**ASSIGNMENT**

# 1. Research about the various cyber security frameworks and how they work.

Cybersecurity frameworks are structured guidelines, best practices, and standards that help organizations manage and mitigate cybersecurity risks. They provide a systematic approach to safeguarding information systems and data from cyber threats. Below is an overview of several prominent cybersecurity frameworks and their functionalities:

## i. NIST Cybersecurity Framework (CSF)

Developed by the National Institute of Standards and Technology (NIST), the CSF offers a voluntary, risk-based approach to managing cybersecurity activities. It is organized into five core functions:

* **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
* **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.
* **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
* **Respond:** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
* **Recover:** Develop and implement appropriate activities to maintain resilience and restore any capabilities or services impaired due to a cybersecurity incident.

These functions provide a strategic view of managing cybersecurity risks and are further detailed in the NIST Cybersecurity Framework documentation.

<https://www.nist.gov/cyberframework>

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf?>

## ii. ISO/IEC 27001

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly developed the ISO/IEC 27001 standard. It specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). The standard emphasizes a risk management process, including people, processes, and IT

systems, by applying a comprehensive set of security controls. The latest version, ISO/IEC 27001:2022, organizes 93 controls into four groups:

* **A.5:** Organizational controls
* **A.6:** People controls
* **A.7:** Physical controls
* **A.8:** Technological controls

These controls cover various aspects of information security, including governance, asset management, and access control.

<https://en.wikipedia.org/wiki/Security_controls?>

## iii. CIS Critical Security Controls (CIS Controls)

The Center for Internet Security (CIS) provides a set of 18 critical security controls designed to help organizations improve their cybersecurity posture. These controls are prioritized and focus on key areas such as:

* Inventory and Control of Enterprise Assets
* Secure Configuration of Enterprise Assets and Software
* Continuous Vulnerability Management
* Security Awareness and Skills Training

Implementing these controls helps organizations defend against common cyber threats and establish a solid foundation for cybersecurity practices.

<https://en.wikipedia.org/wiki/Security_controls?>

## iv. COBIT (Control Objectives for Information and Related Technologies)

Developed by ISACA, COBIT is a framework for developing, implementing, monitoring, and improving IT governance and management practices. It provides a comprehensive model to help organizations achieve their objectives for the governance and management of enterprise IT. COBIT 5, for instance, includes processes such as:

* Evaluate, Direct, and Monitor (EDM)
* Align, Plan, and Organize (APO)
* Build, Acquire, and Implement (BAI)
* Deliver, Service, and Support (DSS)
* Monitor, Evaluate, and Assess (MEA)

These processes ensure effective decision-making and strategic alignment between IT and business goals.

<https://en.wikipedia.org/wiki/Security_controls?>

## v. NERC Critical Infrastructure Protection (CIP)

The North American Electric Reliability Corporation (NERC) developed the CIP standards to protect the cybersecurity of critical assets within the bulk power system. The standards focus on areas such as:

* Asset Identification
* Electronic Security Perimeters
* Personnel Training
* Incident Response
* Recovery Planning

Compliance with NERC CIP standards is mandatory for power system operators and owners under NERC’s jurisdiction, with enforcement overseen by the Federal Energy Regulatory Commission (FERC) in the United States.

<https://en.wikipedia.org/wiki/Information_security_standards?>

## By adopting and implementing these frameworks, organizations can establish robust cybersecurity practices tailored to their specific needs and regulatory environments. Vi.SOC2

[Service Organization Control (SOC) Type 2](https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html) is a trust-based cybersecurity framework and auditing standard developed by the American Institute of Certified Public Accountants (AICPA) to help verify that vendors and partners are securely managing client data.

SOC2 specifies more than 60 compliance requirements and extensive auditing processes for third-party systems and controls. Audits can take a year to complete. At that point, a report is issued which attests to a vendors’ [cybersecurity posture](https://www.bitsight.com/blog/how-and-when-to-reassess-your-vendors-cybersecurity-posture).

Because of its comprehensiveness, SOC2 is one of the toughest security frameworks to implement — especially for organizations in the finance or banking sector who face a higher standard for compliance than other sectors.

Nevertheless, it’s an important security framework that should be central to any [third-party risk management](https://www.bitsight.com/blog/ultimate-guide-tprm-what-third-party-risk-management) program.  
[https://en.wikipedia.org/wiki/Service\_Organization\_control?](https://en.wikipedia.org/wiki/Information_security_standards?)  
  
 **HIPAA (Health Insurance Portability and Accountability Act)**

* **Overview**: HIPAA is a U.S. regulation that mandates healthcare organizations to implement security controls to protect the privacy and security of electronic health information (ePHI).
* **Key Requirements**:
  + Conduct risk assessments to identify vulnerabilities.
  + Implement training programs for employees.
  + Enforce administrative, technical, and physical safeguards.
* **Challenges**: Many healthcare providers face difficulties in staying compliant due to rapidly changing technology and evolving threats.
* **Usage**: Essential for U.S. healthcare providers, insurers, and their business associates.  
    
  [https://en.wikipedia.org/wiki/](https://en.wikipedia.org/wiki/Information_security_standards?)Health\_Insurance\_Portability\_and\_Accountability\_Act[?](https://en.wikipedia.org/wiki/Information_security_standards?)

### **GDPR (General Data Protection Regulation)**

* Overview: GDPR is a European Union regulation designed to strengthen data protection and privacy for EU citizens. It impacts any organization processing the personal data of EU residents, regardless of location.
* Key Features:
  + Includes 99 articles covering data access rights, breach notifications, and data processing guidelines.
  + Requires businesses to notify regulators within 72 hours of a breach.
  + Enforcement includes fines of up to €20 million or 4% of annual global revenue.
* Challenges: Non-compliance can result in severe penalties and reputational damage.
* Usage: Relevant for organizations worldwide handling EU citizen data, ensuring data protection practices align with GDPR mandates.  
    
  https://en.wikipedia.org/wiki/General\_Data\_Protection\_Regulation

### **FISMA (Federal Information Security Management Act)**

* Overview: FISMA provides a framework for protecting federal government systems and extends to contractors and third parties working on behalf of federal agencies.
* Key Requirements:
  + Maintain an inventory of digital assets and identify system integrations.
  + Categorize data based on sensitivity and apply appropriate security controls.
  + Conduct annual security reviews, risk assessments, and continuous monitoring.
* Alignment: Closely tied to NIST standards, including NIST 800 guidelines.
* Usage: Vital for federal agencies and their contractors to ensure robust security practices  
  .  
  https://en.wikipedia.org/wiki/Federal\_Information\_Security\_Management\_Act\_of\_2002

### **MITRE ATT&CK Framework**

* Overview: A globally accessible knowledge base of adversary tactics, techniques, and procedures (TTPs).
* Key Features:
  + Maps the lifecycle of cyberattacks to identify and mitigate vulnerabilities.
  + Helps in threat hunting, incident response, and red/blue team exercises.
* Usage: Widely adopted for enhancing threat intelligence and improving defense mechanisms.

### **Zero Trust Framework**

* Overview: Zero Trust operates on the principle of “never trust, always verify.” It assumes all network traffic is potentially malicious.
* Key Features:
  + Enforces strict access controls based on user identity and device posture.
  + Leverages technologies like micro-segmentation and multi-factor authentication (MFA).
  + Emphasizes continuous monitoring and validation.
* Usage: Particularly effective in cloud environments and for remote work scenarios.

### **PCI DSS (Payment Card Industry Data Security Standard)**

* **Overview**: Designed to protect payment card data during transactions.
* **Key Features**:
  + Includes 12 requirements, such as secure network systems, vulnerability management, and encryption.
  + Mandates regular monitoring and testing of networks.
* **Usage**: Mandatory for merchants and service providers handling cardholder data.

https://en.wikipedia.org/wiki/Payment\_Card\_Industry\_Data\_Security\_Standard

# 2. Research and look further at other Network Protocols being used.

Network protocols are essential rules and conventions that enable communication between devices over a network. They ensure data is transmitted accurately and securely across diverse systems. Beyond the commonly known protocols like TCP/IP, HTTP, and FTP, several other protocols play crucial roles in network operations:

## i. Internet Control Message Protocol (ICMP)

ICMP is used by network devices to send error messages and operational information, such as indicating that a requested service is not available or that a host/router could not be reached. It's fundamental for diagnostic tools like 'ping' and 'traceroute'.

<https://www.ninjaone.com/blog/types-of-network-protocols/>

## ii. Simple Network Management Protocol (SNMP)

SNMP is utilized for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. It's widely used in network management for network monitoring.

<https://www.techtarget.com/searchnetworking/feature/12-common-network-protocols-and-their-functions-explained?>

## iii. Border Gateway Protocol (BGP)

BGP is the protocol underlying the global routing system of the internet. It manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers. <https://www.techtarget.com/searchnetworking/feature/12-common-network-protocols-and-their-functions-explained?>

## iv. Dynamic Host Configuration Protocol (DHCP)

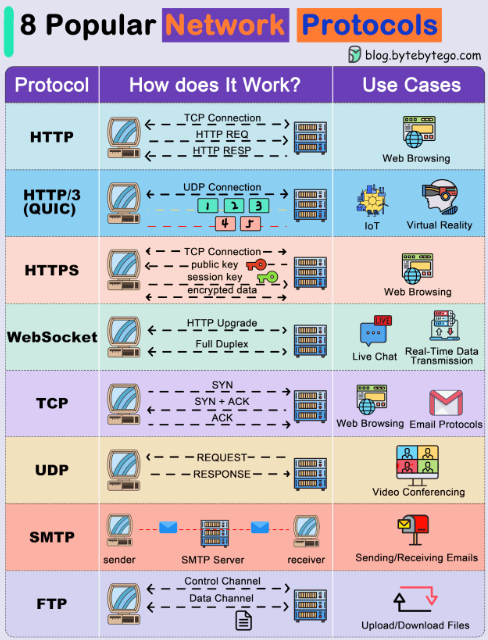
DHCP automates the assignment of IP addresses, subnet masks, gateways, and other IP parameters. This automation allows devices to join networks seamlessly without manual configuration. <https://www.techtarget.com/searchnetworking/feature/12-common-network-protocols-and-their-functions-explained?>

## v. Secure Shell (SSH)

SSH provides a secure channel over an unsecured network by using a client-server architecture, allowing for secure remote login and other secure network services. It's essential for secure data communication, remote command-line login, and remote command execution.

<https://www.auvik.com/franklyit/blog/common-network-protocols/?>

These protocols, among others, form the backbone of network communication, each serving specific functions to ensure efficient and secure data exchange across networks.  
  
vi. Domain Name System (DNS)  
Translates human-readable domain names into IP addresses, enabling browsers to locate and access websites



# 3. Do research to identify companies that provide firewall solutions, their pros and cons.

Several companies offer firewall solutions, each with distinct advantages and disadvantages. Below is an overview of some prominent providers:

## i. Fortinet

Fortinet is a leading cybersecurity company known for its AI-enabled threat detection tools and firewall solutions. The company has demonstrated significant growth, with a 67% rally in 2024.

*Pros:*

* Advanced AI-driven threat detection capabilities.
* Strong financial performance indicating stability and growth.

*Cons:*

* Specific cons are not detailed in the provided information.

<https://www.investors.com/research/ibd-stock-of-the-day/fortinet-ibd-stock-of-the-day-cybersecurity-stocks-to-watch/>

## ii. TinyWall

TinyWall is a free firewall program for Windows users, notable for operating without pop-up notifications.

*Pros:*

* User-friendly with no intrusive pop-ups.
* Lightweight and easy to configure.

*Cons:*

* May lack advanced features found in paid solutions.

<https://www.lifewire.com/free-firewall-programs-8774220?>

## iii. Comodo Firewall

Comodo Firewall offers features like virtual browsing and a game mode, providing robust protection for users.

*Pros:*

* Includes virtual browsing for safer internet use.
* Game mode prevents interruptions during gaming sessions.

*Cons:*

* May present a learning curve for less tech-savvy users.

<https://www.lifewire.com/free-firewall-programs-8774220?>

## iv. PeerBlock

PeerBlock is a free firewall program that blocks lists of IP addresses instead of individual programs, enhancing privacy.

*Pros:*

* Effective at blocking unwanted IP addresses.
* Enhances user privacy during online activities.

*Cons:*

* Requires manual updates of IP block lists.

<https://www.lifewire.com/free-firewall-programs-8774220?>

## v. ZoneAlarm Free Firewall

ZoneAlarm offers features like cloud backup, providing additional security measures for users.

*Pros:*

* Includes cloud backup for data protection.
* User-friendly interface suitable for various users.

*Cons:*

* May include ads or prompts to upgrade to premium versions.

<https://www.lifewire.com/free-firewall-programs-8774220?>

When selecting a firewall solution, it's essential to consider the specific needs of your organization or personal use, including factors like budget, required features, and the level of protection necessary.

## vi. Sangfor Network Secure Next Generation Firewall

[Sangfor's Network Secure Next Generation Firewall](https://www.sangfor.com/cybersecurity/products/network-secure-next-generation-firewall) stands out for its robust protection capabilities. Sangfor offers comprehensive security, including intrusion prevention, malware detection, and secure remote access. Sangfor’s firewall is designed to meet the needs of enterprises of all sizes, ensuring optimal performance and security.

About the Solution

Sangfor's NGFW provides cutting-edge security features, including AI-driven threat detection and automated responses. The firewall integrates seamlessly with other Sangfor security products, providing a unified security solution.

Features

* Intrusion Prevention System (IPS): Detects and blocks attempts to exploit vulnerabilities.
* Advanced Threat Protection (ATP): Utilizes machine learning to identify and mitigate sophisticated threats.
* SSL Decryption and Inspection: Inspects encrypted traffic to prevent hidden threats.

Pricing

Sangfor offers competitive pricing tailored to different enterprise needs. The cost varies depending on the deployment size and specific requirements, making it accessible for small to large businesses.

Customer Testimonials

Customers praise Sangfor for its reliability and comprehensive security features. Many appreciate the user-friendly interface and the seamless integration with other Sangfor products.

Pros and Cons

* Pros: Advanced threat protection, user-friendly interface, comprehensive security features.
* Cons: Limited presence outside of APAC & EMEA.  
    
    
   **Vii.** [NordLayer](https://nordlayer.com/features/cloud-firewall/)

NordLayer is a network security solution that offers secure access to company resources from any location. It helps protect networks, enables remote work, and provides the tools necessary to comply with key regulatory frameworks. Developed by Nord Security, the creators of NordVPN, NordLayer offers a multi-layered defense and features typical of next-generation firewalls (NGFW).

NordLayer enables organizations to implement [Firewall as a Service (FWaaS)](https://nordlayer.com/features/cloud-firewall/) along with [Zero Trust Network Access (ZTNA)](https://nordlayer.com/zero-trust/), and [Secure Web Gateway (SWG)](https://nordlayer.com/secure-web-gateway/) principles.

Five ways NordLayer Cloud Firewall can help:

* Prevent data leaks. Network segmentation is key in access control. Without it, data leaks are more likely.
* Achieve compliance. Many standards focus on network access control and protection of network and encrypted traffic.
* Implement security strategy. Best practices include secure access service edge (SASE), FWaaS, SWG, and ZTNA.
* Unify security across hybrid setups. Securing a mix of data centers, cloud, and on-premise systems can be challenging, but NordLayer helps simplify this.
* Support hybrid work models. NordLayer strengthens security for remote teams while managing network firewalls across locations.

NordLayer’s flexibility makes it ideal for businesses of all sizes that need scalable network protection. It provides [secure internet access](https://nordlayer.com/secure-internet-access/), resource protection, and [compliance with major cybersecurity regulations](https://nordlayer.com/security-compliance/).

Apart from Cloud Firewall, NordLayer offers other security features like:

* Quantum-safe encryption
* Servers with a dedicated IP
* Device Posture Security
* IP allowlisting
* Web protection (formerly ThreatBlock)
* DNS filtering
* NordLynx VPN protocol
* Browser extension for secure browsing

#### **Benefits:**

* Transparent pricing, starting at $7 per user per month
* Proactive setup support
* 24/7 live support with dedicated account managers
* Direct user feedback influences product development

#### **Drawbacks:**

* Less known compared to other competitors
* Fewer security features than large enterprise firewall vendors
* Possible slowdowns with the use of VPN
* Reducing team size requires reaching out to support

## Occasional confusion between NordVPN and NordLayer viii. Cato SASE Cloud

Cato Networks is an Israeli company that offers [Secure Access Service Edge (SASE)](https://nordlayer.com/learn/sase/what-is-sase/) technology. The platform combines communication and security in a cloud-based solution. Founded in 2015, Cato Networks now employs over 900 people globally. When it comes to the firewall, users frequently mention that the solution is easy to set up, with straightforward firewall rule management and affordability. It simplifies firewall management and offers features typical of NGFW.

#### **Most mentioned overall product benefits:**

* Comprehensive security features
* Complete management panel for easy user control
* Low-latency performance through numerous points of presence (PoPs)
* Reliable, with no impact on internet speed or application performance
* Automatic firewall updates
* Agile and scalable solution

#### **Drawbacks:**

* Can be difficult to implement
* License costs are high
* Logs and reports are hard to interpret
* VPN licenses must be purchased in packs of 10
* Sometimes the app fails to log in
* Upgrading bandwidth capacity for a site can be costly  
    
  Ix. Cloudflare WAF

Cloudflare is an American company that offers content delivery networks, cloud cybersecurity, DDoS mitigation, and domain services. As of 2024, over 19% of the internet uses it for web security. Its Web Application Firewall (WAF) features managed rulesets that are frequently updated, geolocation blocking, and proxy detection, making it highly effective in preventing man-in-the-middle attacks. Users also note its useful integrations, such as with Azure AD and Google Cloud.

#### **Most mentioned overall product benefits:**

* Easy installation
* Simple to monitor with actionable features
* Extremely effective with customizable options
* User-friendly interface
* Straightforward to use

#### **Drawbacks:**

* Hard for small businesses to negotiate pricing and add features
* Limited configurations in the Terraform provider
* Implementing network-based rules through code is difficult
* Documentation lacks specific, in-depth configurations
* Some false positives in traffic blocking, though fixable over time
* Slow customer support responses
* Limited flexibility in rate-limiting rules for APIs
* Load balancing requires an additional license

## X. Appgate SDP

Appgate, founded in 2020 and based in Coral Gables, Florida, provides security solutions for organizations and government agencies. It focuses on Universal [Zero Trust Network Access (ZTNA)](https://nordlayer.com/learn/zero-trust/what-is-ztna/) and fraud protection. As for the firewall functionality, users mention that Appgate SDP is straightforward to manage with helpful troubleshooting documentation.

#### **Most mentioned overall product benefits:**

* Stable performance
* Fast operation
* Easy to deploy and manage
* Clear documentation for troubleshooting
* Real-time updates based on risk metrics
* Micro-segmented access to resources
* Intuitive user interface

#### **Drawbacks:**

* Runs on Ubuntu Server, which is not frequently updated
* Per-site licensing increases overall costs
* Slow connection speeds to remote sites
* Occasional resource reduction despite steady internet bandwidth
* Complex to configure
* Limited log management features
* Dashboard is not very helpful for security monitoring
* Frequent need to restart due to slow connection despite good internet
* Insufficient dashboard information for identifying node connectivity issues

## Centralized management lacks efficiency Xi. WatchGuard Firewall

About the Solution

[WatchGuard](https://www.watchguard.com/wgrd-products/firewalls) provides advanced security features with a focus on ease of use. Their NGFWs are designed to be user-friendly while providing robust protection.

Features

* Advanced Persistent Threat Blocker: Detects and stops advanced threats.
* Threat Detection and Response: Provides real-time threat detection and automated responses.
* Secure [Wi-Fi:](https://www.techtarget.com/searchmobilecomputing/definition/Wi-Fi) Protects wireless networks with integrated security.

Pricing

WatchGuard offers mid-range pricing with a variety of models to suit different business needs.

Customer Testimonials

Customers value WatchGuard’s ease of use and robust security features. It is often praised for its user-friendly interface and reliable performance.

Pros and Cons

* Pros: User-friendly, reliable, comprehensive protection.
* Cons: Limited high-end features compared to some competitors.

# 

# 4. Research about the various backup tools that are being used.

There are numerous backup tools available, each catering to different needs and environments. Below is an overview of some notable backup solutions:

## i. EaseUS Todo Backup

EaseUS Todo Backup is a comprehensive backup solution that offers features such as system backup, file backup, disk imaging, and cloning. It also includes an AI smart backup feature to automate backup tasks on a schedule.

<https://www.pcworld.com/article/407021/best-windows-backup-software.html?>

## ii. Veeam Backup & Replication Community Edition

Veeam provides a free backup solution capable of securing virtual, physical, and cloud workloads. It's suitable for small businesses and home labs, offering reliable data protection and recovery options.

<https://www.veeam.com/products/free/backup-recovery.html?>

## iii. Acronis True Image

Acronis True Image is a personal backup software that allows users to store files securely in the Acronis personal cloud. It offers comprehensive backup solutions for home and office use, ensuring data protection and easy recovery.

<https://www.acronis.com/en-us/products/true-image/backup/?>

## iv. Macrium Reflect

Macrium Reflect is a disk imaging and backup utility for Microsoft Windows. It creates disk images and file backup archives using Microsoft Volume Shadow Copy Service to ensure 'point in time' data accuracy. It's known for its ease of use, speed, and robust feature set.

<https://en.wikipedia.org/wiki/Macrium_Reflect?>

## v. Syncovery

Syncovery, formerly known as Super Flexible File Synchronizer, is backup and file synchronization software that allows backing up and synchronizing files to the same or different drives, to different media, or to a remote server. It supports various Internet protocols and cloud storages, including Amazon S3, Microsoft Azure, Google Drive, and more.

<https://en.wikipedia.org/wiki/Syncovery?>

## vi. Duplicati

Duplicati is a free, open-source application that enables users to back up their computers to various cloud services, such as Microsoft OneDrive and Google Drive. It offers encryption to secure files and a web browser interface for configuration.

<https://www.wired.com/story/duplicati-free-app-back-up-your-computer-to-any-cloud-service/>

## vii. Rubrik

Rubrik simplifies data backup and recovery for virtual and physical environments. It combines data orchestration, catalog management, and storage into one platform, providing instant data backup and recovery solutions.

<https://www.rubrik.com/solutions/backup-recovery?>

When selecting a backup tool, it's essential to consider factors such as the specific needs of your environment, the types of data you need to protect, the platforms you use, and your budget. Evaluating these aspects will help determine the most suitable backup solution for your requirements.  
  
viii. **MSP360 (formerly CloudBerry Backup)**

* **Overview**: MSP360 provides backup solutions for cloud and on-premise environments, supporting major cloud providers such as AWS, Google Cloud, Microsoft Azure, and more.
* **Pros**:
  + Flexible cloud storage support and integration with various cloud platforms.
  + Advanced features like encryption, compression, and backup scheduling.
  + Cost-effective for businesses due to its pay-per-use model.
* **Cons**:
  + The initial setup can be overwhelming due to the variety of features.
  + The interface is not as intuitive as some other solutions.

### **Ix. Barracuda Backup**

* **Overview**: Barracuda Backup provides cloud-integrated solutions that offer both on-premise and offsite data protection. It is tailored for businesses of all sizes and can handle virtual environments as well as physical servers.
* **Pros**:
  + Offers hybrid backup solutions combining on-site and cloud backups.
  + Easy-to-manage centralized platform.
  + Reliable recovery process with a wide range of supported platforms.
* **Cons**:
  + Some users report that the software can be slow during backups.
  + The cloud storage options can become expensive at scale.

Xi. **Carbonite**

Carbonite mainly targets small businesses. Carbonite Endpoint 360 [protects endpoint devices](https://www.techtarget.com/searchdatabackup/news/252466803/Carbonite-Endpoint-360-protects-and-backs-up-Office-365-apps) and data stored in common SaaS applications. Users can store backup data in their organization's data center, in a Microsoft Azure Enterprise account or in Carbonite's own Azure-hosted vault.

Carbonite Backup creates backup images that can also provide DR capabilities with Carbonite Availability. Carbonite replicates data in near real time to provide recovery point objectives (RPOs) of a few minutes or even seconds. In a disaster scenario, applications fail over to Carbonite Cloud Backup through predefined runbook automation.

Organizations can deploy Carbonite Backup on a local backup server and provide protection for common OSes and Microsoft applications, including Microsoft SQL, Exchange and SharePoint, and Oracle databases. The service [replicates a backup](https://www.computerweekly.com/feature/Storage-101-Replication-vs-backup-and-synchronous-vs-asynchronous) copy to Carbonite Cloud, a proprietary public cloud storage target.

**Xii Clumio**

Clumio is a data protection startup that focuses on protecting data in the public cloud and on premises. The Clumio platform runs entirely as a service in the public cloud, [protecting native AWS services](https://www.techtarget.com/searchdatabackup/news/252474337/Clumio-extends-support-to-AWS-EBS-with-135M-funding-bump), Office 365 and VMware either in AWS or on premises.

Like similar SaaS-based offerings, Clumio scales on demand, storing encrypted backup data in its AWS accounts. This architecture provides a virtual "airgap" between primary data and backup copies, protecting organizations if their on-premises or cloud accounts are compromised by ransomware.

Clumio charges per resource protected, including virtual instance, VM and Office 365 seat.

Xiii Druva  
Druva is a data protection company based fully in the public cloud and delivered as SaaS. Organizations don't install any hardware on premises but replicate all backup data directly into the public cloud. The Druva product is best suited to businesses that have some degree of diversification, either with multiple data centers, branch offices or a mobile workforce.

The Druva Cloud Platform protects cloud-native workloads running in hyperscale environments such as AWS, Azure and Google Cloud Platform. This feature is delivered by CloudRanger, a startup acquired by Druva in June 2018. Druva Phoenix protects traditional data center applications, including virtual infrastructure, databases and physical servers. Druva InSync protects endpoint devices such as desktops, laptops, tablets and smartphones. InSync also protects SaaS-based applications, including Office 365, G Suite and Salesforce. Druva now supports Outposts, [on-premises AWS infrastructure](https://searchconvergedinfrastructure.techtarget.com/tip/AWS-Outposts-vs-Azure-Stack-vs-HCI).

The Druva platform is entirely cloud-native and built on AWS, using intrinsic cloud services such as EC2 virtual instances, Amazon Relational Database Service and S3 storage. With this approach, an organization doesn't need to deploy or manage any infrastructure. The backup service is effectively limitless, with pricing charged based on data stored.