













# ContentKeeper Cloud Services

## Access Control. Threat Prevention. App Usage & Data Protection.

Securely connect users, devices, and apps, regardless of location, to protect your organization from internal and external threats. ContentKeeper's multi-layered cloud security platform delivers security as a service, enabling secure cloud access to enterprise resources in a distributed user environment. With ContentKeeper Secure Cloud Gateway, organizations can easily scale protection and seamlessly transition towards a SASE future.

### ContentKeeper Secure Cloud Gateway Innovative Approach to Cloud Security

Access Control	Threat Prevention	App Usage & Data Protection
 <b>Firewall as a Service (FWaaS)</b> Increase network visibility and control access across all ports and protocols.	 <b>SSL Inspection</b> Find hidden threats with granular and selective inspection of SSL traffic at scale.	 <b>Analytics/Reporting</b> Provide real-time visibility, in-depth analytics, and comprehensive reporting of cloud application usage.
 <b>URL Filtering</b> Ensure policy compliance, productivity and safety with category and policy-based management.	 <b>Streaming Malware Defense</b> Block known malware threats using high speed scanning technology and streaming malware intelligent feeds from Bitdefender.	 <b>Microsoft® CASB Integration</b> Enforce compliance and better manage cloud application use with centralized visibility and reporting.
 <b>DNS Filtering</b> Control and block access to known malicious sites for managed and non-managed devices in the cloud.	 <b>Predictive Malware Blocking (Powered by Cylance)</b> Extend threat protection with artificial intelligence and machine learning to identify, predict, and block unknown targeted threats.	 <b>SIEM Integration</b> Ensure efficient incident response and compliance with consolidated analytics-driven reporting.
 <b>Zero Trust Network Access (ZTNA)</b> Eliminate security gaps by providing role and policy-based access to web content, cloud, and private Internet apps and resources.	 <b>Cloud Sandbox</b> Block zero-day attacks by analyzing suspicious files for malicious behavior with reverse engineering and forensic level reporting.	 <b>Cloud DLP</b> Control DLP across users while ensuring productivity, by blocking actions only when needed with pre-defined policy dictionaries.