daisy.

WHITEPAPER

AN INSIDER'S GUIDE TO DATA PROTECTION AND RECOVERY

Leading vendors speak out on key issues shaping the future of the industry, address your biggest challenges and share their top tips

Acronis NetApp VEEAM zadara Zerto

Industry Insiders Guide to the Future of Data Protection & Recovery

The leading vendors speak out about:

- The key issues shaping the future of the industry
- How they are addressing your biggest challenges head-on
- Their top tips for keeping your data safe and recoverable
- Topics covered include: cyber security, compliance and legislation, public cloud, the impact of COVID-19

Table of Contents

03 **Acronis**

Ronan McCurtin – VP Europe, Israel and Turkey in Sales Northern Europe

07 **Netapp**

Grant Caley – Chief Technologist

09 **Veeam**

Nick Furnell – Systems Engineer

12 **Zadara**

Steve Costigan – Field CTO, EMEA

15 **Zerto**

Chris Rogers – Cloud Architect

17 **Daisy Corporate Services**

Les Price – Head of Availability Services

19 **Working with Daisy**

20 **About the Authors**

Acronis

1. What functionality/features does your platform have to address and mitigate cyber security concerns?

Our recently conducted survey found 80% of organisations can have up to 10 different protection and security tools – and agents – running simultaneously. The complexity of juggling multiple solutions can create gaps in your defences which hampers your overall security.

Acronis Cyber Protect eliminates that complexity by natively integrating backup and recovery with advanced next-generation anti-malware and endpoint protection management into one cyber protection solution, simplifying management and delivering greater security.

> *"With unplanned downtime ranging from £6,200 to £72,000 per hour, a quick recovery can be the difference between surviving an incident or closing down."*
>
> Ronan McCurtin – VP Europe, Israel and Turkey in Sales Northern Europe

Acronis

Our cyber protection solutions are developed based on a five-point framework:

1. Prevention

Proactively preventing attacks on your data, systems and application is key. Acronis accomplishes this with capabilities including vulnerability assessments, automated patch management, URL-filtering, continuous data protection (CDP), and smart protection plans developed by analysts at our global network of Cyber Protection Operations Centres.

2. Detection

Our advanced, next-generation anti-malware is powered by cutting-edge machine intelligence. As a result, our behavioral detection engine stops all manner of malware, ransomware, and zero-day attacks in real-time.

By integrating backup and cybersecurity capabilities, our VB100-certified solution can automatically generate allow lists from backed up data – reducing the number of false positives to ensure what is detected really needs to be addressed.

3. Response

The faster an organisation responds to an incident, the faster it can minimise risk. The integrated nature of Acronis delivers benefits that standalone solutions cannot.

The integration with backup means our solutions can automatically restore files affected during a ransomware attack. It also provides the ability to scan backups for malware, ensuring the file is clean before it's used to recover a file or system, which eliminates the risk of reinfection.

4. Recovery

With unplanned downtime ranging from £6,200 to £72,000 per hour, a quick recovery can be the difference between surviving an incident or closing down.

With an 18-year history of providing best-in-breed backup, Acronis backup and recovery solutions provide full-image and file-level protection for more than 20 workload types.

We provide fast recovery for physical, cloud, mobile, and virtual environments either on-premise or to the Acronis cloud.

Automated runbooks enable you to minimise RTOs with fast failover and failback. Acronis cloud provides isolated testing environments so you'll be sure of your recovery when a disaster actually occurs.

5. Forensics

Following an incident, it's important to know what happened and how it happened so you can take steps to avoid a repeat in the future.

Our solutions help mitigate future risk by collecting the information when performing forensic investigations. This includes forensic backups, metadata and memory dump storage, and audit support.

2. What functionality/features does your platform have to address and mitigate compliance /regulatory concerns?

Each regulatory and compliance regime is different, so Acronis looks to provide a range of capabilities that can help an organisation in its efforts to meet those requirements, including:

- Data sovereignty, Acronis has more than one hundred data centres located worldwide
- As well as full audit logs, Acronis Cyber Protect captures metadata backups for further forensic analysis
- Acronis enforces in-transit and at-rest AES-256 encryption
- Acronis provides enforced two-factor authentication on user accounts
- Provides customisable retention rules, which can help meet data retention requirements
- Enhanced compliance reporting with detailed information about stored data and automatic data classification to track the protection status of important files
- In-built notarisation and e-signature based on blockchaintechnology, providing users with a way to document and publicly prove a file is original and unaltered

Protecting customer data from modern threats means our products must be developed with security in mind. Acronis achieves this objective by:

- Applying Secure Software Development Life Cycle (S-SDLC) which focuses on incorporating security into the development cycle, and
- Developing and continuously maintaining a corporate culture dedicated to security

Acronis

3. How well does Acronis work with other technology providers?

While 53% of security professionals admit that the number of security tools is so burdensome that it adversely impacts security and increases risk, Acronis understands some organisations are more comfortable with specific solutions. As a result, we've designed our cyber protection solution to be compatible with the vast majority of popular protection and cybersecurity software products.

More than that, however, our commitment to protecting all data, applications, and systems – wherever they are – is why we have opened up the Acronis Cyber Platform. Developers and ISVs now have access to the APIs and SDKs needed to incorporate cyber protection capabilities directly into their own solution.

As for interoperability for our channel partners, our service provider solution Acronis Cyber Protect Cloud is integrated with popular RMM and PSA systems, so they can run everything and manage it all using the system they already rely on – including Kaseya, ConnectWise, Atera, and Autotask.

4. What do you see as the developing/emerging trends in the data protection and recovery market?

1. Data protection (traditional backup and recovery) will become completely intertwined with security. Modern cyberthreats are targeting backup files, agents, and software as their first attack action, rendering traditional backups obsolete. Backup that is not integrated with cybersecurity is no longer enough, just as cybersecurity without integrated backup is insufficient – so traditional data protection will give way to comprehensive cyber protection.
2. Protecting data will become an enterprise and supply chain-wide endeavour as more data is propagated throughout the organisation, more workers permanently work remotely, and SaaS offerings continue to grow.
3. Machine intelligence – the next frontier of artificial intelligence (AI) will play an increasing role in the future of data protection. Only by utilising such cutting-edge technologies will the industry be able to stop issues before they happen or make data protection decisions without human interaction.

5. Many organisations are moving workloads to public cloud and using native data protection options, are they protected?

When discussing workloads in public cloud, there are several protection concerns that organisations should consider, but often do not. There's a misunderstanding about what protections are provided by SaaS solutions such as Microsoft 365 and Google Workspace. While vital for many organisations, few realise these services do not provide data protection.

Having the ability to create cloud-to-cloud backups of Google Workspace and Microsoft 365 account data – including the files stored in the attached services like OneDrive and Outlook mailboxes – is critical to ensuring that data is protected. Another consideration is ensuring the proper configuration of data stored in public cloud. With the rush to switch to remote working during the pandemic, many organisations were ill-prepared, overburdened, and overwhelmed by the complexity of migrating to the cloud.

Without the ability to work with experts, a lot of leaks were enabled by incorrectly configured AWS S3 data buckets or cloud databases where the credentials were in the source code and available in a Git hub repository. Such mistakes make an attacker's job infinitely easier.

Finally, consider the cloud tools available to your organisation. Ingesting cloud logs is a prime example. Azure and AWS provide very good logs, but few companies only try to use them after it's too late. Adding the ingestion into your workflow using an SIEM solution to analyse the information to raise alerts, can be an important step in protecting the data placed in public cloud.

6. How has COVID-19 affected you and your customers and in what ways do you think the pandemic will change the data protection and recovery market?

Many organisations may have started considering their digital transformation plans, but the pandemic exponentially accelerated that trend.

While some companies were able to navigate that change on their own, we saw managed service providers step up in a big way to help their customers transition to remote work while keeping the company data protected and secure.

With so many organisations – and employees – seeing the benefits of remote work, it's hard to imagine that the future won't involve at least a hybrid work-from-home model.

Yet protecting valuable corporate data that is being accessed on less-secure home networks and home devices creates new challenges for the organisation.

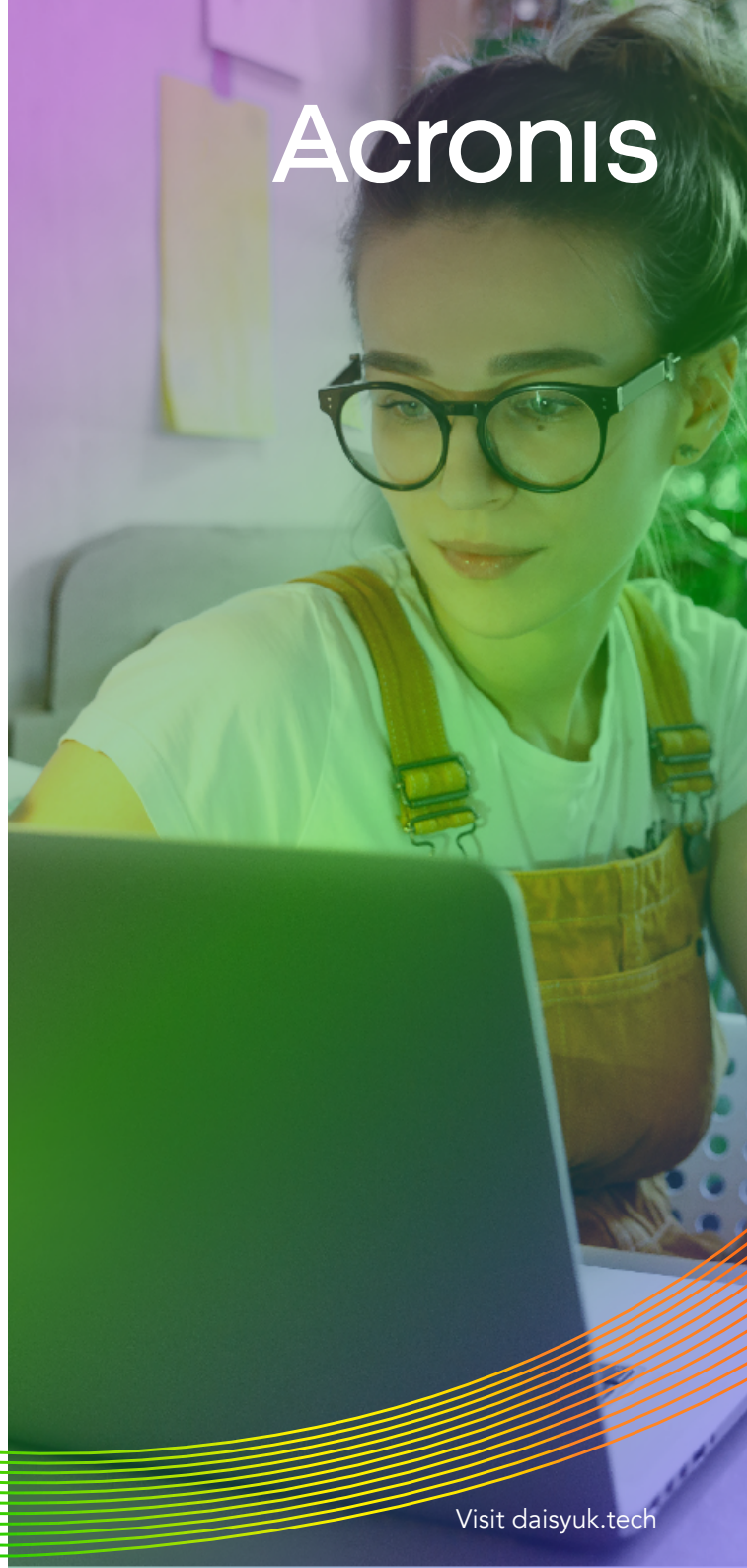
Endpoint protection, remote recovery, monitoring, data loss prevention, email security, and securing video conferencing and work collaboration apps will increasingly take a greater role for organisations looking to protect their data.

7. What are your top data protection and recovery tips for UK organisations?

Following the 3-2-1 rule of backup is just as important now as it always has been, and the availability of cloud backups has made following it extremely easy. Keeping multiple copies of your backups in a combination of locations – both local and off-site – is vital since either storage option can be threatened in an instant, as we saw with the OVHcloud fire earlier this year.

The other tip is to stop keeping your data protection and cyber security operations in silos. Business continuity and disaster recovery (BCDR) plans need to become more closely affiliated with cyber security plans.

The cyber threat landscape is demanding those disciplines merge into modern cyber protection – and your teams and your organisation need to recognise that backup without integrated cyber security is insufficient, as is cyber security without integrated backup.



1. What functionality/features does your platform have to address and mitigate cyber security concerns?

Usually cyber security is focused on detection, prevention, and recoverability. NetApp provides tools such as our Cloud Insights service, which continually monitors user access to unstructured data (on-premises or cloud) and detects when that user may be performing anomalous actions.

For example, an authorised user is accessing all files in a shared area, on a Sunday evening, outside of their usual pattern of daily use. Cloud Insights detects this anomalous behaviour, stops it and alerts admins.

It can also trigger NetApp storage snapshots to provide a recovery point should the activity prove to be Ransomware or Malware that has gained user access through the likes of a phishing attack.

Where attacks have gone un-noticed, and often they do, NetApp has a range of options to protect and minimise the damage that they cause. For example, our on-premise and cloud storage can take thousands of no-impact read-only snapshots providing restore points to minimise the damage an attack may cause.

In addition, to protect against rogue admins, these snapshots can also be made immutable so tht even admins cannot delete them until a future retention date is reached. [Click for more information].

2. What functionality/features does your platform have to address and mitigate compliance /regulatory concerns?

NetApp's Cloud Compliance is a SaaS service that can monitor on-premises and cloud files, databases and S3 object repositories. The service enables any number of regulatory or organisation policies to be tracked, alerting quickly when data creation breaks these.

So, for example, you can track for regulations such as GDPR, HIPAA, PCI and a wide range of others. In the case of GDPR, for example, you can also easily respond and report on GDPR requests, with Cloud Compliance able to generate and publish Data Protection Impact Analysis Reports.

3. How well does NetApp work with other technology providers?

NetApp recognises that a customer solution is based on a range of technologies, integrated and deployed to solve particular business challenges and outcomes.

NetApp focuses on best of breed data management solutions, on-premises and in the cloud and partnering with a wide eco-system of partner technologies ensures customers can build successful outcomes.

For example, we partner with industry leaders such as CommVault, Veeam and Rubrik, for backup, NVIDIA for AI and SAP, Oracle and others for enterprise applications. In the cloud we closely partner with Microsoft, Amazon Web Services and Google Cloud, all with the aim of delivering better aligned customer solutions.

4. What do you see as the developing/emerging trends in the data protection and recovery market?

As in other areas of IT, the cloud as a backup destination is becoming more popular. NetApp storage arrays can backup up straight in the likes of AWS S3, offloading, optimising and simplifying backup via our Cloud Backup Service.

Many of our backup partner technologies also provide similar capabilities.

Ransomware detection, prevention and recovery are hugely popular at the moment. NetApp's ability to deliver this on-premises and in all the public clouds, is especially relevant today.

On the edge of popularity is also the demand for Kubernetes integrated data protection, the persistence of data across any hybrid cloud platform, but also providing integrated backup and disaster recovery, NetApp's Astra service delivers this directly into the Kubernetes stack.

> *"Don't assume the cloud protects your data, you should be architecting this into your solutions and at the service levels you require, not accepting the lower levels offered."*
>
> Grant Caley – Chief Technologist

5. Many organisations are moving workloads to public cloud and using native data protection options, are they protected?

Yes and no is the short answer! Many of the hyperscaler cloud services provide either durability or backup options.

Durability is just the guarantee that they probably won't lose your data, whereas a backup offering protects the relevant service that offers it.

The challenge is when you need to be 100% sure the data can't be lost, or where you build your own IaaS or PaaS based cloud offerings. In these instances, you must provide your own backup mechanisms to protect your data.

This is where NetApp's cloud services such as Cloud Volumes, Azure NetApp Files, Cloud Volumes ONTAP, Cloud Backup and SaaS Backup all come into play.

6. How has COVID-19 affected you and your customers and in what ways do you think the pandemic will change the data protection and recovery market?

COVID-19 has affected every company, for some customers many projects were put on hold, but for others they massively accelerated the delivery of projects such as remote working, cloud adoption and others.

NetApp's hybrid cloud capabilities have enabled us to help customers deliver on many urgent projects, both in the data centre and all of the public clouds.

I think COVID-19 has meant that the data protection and recovery market has needed to be more capable, more expansive, and better delivered in response to increased cyber-attacks, but also in response to having to protect a wider hybrid cloud landscape.

7. What are your top data protection and recovery tips for UK organisations?

Our three top tips for data protection and recover are as follows:

- Don't assume that the cloud protects your data, you should be architecting this into your solutions at the service levels you require, not accepting the lower levels offered
- Ransomware and malware attacks are real and pervasive. Build a data detection, data protection and data recovery environment to mitigate the risk this poses. Don't forget to ensure this is hybrid cloud capable too
- Data protection and recovery is a complex issue, it takes a combination of technologies such as those offered by NetApp and our eco-system partners, under the expert integration of Daisy, to really ensure your organisation is protected

1. What functionality/features does your platform have to address and mitigate cyber security concerns?

Veeam® Backup & Replication™ delivers availability for ALL of your cloud, virtual and physical workloads. Through a simple by design management console, you can easily achieve fast, flexible and reliable backup, recovery and replication for all your applications and data.

Protecting backup data from attack

Air-gapped or "immutable" backups offer a powerful technique for being resilient against ransomware and other threats. Enable a replica of your backup, stored out of the reach of cyber attacks, utilising controls that ensure deletions or changes cannot happen without strict multi-level approvals.

Veeam Scale-Out Backup Repository (SOBR), partnered with Capacity Tier (also known as Cloud Tier), enables an easy-to-use capability that writes backup data into object storage either on Microsoft Azure, Amazon Web Services (AWS), IBM Cloud or any platform that supports object store. Using AWS S3 or select S3-compatible storage, you also get access to Object Lock, enabling backup data to be stored as an immutable backup. Daisy has its own S3 storage that supports immutability to complement the Veeam services.

Detecting ransomware

Detecting a ransomware attack in its initial stages can be difficult. Veeam ONE provides the ability to monitor your environment closely and be aware of any suspicious or abnormal activity.

By analysing CPU usage, datastore write rate and network transmit rate, Veeam ONE can help identify whether there are higher than normal amounts of activity on a particular machine.

When the alarm is triggered, this immediately notifies you to inspect the machine, look at the resource counters and determine for yourself whether or not the activity is normal. If it's not, this is a good indicator that more steps should be taken to determine if ransomware is the culprit.

Ensuring ransomware-free backups

Viruses can lie undetected and dormant in your current systems, ready to pounce. Use the power of your backup to root out ransomware threats before they attack. At all stages of backup and recovery, you want to be protected. Keep ransomware out for good with an automated step to scan the backup for malware, delivering confidence for future restorations.

Restoring guaranteed virus-free workloads

What happens if your backups have an undetected virus? Viruses can remain undetected and lie dormant in older backups. Make sure you can protect yourself. Secure Restore enables a complete antivirus scan of your backups when restoring. Having access to the latest virus definitions helps safeguard against previously unknown viruses, providing greater confidence that dormant threats won't be reintroduced back into the environment.

Testing your workloads securely

Unsure of a current workload? Suspect that it may be infected? Restore them into a fully-secured and isolated environment to test. Tap into the power of Veeam DataLabs to restore data, workloads and applications into a fully-isolated virtual sandbox environment. Test for cyber threats and other issues while performing potential remediation activities — without impacting any production systems.

2. What functionality/features does your platform have to address and mitigate compliance /regulatory concerns

Veeam® Availability Suite™ combines the monitoring capabilities of Veeam ONE™ with the powerful data protection features of Veeam Backup & Replication™ in one Enterprise bundle to meet both your protection and analytics needs. By combining these two industry leading products, customers can more easily achieve their advanced data protection needs while also gaining key insights of their configurations for greater data protection and business agility.

Veeam ONE delivers deep, intelligent monitoring, reporting and automation through interactive tools and intelligent learning, identifying and resolving real customer problems before they become major issues. Veeam remains focused on delivering key capabilities that ensure organisations like yours get complete visibility into their backup infrastructure and the operational aspects of their backup and recovery processes.

Veeam ONE delivers feature-rich monitoring and analytics to provide the clear visibility you need:

Built-in Intelligence: Identify and resolve common infrastructure and software misconfigurations before operational impact.

Governance & Compliance: Organisations know their data protection posture instantly through consistent monitoring and reporting on backup SLA compliance. Intelligent Automation: Machine Learning-based diagnostics as well as remediation actions to resolve issues faster. Forecasting and planning: Visibility into the costs of compute, storage and backup repository resources to forecast utilisation rates and resource requirements.

Veeam Backup & Replication v11 introduces the Hardened Repository as a secure place where backups can be stored immutably for a configured amount of time. With the Hardened Repository, Veeam created a write once, read many (WORM) storage option for Veeam backups. And the best part, this new role can be deployed on ANY general-purpose Linux server, without locking you down to the special proprietary hardware.

3. How well does Veeam work with other technology providers?

Veeam is software-defined and hardware-agnostic. It partners with a broad ecosystem of dedicated partners to help customers achieve their goals without having to implement proprietary solutions.

4. What do you see as the developing/emerging trends in the data protection and recovery market?

2020 was a unique year for everyone, and business was no exception. External pressures unknown to our generation have forever changed the IT landscape, creating new challenges for all. Veeam's recent Data Protection Report 2021 looked into a survey of more than 3,000 unbiased enterprises worldwide to understand how they approach data protection and management today, as well as future trends. The results provide key insights into how this data can help you with your own IT challenges when tackling modern data protection.

Key findings:

- 11% growth in global economic uncertainty. Economic impact is driving organisations to think about their IT direction differently
- 96% of organisations will accelerate cloud usage. COVID-19 significantly accelerated cloud adoption to ease on-prem management
- 80% of organisations now have an availability gap. Faster modernisation is increasing pressure on aging legacy systems
- 58% of data cannot be recovered. Failed backups and unverified restores means lost data and productivity
- #1 driver for change is backup reliability. Organisations are looking for better reliability through modern protection

2020 changed the landscape of IT. Economic uncertainty is undoubtedly topping the list of anticipated challenges in 2021 as reported by 40% of organisations worldwide, which is up from 11% globally from the previous year. Including growth in meeting changing customer needs, it confirms much of what we expect.

Businesses are laser-focused on driving growth whilst ensuring they exceed customer expectations. This is putting more pressure on data protection, as in times of business stress, business continuity becomes hyper-important, and that rests on having a strong data protection solution.

5. Many organisations are moving workloads to public cloud and using native data protection options, are they protected?

When it comes to using a public cloud storage service, it's critical to be aware of how the security and compliance responsibilities break down. In other words, how does the cloud service and the organisation using it "share" the responsibility of data? The answer: the Shared Responsibility Model or Matrix – the two are intechangable. The Shared Responsibility Model offers increased flexibility and customer control, but organisations are always responsible for their own data security, protection, and availability.

In the case of AWS, here's how the Shared Responsibility Model works:

- AWS is responsible for security of the cloud. That meansAWS is responsible for all the infrastructure that runs AWS Cloud services like hardware, software, and networking
- Customers are responsible for security in the cloud. This responsibility extends to all operating systems, applications, network configurations, and data

Similary, Azure, Google Cloud Platform, etc. aren't responsible for your cloud data, they are responsible for the cloud in which that data resides. Your responsibility is for everything you deploy in the cloud. Your apps, accounts, settings, and, yes, even your data are entirely your responsibility.

6. How has COVID-19 affected you and your customers and in what ways do you think the pandemic will change the data protection and recovery market?

COVID-19 also had an extraordinary effect on digital transformation (DX) efforts. In many cases, you would expect DX plans to slow down due to the reallocation of efforts, and in 30% of organisations, that is precisely what happened.

But there was also a massive increase in DX speed, with 54% of organisations accelerating their initiatives.

Organisations with mature DX plans accelerated their investments, however, the companies that have less mature efforts tended to pause to focus on sustainability.

What will 2021 bring to IT strategy? The results show a massive investment change in IT delivery. In fact, only 4% of organisations surveyed were not anticipating any significant changes in 2021.In the first months of the pandemic, 91% of organisations increased their cloud services usage (31%) significantly.

This came from remote workers using SaaS-based collaboration services and the increased challenge for IT to maintain on-premise, physical operations.

ost organisations planning to add more cloud services and cloud usage to IT delivery strategy.

7. What are your top data protection and recovery tips for UK organisations?

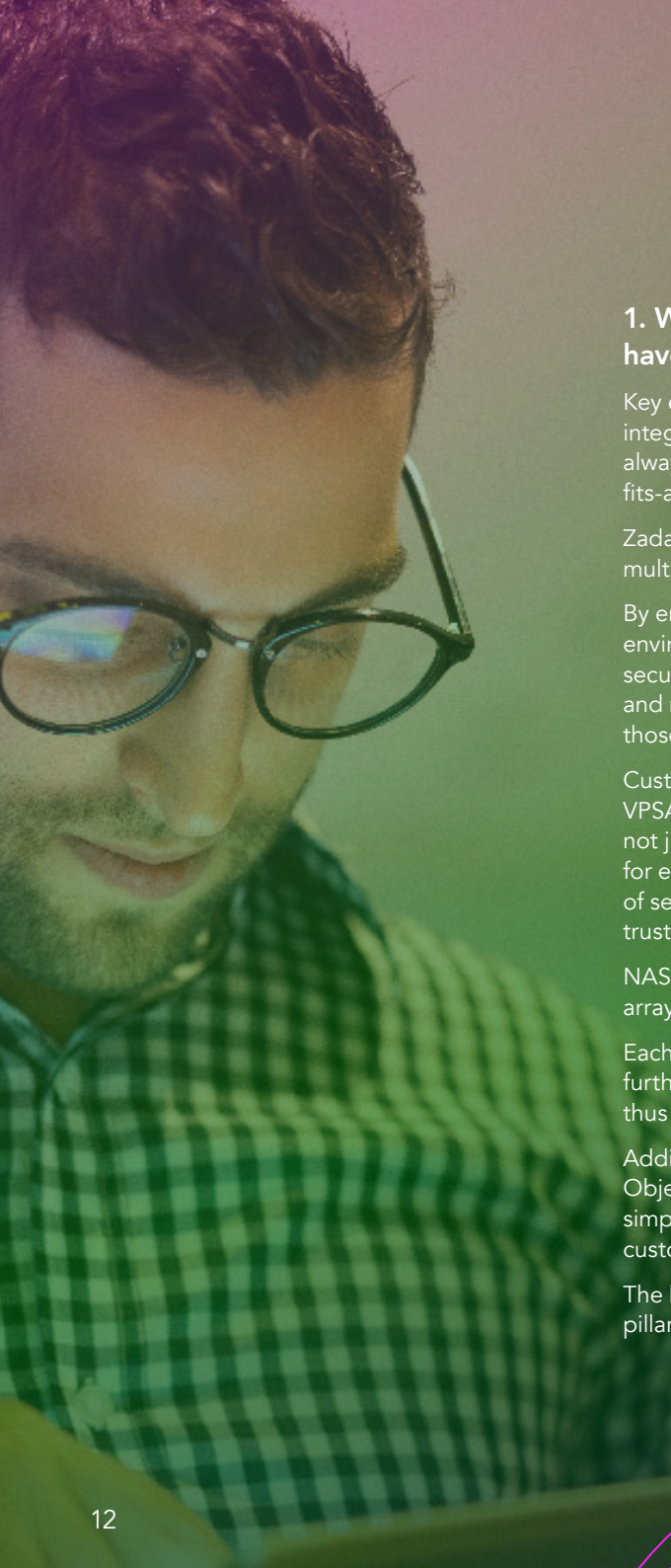
Multi-layered approach – No single thing is going to completely protect an organisation from every conceivable event. This is reflected in the fact that Veeam has multiple products, each one designed to address various solutions.

Education – Prevention is always better than a cure. it is only through constant education and conditioning that we will "do the right thing". Reducing any type of data loss at the source is better than recovering after the event – no matter how capable and sophisticated the solution.

Understand the value – Losing data has a financial impact, not just the zeros and ones, but also the intellectual property, any personal data and the time taken to create that information in the first place. Instigating a process to protect, recover and even reuse this data is not free.

Get the right people involved – discussions and planning for data protection, disaster recovery and business continuity scenarios are all business decisions, not simply technical ones. The protection and recovery process needs to be understood and acted upon at all times.

> *"When it comes to using a public cloud storage service, it's critical to be aware of how the security and compliance responsibilities break down. In other words, how do the cloud service and the organisation using it "share" the responsibility of data?*
>
> Nick Furnell – Systems Engineer



zadara

1. What functionality/features does your platform have to address and mitigate cyber security concerns?

Key elements of cyber security are in adoption CIA (confidentiality, integrity and availability) within your security modelling. This is always a best-fit model for each and every organisation as a one-size-fits-all approach rarely works.

Zadara built its patented zStorage platform to be a cloud-native multi-tenant platform with security at the forefront of its design.

By employing an isolated Virtual Private Storage Array (VPSA) environment running on dedicated physical resources, a tiered security model offering each tenant its own security policies, users and multi-factor authentication (MFA) is used to ensure that only those that need access to data and management have access.

Customers have the option of having unique encryption keys per VPSA and deciding which data is encrypted down to a volume level, not just a system-wide setting. We have recently added support for external key management systems to provide additional levels of security by offloading the management of keys to a third party trusted system controlled by the customer.

NAS Volumes have the option of running antivirus within the storage array, powered by McAfee.

Each VPSA can support multiple virtual network interfaces (VNIs), to further limit access based upon source and destination network only, thus enabling accessibility and security concurrently.

Additionally, utilising different technologies such as Block, File and Object capabilities with centralised platform management enables simple segregation of data in limiting access to data in the event of a customer environment compromise.

The key is a multi-layer approach and this has been one of the major pillars in the design of Zadara's storage portfolio.

2. What functionality/features does your platform have to address and mitigate compliance /regulatory concerns?

Zadara conforms to ISO 27001, SOC and SOC2 best practices for operational support and management. By providing the customer with choice on which features to deploy and how, enables a greater range of flexibility to achieve the different goals of each organisation.

Zadara operates a shared responsibility model and works closely with customers providing them with the tools they need to have complete confidence and control of their own data management requirements.

With support for features such as external key management services (KMS) and AES 256 encryption, it provides an even greater level of security and control for customers and their environments. Coupled with granular role-based access control (RBAC) and multi-factor authentication, even support functions can be restricted if required.

Separation of the data and management planes further enhances an organisation's ability to design around different customer needs, all the way down to the physical storage medium where disks can be allocated to a single tenant.

This gives complete control to the customer or service provider by providing the appropriate model to maintain in an ever-changing regulatory landscape.

By providing the enterprise capabilities and functionality of a truly multi-tenant platform, Zadara allows customers to have confidence that they are in control of their needs.

zadara

3. How well does Zadara work with other technology providers?

No organisation can work in isolation; different organisations have different needs and therefore having strong partnerships is essential. Building on key partner capabilities such as Veeam's Object-Lock (immutable storage) capability with Zadara Object Storage provides a key example of where two partners combine to provide a solid option around backup and recovery, especially in view of the ever-growing threat of ransomware.

The Zadara zStorage platform also provides the capabilities of utilising Intel Optane NVMe Disk technologies, thus demonstrating that everything from the hardware components to the operating system and application stack is critical in supporting a wide range of customer needs.

This is further enhanced when adding multiple partners such as the use of Zadara in conjunction with VMware and Nvidia (Mellanox) to support high-speed, low-latency storage capabilities using the iSCSI extensions over RDMA (iSER) protocol over a common Ethernet bearer, delivering up to 100Gb/s connectivity using current generation technology.

Zadara operates on open standards and this helps in driving partnerships simply and easily, by offering multiple tiers such as Block, File and Object storage supporting iSCSI, iSER, Fibre Channel, NFS, SMB, S3 and Swift protocols. We provide a comprehensive platform that allows organisations to easily plug the Zadara platform into almost any existing environment.

We were the first vendor to support multiple VLANs with iSER in conjunction with Mellanox, this demonstrates the drive to constantly explore new capabilities and push the boundaries further with our partners to achieve greater capabilities for our customers. Zadara was an early partner with Veeam in supporting Immutability within the Object Storage tier in Veeam v10 and we continue to work closely with Veeam on this capability.

4. What do you see as the developing/emerging trends in the data protection and recovery market?

Data continues to be the central lifeblood of many organisations; the value of data is increasing hence why we have seen the growth in ransomware attacks over recent years. We are entering into a phase where it is not a case of if, but when, an organisation needs to be thinking about the impacts.

Robust data protection and disaster recovery planning is going to be an essential part of keeping a business operational if it is not already in place – regardless of size. Simple backup to tape of yesterday, or just copying live data to a cloud provider is not robust enough. We are seeing variants of ransomware that are lying dormant until an opportune moment that could be weeks or months down the line.

As the data size gets larger so does the problem, then comes the data migration problem which is why organisations are looking at alternatives to tape. Having a common envelope regardless of underlying physical media is the only option for the future. This is being played out in other areas such as virtual machine types and containerisation, the latter of which will bring new challenges for data protection that must be overcome. This is all going to add complexity to the IT landscape and it is important to pick the right partners, especially those that have specialist skills. As the complexity rises so does the threat and therefore the risk.

It is vitally important that not just systems, but people, skills, and planning are understood and in place. The recovery process must have flexibility to support differing customer demands simply and easily, which requires specialists who can help under stressful conditions because they have the right level of experience and testing that a generalist person may not.

> *"Equipment and software does, and will continue to fail, so will people. Identify your key assets, put a plan in place to protect them and ensure that you have tested you can recover them."*
>
> Steve Costigan – Zadara Field CTO, EMEA

zadara

5. Many organisations are moving workloads to public cloud and using native data protection options, are they protected?

Public clouds have their place and like any other technology innovation, some things are suited and some are not. Where massive scale and dynamic change is required, the public cloud offers options, but they may be limited by legal, regulatory, access or latency constraints.

Organisations will eventually want the best of both worlds in terms of a cloud-like service but with the choice of locations; on-premises or in a hyperscaler or delivered by a service provider that can help them manage the complexity.

This is where Zadara is able to provide a complete end-to-end offering with a key partner like Daisy. The other impact of public cloud is that the size of the outage, if and when it happens, is on a much larger scale, something that has been demonstrated many times over recent years.

Unless you have a valid plan that includes multiple locations, you are still susceptible in the same ways as you would be running in your own data centre or a co-location provider. This includes SaaS services such as Microsoft 365, where a shared data model is in place and an organisation is responsible for protecting its most valuable asset – its data.

6. How has COVID-19 affected you and your customers and in what ways do you think the pandemic will change the data protection and recovery market?

In 2020, Zadara and Veeam conducted a number of joint webinars that included details on COVID-19 and how the need to work from home would increase the possible attack footprint and scenarios deployed by ransomware groups. Sadly, much of this has proven to be true with the number of attacks continuing to increase.

This has raised the profile for the need to ensure that organisations have a more comprehensive recovery strategy in place, one that is tested and adheres to Veeam's 3-2-1-1-0 zip code recovery options.

Simply backing up your data and testing a disaster recovery plan once every few months is not enough any more, backup streams are becoming infected over time, therefore even recovery without cleansing becomes just a wasteful exercise of valuable resources.

More organisations have adopted the use of Microsoft 365 and Teams which contains valuable company data that could be lost if not protected.

Interestingly, organisations have had to deploy more endpoints, either as laptops that need to be protected or using Remote Desktop Access (RDA) mechanisms such as Citrix, VMware Horizon View, Parallels or just native Windows RDP services.

Some of these environments may have been deployed without best practices, exposing organisations to brute force attacks and zero-day vulnerability attacks.

Additionally, organisations have relied on external access to systems like Microsoft Exchange and the recent high-value vulnerabilities have left many organisations exposed with little chance of tracking users' action before it is too late.

As we migrate to more a more flexible working environemnt, the protection landscape has to adapt and adopt new technologies and techniques to cater to this.

Zero trust environments will become the norm, backup and recovery will need to address the needs of this, and a hybrid cloud model that is evolving will place even more reliance on expertise such as those provided by Daisy.

7. What are your top data protection and recovery tips for UK organisations?

Fail to plan and you plan to fail – it is not a case of if but when. It is foolish to think it won't happen to you. Whether you are a small one man band or a large multinational corporation, you are a target for ransomware. Equipment and software does and will continue to fail, so will people.

Identify your key assets, put a plan in place to protect them and ensure that you have tested you can recover them – your business depends on this.If you don't know where to start, ask people like Daisy, who do it day in and day out.

Zerto

1. What functionality/features does your platform have to address and mitigate cyber security concerns?

Cyber security needs a combination of solutions both preventative, including software and education, as well as corrective. The sad truth is that cyber criminals can find ways to penetrate even the most secure environments, so you always need a plan b.

Daisy utilises the real time protection and journaling aspect of Zerto to offer clients the ability to be able to roll back to seconds prior to their systems being locked down by a ransomware attack, reducing your organisations downtime from days to minutes and avoiding the requirement to pay for expensive ransoms.

Zerto's recovery point objective (RPO) and recovery time objective (RTO) are unrivalled, combined with the automation and orchestration Zerto has built in, this provides customers the ability to recover whole environments to seconds before a ransomware attack with just four clicks.

2. What functionality/features does your platform have to address and mitigate compliance /regulatory concerns?

Zerto has the ability to perform non-intrusive test fail overs, generating reports that can be used for compliance that highlight the recovery times of the platform in the event of a disaster. This on its own is key for most organisations.

These same test failover environments can also be used to test patch updates, application upgrades and even vulnerability scanning whilst putting no additional load on your product environment.

Zerto also has the ability to replicate up to three different locations at the same time, these can even be different hypervisors or clouds as well. This gives customers who have high regulatory compliance peace of mind that their data will always be available in any circumstance and can mitigate risk by using multiple different platforms to avoid any vendor lock in.

Zerto

3. How well does Zerto work with other technology providers?

Zerto has nearly 20 Major Technology partners that work on variety of joint initiatives to position and market the full end user solutions stack for enterprise IT.

Zerto is a member of VMware's Technology Alliance Partner (TAP) program at the advanced tier and part of VMware's Solution Exchange. As a design partner, Zerto continues to drive innovation and further integration with VMware vSphere.

Zerto is also vendor agnostic so can play a pivotal role in helping organisations avoid vendor lock-in.

4. What do you see as the developing/emerging trends in the data protection and recovery market?

Zerto believes we will see a move towards a more continuous approach – with the aim for organisations to minimise data loss with only seconds being lost rather than days or hours. This combined with new technologies such as Kubernetes and organisations understanding that this infrastructure requires the same level of protection as traditional VM workloads.

Useful links:

Ransomware recovery video

Cyber-attack survival guide

IT Resilience

Zerto technology partners

5. Many organisations are moving workloads to public cloud and using native data protection options, are they protected?

Moving workloads into public cloud and SaaS applications can save time and money and is a great move for many organisations, however the data is still the organisations responsibility – so wherever your data is located make sure you are aware of the backup and disaster recovery solutions to ensure that your organisation's requirements are met.

Some vendors may offer some level of data protection however this may not meet your required SLAs, I would advise speaking to a data protection specialist team to discuss your overall strategy for all of your environments.

6. How has COVID-19 affected you and your customers and in what ways do you think the pandemic will change the data protection and recovery market?

The pandemic has accelerated cloud adoption and disaster recovery as a service (DRaaS) has seen a big take up over the course of the pandemic allowing businesses to focus on their own strategic initiatives and allowing a DRaaS provider to look after data protection for them.

The pandemic has changed data protection as there has been a huge spike in ransomware attacks, data protection has long been a tick box exercise to ensure it is done, however we have found that organisations are starting to test the limits of their data protection strategy when thinking about recovering a whole infrastructure rather than just individual files, folders or VMs.

7. What are your top data protection and recovery tips for UK organisations?

Always challenge your SLAs and don't just accept the status quo, make sure you are looking at what is possible and not just what you already have in place.

Make sure your data protection strategy can recover your whole infrastructure in an effective and timely manner – making sure testing this type of recovery is done on a regular basis.

> *"Moving workloads into the public cloud and SaaS applications can save time and money and is a great move for many organisations, however the data is still the organisations responsibility."*
>
> Chris Rogers – Cloud Architect

1. What functionality/features does your platform have to address and mitigate cyber security concerns?

At Daisy, our security portfolio is structured to help you effectively discover, prevent and respond to security threats and build a layered security strategy that fits your business.

Our services encompass the detection and discovery of threats and vulnerabilities with Security Insights, the protection of your business through Network Security, Cloud Security and Endpoint Security.

It's an unfortunate fact of life that at some point your business will be affected by a cyber incident, either directly or indirectly. Our award-winning continuity and resilience services can help you to recover from a cyber event.

Without good planning you're a sitting duck for cyber criminals. Once you have a plan for how you would manage a cyber incident, it is essential that you test it.

Crisis management exercises are an invaluable way to understand how your teams react to a breach and how your business would be affected in real-world scenarios.

Run by experienced business continuity and information security consultants who are experts in their field, these are an ideal way to test your plans in a safe, controlled manner.

During a cyber incident, our data protection and recovery solutions like backup, replication, IT disaster recovery and work area recovery can be invoked in a variety of ways to best meet the nature of the breach you are experiencing.

For example, you may need a complete recovery of your entire IT and office environment or a partial recovery of key elements such as networking, systems or offices.

Our comprehensive recovery infrastructure and our flexible options are all designed to help you manage the common and the more unexpected impacts of a breach.

We work with your insurance provider, IT and business continuity teams to ensure the best recovery outcomes for your organisation.

We can also undertake forensics work, or work with your provider to analyse what happened.

2. How do you help organisation address and mitigate compliance and regulatory concern?

Daisy offers several consultancy services specifically for customers needing compliance and regulatory advice and help with controls, policies, procedures and audits.

In the delivery of our data protection services, all data is securely stored in full compliance with the relevant industry legislation, including GDPR, FCA, PRA etc. All data is encrypted at rest and in flight, using AES-256, FIP 140-2 etc. depending on the service being taken, using the customer's own private keys.

3. How well does Daisy work with other technology providers?

In today's "as-a-service" world, organisations expect to work with multiple suppliers who come together either directly or indirectly to deliver the agility required to remain competitive.

Daisy can work with other suppliers or can manage them on behalf of the customer.

Daisy is vendor and technology agnostic. Because we've been around since the formation of the business continuity industry, we have expertise in legacy technology and everything that has come since.

We partner with all the leading technology vendors at the highest levels of accreditation. Our data protection and recovery services, methodology and expertise, integrate with a broad selection of best-of-breed vendor technologies.

4. What do you see as the emerging trends in the data protection and recovery market?

We have seen with recent cyber attacks that insurers are withdrawing ransomware payments and concentrating on preventing future attacks through forensic analysis and limiting cover to keeping the business running.

Cyber threats are driving technology changes – backup, replication and storage vendors are building evermore resilience and additional security features into their platforms.

Technology providers are responding to the fact that multiple solutions create opportunities for cyber criminals to exploit – so there is a move towards integrating more functionality into single solutions to address this.

This quickly changed to homeworking being the priority, for many organisations this solved both the social distancing and self-isolation issues raised by the pandemic.

The pandemic highlighted how many IT processes for DR, backups, etc. relied on being at an office. We saw, for example, how many businesses moved their backups and DR off-site to Daisy, replacing the need for tape backup requiring manual intervention, to our cloud-based services that don't.

As has been widely observed, the pandemic has accelerated the pace of change for both IT and business practices.

Organisations that can take advantage of hybrid or homeworking long term, get a bigger pool of candidates and employees get a better work/life balance, which is win-win for everyone.

We're seeing this reflected in our DR contracts, especially in the work area market, where a more flexible, combined recovery and serviced office requirement is emerging.

7. What are your top data protection and recovery tips for UK organisations?

We recommend partnering with a trusted and experienced provider, to ensure adequate planning and awareness.

You cannot just build processes and procedures for managing a breach, as cyber criminals don't follow them. Regular crisis exercises and DR testing are needed to understand what happens in real life and test your ability to execute your plans.

Get the right people involved – discussions and planning for data protection, disaster recovery and business continuity scenarios are all business decisions, not simply technical ones. The protection and recovery process needs to be understood and acted upon at all times.

> *"Cyber threats are driving technology changes – backup, replication and storage vendors are building evermore resilience and additional security features into their platforms."*
>
> Les Price – Head of Availability Services

WORKING WITH DAISY

Acronis

Daisy is a genuine thoroughbred of business continuity and data protection services in the UK. It's no wonder Daisy's accomplishments have been acknowledged with multiple awards and industry acclaim.

Through their dedication to providing systems resilience, protecting data, and ensuring that business systems are secured from the ever-evolving threat of modern malware and system exploits, Daisy shows the kind of commitment to their customerslients that Acronis values in a cyber protection partner.

NetApp

Daisy is the trusted advisor to its customers, bringing together expertise, solutions and consultancy across a customer's IT environment. This includes, but isn't limited to, compute, storage, networks and software.

The cross-domain expertise, customer understanding and tight vendor relationships and knowledge, are all leveraged to ensure customers can build and deploy the best-of-breed data protection solutions.

VEEAM

Daisy is an established and competent provider of data recovery and protection (DR&P) services. Delivering their breadth of services requires strong technical abilities both from the staff themselves and the 50+ technology platforms they rely on.

Daisy's ability to offer tailored solutions, ranging from data recovery and disaster recovery through to business continuity and even emergency workplaces makes them an excellent choice for any business looking for a safe pair of hands.

zadara

Daisy is a world-class organisation with a long-established history providing business continuity, disaster recovery and data protection.

This makes them the perfect partner to help Zadara enhance our storage proposition.

If you value your data it's good to know that Daisy has the skills, experience and solutions to look after it!

Zerto

Daisy has been a strategic partner with Zerto for nearly a decade, providing a disaster recovery solution powered by the Zerto Cloud Data Management and Protection platform. Daisy enables organisations to resume operations and remain resilient when facing any disruption.

The managed services, support, and expertise of Daisy, gives end users the confidence they need to protect their critical applications and data with our joint solution.

ABOUT THE AUTHORS

Ronan McCurtin – Acronis

Ronan McCurtin is the Vice President for Europe, Israel and Turkey at Acronis, a global leader in cyber protection solutions.

With more than 20 years of experience in the international IT and software industry, Ronan brings extensive experience in this segment, where he has successfully led multiple teams.

He is highly qualified and experienced in developing and improving channel business and customer relationships to create efficient distribution channels and partnerships. These efforts include working with resellers and managed service providers.

Grant Caley – Netapp

Grant is an experienced Chief Technologist with a demonstrated history of working with UK customers and partners across all industry and technology verticals.

Skilled in helping customers understand and develop their data fabric strategy across on-premises and the hybrid cloud, Grant focuses on enabling business agility, cost efficiency and operational consistency, governance and risk control to drive business and operational outcomes.

Nick Furnell – Veeam

Nick works with greenfield sites to established MSP/ CSPs, and every combination in between.

Applying the various scenarios which can be built from the underlying Veeam platform keeps Nick on his toes. Being able to leverage 25 years of experience in IT, consuming, providing and now implementing services proves invaluable in enabling Nick to 'see beyond the software'.

Chris Rogers – Zerto

Chris is a Technology Evangelist at Zerto. More than 10 years' experience working in the DR and the IT Service Provider industry, enables Chris to draw from this to ensure Zerto and Daisy provide the best possible outcomes for its customers. Chris can help Daisy and its end users' architect and deploy Zerto to achieve industry leading RTO and RPO across hybrid and multi-cloud environments.

Steve Costigan – Zadara

Steve has more than 30 years' experience across many data centre and cloud technologies and systems, taking complex technical subjects and making simplified solutions achievable. Steve joined Zadara in 2014 and has experience with key OEMs such as IBM, SUN, SGI and HP in delivering solutions around the StoreAge SVM/HP SVSP solutions. He holds a Masters in Management (IT) from Charles Sturt University.

Les Price – Daisy

Les has been responsible for all operations and service delivery to Daisy's Business Continuity customer base for more than 20 years.

His commitment to customer service has helped Daisy achieve and maintain outstanding customer service levels for rehearsals (testing) and invocations throughout this time.

NEXT STEPS

If you want to find out how Daisy can help you to improve your data protection strategy contact us on:

0344 863 3000

Or if you're an existing customer, get in touch with your account manager directly.

Visit daisyuk.tech