Acronis

WHITE PAPER

Distributed vs. centralized management of cyber protection for multilocation businesses

How distributed management of cybersecurity and data protection can make your business more cyber resilient

Businesses of all sizes are struggling to protect their systems' uptime and data integrity against a welter of threats, from AI-enabled cyberattacks to hardware failures to software issues to human error. While many companies choose to centralize their IT operations and cybersecurity management, there are other use cases in which ceding some of that control to IT and cybersecurity staff located at remote sites can yield better cyber resilience.

This white paper examines the scenarios in which a business can achieve higher uptime, more effectively prevent data loss, and reduce the costs of managing and securing IT infrastructure and data by delegating some control to their regional and remote locations. It weighs the pros and cons of this approach and considers ways that businesses can achieve their compliance and governance goals without fully centralized cybersecurity and IT operations management.

Many businesses are distributed

Roughly one quarter of U.S. businesses operate out of more than one location. And while the European Union (EU) does not specifically report on businesses based on number of locations, the prevalence of retail, hospitality, medical, financial services and other business segments that tend to have multiple locations suggests multilocation businesses are a significant part of the EU economy as well. Larger enterprises are even more likely to have multiple locations, including regional offices, manufacturing plants, warehouses and distribution centers.

Companies that use mergers and acquisitions to expand within their sector, into other lines of business and to other geographical regions, are also likely to have a large number of locations that are physically remote from centralized IT and cybersecurity staff.

Examples of distributed businesses

The retail industry provides one obvious example of a highly distributed business. The typical retailer includes global and regional headquarters, distribution warehouses and consumer-facing brick-and-mortar stores. But many businesses outside of the retail industry are also physically organized like retail enterprises in that they have many geographically distributed stores or offices, as in the following examples:

- Health care services delivery, as in optician services, primary-care doctor's offices, dental clinics, walk-in urgent care facilities, pharmacies and veterinary clinics.
- Consumer-oriented retail banking, insurance and financial services firms with many branch offices.

- Shipping / receiving, transportation and logistics companies with many distribution centers and a large number of retail shipping and business services stores.
- Gaming enterprises with multiple locations for casinos, bingo halls, off-track betting parlors, pachinko parlors and similar facilities.
- Roadside services, which often combine automobile fuel dispensing and electric vehicle charging with convenience retail and quick-service restaurants.
- Enterprises organized under a federated architecture, in which a centralized team may oversee company-wide IT operations, cybersecurity and compliance; however, individual facilities have their own budgets, staff hiring responsibility and local autonomy to manage the business unit's IT infrastructure.

Centralized management of IT and cybersecurity can be challenging

The typical highly distributed business has a heterogeneous mix of hardware, virtualization and operating systems, and applications like inventory or point-of-sale systems from different technology vendors. The mix of tech infrastructure and software revision levels may vary significantly from location to location. The need to preserve legacy applications, custom-built software and computers used to control stable operational technology environments can make it difficult to achieve IT standardization across the company, leading to a proliferation of IT and cybersecurity tools.

Centralized staffers may struggle to become experts in all the tools necessary to protect, manage and secure applications and data across the entire organization. Meanwhile, the complexity and diversity of applications as well as the tools necessary to manage and secure them is growing steadily.

Remote locations with high security requirements, e.g., factory floor environments, may need to be air gapped, i.e., physically isolated from the corporate network and the public internet to minimize exposure to cyberthreats. This limits the ability of centralized staff to diagnose and resolve problems using remote desktop management and other network-based tools, potentially requiring physical travel to remote locations to solve problems.

This can be prohibitively expensive and time-consuming for difficult-to-reach locations, e.g., desert refineries, offshore oil platforms, mining facilities and other sites far from commercial air and ground transportation hubs.

Managing data protection and security in a large, single-location enterprise is less complex and time-consuming than protecting the same number of applications and endpoints scattered across multiple geographically separated locations. If backup data is not segregated by location, then restoration from backup at one location can adversely affect performance across all locations.

Wide-area network connectivity and network speeds in remote locations can vary significantly by geography, making restoration times both unpredictable and potentially too slow to meet recovery time standards.

Remote site management can require IT staffers to log into local data repositories and security management consoles separately and repeatedly, which can be inefficient, error prone and slow. Many traditional backup, disaster recovery and security tools are specialized for particular application environments, making it difficult to standardize on common tools across the organization.

The resulting proliferation of IT operations and security tools is expensive and drives up support staff onboarding and training costs — a growing problem in a world where IT and cybersecurity staffing costs remain stubbornly high.

Compliance can be difficult to manage centrally

Compliance requirements also vary significantly from country to country, and in some cases by state, province and municipality. For example, companies doing business in the U.S. may have to comply with privacy regulations enforced by the federal government, multiple U.S. states and even some individual cities.

Data sovereignty compliance is also a growing challenge. These regulations limit the physical locations, data centers and networks in which sensitive data can be stored or allowed to transit over a network, under the premise that some national governments will violate data privacy with covert surveillance. Honoring these requirements across a widely distributed business is complex to manage and can adversely affect application performance.

Keeping track of what data must be protected on which devices, which IT infrastructure elements are certified as compliant with various security and regulatory standards, and which employees have authorized access to that data can lead to confusion and costly compliance gaps across the organization. These complexities come at a time when most businesses are facing flat or shrinking budgets for IT and cybersecurity staff, while the number of applications and the volume of data they must manage and protect are growing.

Regulatory authorities now wield significant penalties to encourage compliance. For example, the EU routinely imposes fines of two to four percent of a company's annual revenue for repeated failures to protect consumer data.

This can present significant problems for some distributed and multilocation enterprises, including potential networking challenges and difficulties finding compliant, secure third-party hosting of applications and storage with features like secure access control and immutable storage.

Acronis addresses the challenges of managing and securing distributed enterprises

Acronis Cyber Protect addresses the challenges of delivering data protection and security solutions in distributed environments by integrating remote management, backup, disaster recovery and security in a single platform. Individual remote locations can be configured and managed separately by local staff from a console that is dedicated to their location, either installed on-site or hosted in the cloud.

Data protection plans and backup schedules for each location can be customized, or standardized plans and schedules can be rolled out across more than one location. Data protection and security for all local resources can be managed from a single console without having to switch between screens or applications.

All security and data protection functions are managed through a single agent installed on each endpoint. Full data encryption and secure transfer via transport layer security (TLS) ensure that data is secure in transit. Furthermore, data compression, deduplication and bandwidth throttling are managed automatically to optimize traffic at any reasonable connection speed while ensuring minimal impact on active operations.

Meanwhile, headquarters IT and cybersecurity staff can monitor remote locations from a centralized dashboard to assess overall cyber risk, data protection status and compliance across the organization, as shown in Figure 1.

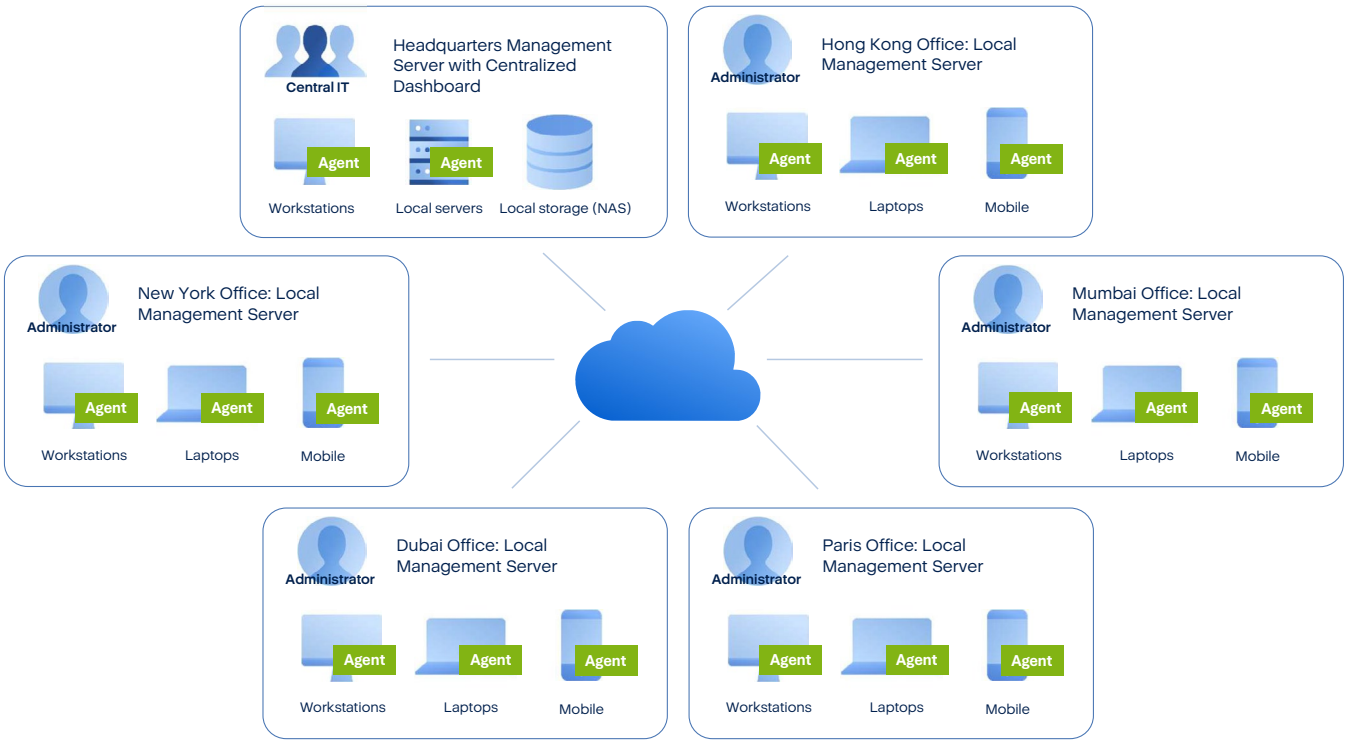

Figure 1. Multisite management of cybersecurity and IT operations with local control and centralized monitoring

Key benefits of Acronis Cyber Protect

- Isolates data storage and security by location.
- Reduces or eliminates compatibility issues in cybersecurity related to hardware, software and virtualization.
- Solves data sovereignty issues and facilitates regulatory compliance.
- Removes issues related to differing network configurations and connections.
- Reduces or eliminates the need for multiple hosting environments for data protection.
- Creates consistent and predictable costs across physical locations.
- Streamlines deployment of georedundant storage.
- Enables centralized monitoring for business-wide cyber risk assessment, data protection status and compliance status.

Acronis solutions are image and file based, using a cross-platform agent that is compatible with most computing environments used in business and manufacturing. Acronis also protects cloud-based email and collaboration platforms, e.g., Microsoft 365 and Google Workspace, and premises-based ones, e.g., on-site Microsoft Exchange.

Acronis supported environments

VMWare vSphere 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Microsoft Hyper-V Server 2022, 2019, 2016, 2012/2012 R2, 2008/2008 R2

Citrix XenServer / Citrix Hypervisor 8.2 – 4.1.5

Linux KVM 8 – 7.6

Scale Computing HyperCore 8.8, 8.9, 9.0

Red Hat Enterprise Virtualization (RHEV) 3.6 – 2.2

Red Hat Virtualization (RHV) 4.0, 4.1

Red Hat Virtualization (oVirt) 4.2, 4.3, 4.4

Virtuozzo 7.0.14 – 6.0.1.0

Virtuozzo Infrastructure Platform 3.5

Oracle Linux Virtualization Manager (Oracle LVM) 4.3

Nutanix Acropolis Hypervisor (AHV) 20160925x – 20180425x

Virtuozzo Hyper Server 7.5

Virtuozzo Hybrid Infrastructure 4.3 – 3.5

Data sovereignty and compliance for distributed environments

Acronis operates a global, independent data center network with points of presence throughout the industrialized world, giving distributed businesses great flexibility for secure data storage to optimize data protection performance and support data sovereignty compliance regulations. Individual remote locations can manage their data protection and security by location, and keep their server, endpoint, email and collaboration data in countries when and where necessary for compliance purposes.

Integrating endpoint management, data protection and cybersecurity in a single platform with local consoles can reduce IT operation costs by as much as 60%. Businesses will realize additional savings with reduced overhead associated with training staff on and maintaining multiple IT and cybersecurity tools, as well as the costs of third-party, geographically compliant data storage and transit.

Distributed and multilocation enterprises have unique challenges in deploying and maintaining security, backup and disaster recovery solutions. These include managing solutions across multiple locations, navigating and maintaining services across innumerable combinations of hardware and software technologies, ensuring compliance with data privacy and data sovereignty regulations, and delivering these services in a resource- and budget-constrained environment. These challenges are amplified when enterprises span international borders.

Benefits of multisite management

Local consoles for remote locations with independent agents

- Single on-premises or cloud-hosted console for each location, department, business unit or brand.
- Bandwidth throttling, data compression and deduplication, always incremental, with optional physical disk transport.
- Agent at source with data encryption and secure transfer via TLS; no need to use corporate network.

Centralized dashboard at corporate HQ to monitor all remote-site Acronis consoles

- Monitor all remote-site Acronis consoles collectively or individually.
- Get a consolidated view of all remote devices, alerts and activities.
- Download data from remote-site Acronis console widgets.
- Drill down to specific devices on any remote Acronis console.

Consolidation of multiple tools

Single agent and console to manage:

- Backup and disaster recovery.
- Email and endpoint security with endpoint detection and response (EDR).
- Patching, inventory, remote assistance, scripting and monitoring.

Protected workloads

- Server, VM, cloud VM and workstations.
- Desktops, laptops and mobile devices.
- Windows (back to 2003 / XP), Mac, Linux.
- Microsoft 365 and Google Workspace.

Improved local compliance

50+ global data centers.

- 11 European data centers.
- 2 German data centers.

Data encrypted at source via AES-265 with business-held passwords.

Data encrypted in transit via SSL / TLS.

Immutable storage.

Multifactor authentication.

Role-based access.

Global compliance certifications.

Reduced costs and vendor complexity

Consolidation on Acronis can save as much as 60% vs. assortment of tools from multiple vendors.

Mitigation of resource limitations

Single console, single management.

AI and machine learning (ML) to assist in everyday tasks.

- Device monitoring and automated fixes.
- AI security incident investigation and remediation.
- Automated backup and DR testing.
- Automated script library for maintenance tasks.

Final thoughts

While most enterprises manage IT operations and cybersecurity with centralized staffs, some businesses will find that delegating some IT and security management functions to teams in regional and / or remote locations can yield improved cyber resilience.

Distributing the management of a company's defenses against cyberthreats and other sources of downtime and data loss, as well as its ability to quickly restore data and uptime when incidents do occur, can reduce business risk more effectively than centralized control.

In these multisite, locally managed scenarios, businesses should equip their regional and remote-site teams with tools that natively integrate cybersecurity, data protection and endpoint management. Adding centralized monitoring of the consoles used at the regional and remote-site level can help headquarters IT and cybersecurity teams audit and enforce company standards for IT governance and compliance.

This combination of centralized monitoring and distributed management of IT operations and cybersecurity can streamline support responsiveness (particularly for air-gapped and very remote facilities), improve compliance with regional security and IT regulations, and reduce overall business risk.

Learn more

To get a complimentary consultation with an Acronis solutions engineer to explore whether a centrally monitored, distributed control topology for cybersecurity and IT operations management makes sense for your business, contact Acronis here.

Get a complimentary 30-day trial of Acronis Cyber Protect here.

About Acronis

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection, and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs), and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond, remediate and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity. Acronis offers the most comprehensive security solution on the market for MSPs with its unique ability to meet the needs of diverse and distributed IT environments.

A Swiss company founded in Singapore in 2003, Acronis has 45 locations across the globe. Acronis Cyber Protect Cloud is available in 26 languages in 150 countries and is used by over 20,000 service providers to protect over 750,000 businesses. Learn more at www.acronis.com.

Acronis

Learn more at
www.acronis.com