Royal Boulevard South, Alpharetta, GA 30022
770-428-5000
www.iTivity.net