

MULTI-LAYERED SECURITY & CONTROLS

For Superior Data Protection



Secure Virtual Desktops

Dizzion helps companies eliminate the expense and frustration of traditional hardware management by offering a scalable, fully-managed virtual desktop environment for end users. This includes quick spin-up, virtualization software, patching and updates, security, bandwidth, and reporting and monitoring as a predictable monthly operating cost.

Dizzion's high-performance virtual desktops not only provide the fastest end-user experience, our solution is also customizable for businesses with stringent security and compliance needs.

Multiple Layers of Built-In Security

Dizzion takes a comprehensive approach to security and controls to specifically address each layer of the cloud delivered desktop. From the user and his/her endpoint devices, all the way to the physical data center infrastructure, security has been built in using a combination of virtual technologies, hardware and customizable user controls.

Dizzion also offers PCI and HIPAA HITECH compliant desktop environments, helping regulated organizations more easily achieve and maintain compliance.

User Controls

Dizzion's cloud delivered desktops enable organizations to restrict access and capabilities using more than 100 available control attributes. Controls can be customized per user, according to groups using Group Policy Objects and other methods. Commonly implemented controls include:

- Restrict user administrative rights
- Deny printing (local, network, screen)
- File and folder redirection
- Disable USB access to peripheral devices
- Clipboard redirection
- Turn off copy and paste completely

To understand our multi-layered approach to security and controls, view the chart on the following pages.

Key Benefits

Secure the Endpoint

Protect against device theft or loss and control where data resides by getting it off the endpoint.

Protect Sensitive or Proprietary Data

Control or restrict specific behaviors to ensure users can access only what they need.

Seamless Integration with Existing App Infrastructure

No need for duplicate authentication systems or to require users to manage multiple logins and passwords.

Eliminate Network Vulnerabilities

Highly redundant, highly available network security configuration including HA firewalls and load balancers, front-side/back-side network isolation, VLAN and IP address, isolation and customer-specific security configurations.

Reduce Device & OS Maintenance

Hardened OS results in greater security and control while enterprise-grade antimalware, rigorous patching and updates, and golden image management ease traditional IT burdens.

BENEFITS OF MULTIPLE SECURITY LAYERS

| SECURITY LEVEL | FEATURES | BENEFIT |
|------------------|---|---|
| User | More than 100 user control attributes available to restrict access to users and Group Policy Objects | Control what users are able to do and what they are able to access. |
| Endpoint Device | Data Residency Management – file/folder redirection, allow/disallow access to endpoint file system, allow/disallow data storage Peripheral Management – allow/disallow local or network printing, mass storage device access, screen capture, etc. | Remove corporate data and IP from endpoint devices by using cloud delivered desktops in tandem with thin/zero clients or Dizzion zLink. |
| Endpoint Session | GPO Controls (user group policy support, computer group policy support) Session Management with statistics and connection real-time health display 256 bit TLS encrypted end user connection (optional) Customer Managed User Authentication; Dual Factor Authentication and Single Sign-on (optional) Dedicated Connection Broker and Security Gateway per customer/environment Softphone/SIP telephony integration Video playback support | User experience is greatly enhanced with an TLS-encrypted tunnel that ensures secure content access without impacting performance. Support for SSO, MDM, softphone integration and video provide a robust end user computing experience. |

Security holistically within Dizzion is one of the things that sets us apart. We put our mind's eye on security out of the gate, and designed our system to be very secure.

*- Rob Green
Chief Technology Officer Dizzion*

MULTI-LAYERED SECURITY & CONTROLS

For Superior Data Protection



BENEFITS OF MULTIPLE SECURITY LAYERS

| SECURITY LEVEL | FEATURES | BENEFIT |
|-----------------------------|---|---|
| OS & Application | <p>Antimalware including antivirus protection, virtual patching, virtual firewall, IDP, web application protection, integrity monitoring, application controls, and log inspection (some features optional)</p> <p>Monitoring & Reporting</p> <p>Golden image OS support</p> <p>Administrative privilege management</p> <p>Persistent & non-persistent desktop support</p> <p>Rapid automated re-imaging</p> <p>Data backup/retention (2 weeks)</p> <p>Monitoring and Reporting 24x7x365</p> <p>Self-healing and automated problem remediation</p> <p>Dedicated VMware ESX server virtualization per customer/environment</p> | <p>Greater control is achieved through a hardened OS and enterprise-grade antimalware.</p> <p>Managed patching and updates in addition to golden image management save IT time and resources.</p> |
| Network | <p>Redundant 1, 10 and 40Gbps Network to ensure maximum end user performance</p> <p>High availability physical firewalls</p> <p>Dedicated private IP Addressing per customer/environment</p> <p>Dedicated VLAN per customer/environment</p> <p>High availability dedicated virtual firewalls</p> | <p>Highly available, fully redundant network connectivity ensures users can be fully productive.</p> |
| Physical | <p>Physical data center security & redundant infrastructure</p> <p>PCI-DSS & HIPAA HITECH Physical Security Certification</p> | <p>Audits are simplified when relying on existing PCI DSS and HIPAA physical security certifications.</p> |

Learn more at www.dizzion.com/secure