WHITE PAPER

Best practices in cybersecurity and cyber resilience

A Data Security Alliance paper

Table of Contents

Executive summary

Imagine your business or government agency is a Formula 1 race car. You spend hours a day preparing to compete in the highest class of international racing, but no track is the same. The competition varies. Drivers are human. The weather changes. More than any other factor, though, your success depends largely on one thing: having an exceptional pit crew.

The same is true for cyber resilience. Having an integrated, technical cyber defense that combines exceptional data security and data management, similar to a Formula 1 pit crew, helps ensure your organization stays on track and finishes strong.

In November 2022, more than a dozen security industry heavyweights formed the **Data Security Alliance** to give businesses and governments more ways to win the race against cyberattacks. Its mission is clear: to secure and protect data. The Alliance accomplishes this by unifying data security and data management with cybersecurity to improve cyber resiliency, delivering critical technical integrations and architectures, best practices, and thought leadership around a common focus.

This white paper from the Data Security Alliance outlines how senior leaders can address top business priorities, including reducing risk and strengthening compliance through smarter cyber resilience investment. With a nod to the new NIST cyber resiliency engineering discipline, this paper highlights best practices aligned with the Data Security Alliance's collective vision and technologies. It illustrates how member organizations are elevating ideas and strategies for countering threats from an individual company level to an industry level—and doing so in sync with the NIST Cybersecurity Framework—focusing on identify, protect, detect, respond, and recover.

Cyber resilience matters

In today's digital world, consumers and employees expect organizations of all types and sizes to operate without interruption. Contractual obligations such as service-level agreements even demand it. Yet incidents—both planned and unplanned—can introduce downtime. That's when cyber resilience matters.

> "Converting data into value in a secure and ethical manner is the business imperative of the next decade. Whoever controls their data lifecycle will most direct their destiny. As the perceived value of data increases, it will become a heightened target of corporate espionage and state-based cyberattacks."[1]
>
> – **Dr. Jan-Peter Ohrtmann,** Partner, PwC

The goal of cyber resilience is to achieve the highest level of operational and business continuity in the face of escalating threats. Cybersecurity—the practical, must-have cyber hygiene practices that include regular patching, detecting threats, discovering vulnerabilities, and more—is foundational to cyber resilience but incomplete. Cyber resilience goes well beyond disaster recovery, also requiring organizations to anticipate, withstand, recover from, and adapt to disruptions quickly, in minutes or hours, not days or weeks.

[1] PwC. "Privacy Megatrends 2030: A Roadmap for CEOs," Dr. Jan-Peter Ohrtmann, 21 Jan 2021.

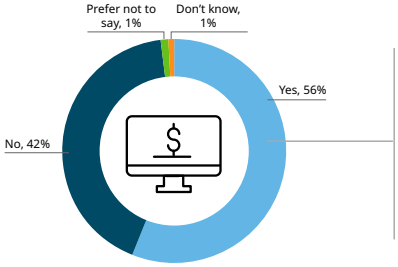
"Resilient companies have a strategy and framework for risk identification and mitigation; thorough business continuity planning and preparedness; flexible crisis and incident response capabilities; and business systems designed for redundancy and dependability," Forrester's Stephanie Balaouras, VP, Group Director wrote in May 2020.[2] Just a few years and hundreds of thousands of ransomware attacks later, companies also now need cyber resilient strategies and frameworks, too.

Cyber threats, particularly ransomware, continue to become more frequent and sophisticated. So organizations worldwide must advance new cooperation among typically siloed security and data management teams and solutions to maximize cyber resilience in 24x7x365 environments—all while meeting business continuity needs. Only through the integration of technologies and processes can organizations' modern digital foundations withstand and recover from cyberattacks, natural disasters, and system failures.

Against this backdrop, data protection is quickly becoming a top priority for business and government leaders. Customer loyalty, brand reputations, and national security depend on exceptional data safeguarding, and strategic leaders are looking to their technical counterparts—chief information officers (CIOs) and chief information security officers (CISOs)—to put the necessary people, policies, and solutions in place to achieve cyber resilience goals. It's challenging to manage often siloed, threat-centric, and complex standalone security solutions as ransomware threats evolve. Data security and data management has been similarly disjointed and inconsistent in seeing, preventing, and stopping cybercriminals from extorting large payouts.

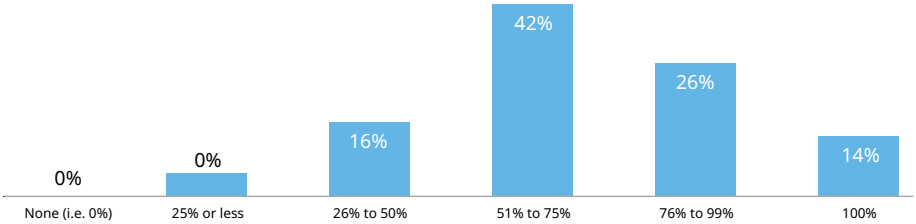
More than half of organizations victimized by a successful ransomware attack admit to having paid a ransom to regain access to data, application or systems,[3] reports Enterprise Strategy Group (ESG). Moreover, the average ransom payment was up 71% during the first five months of 2022, approaching the unprecedented $1 million mark,[4] according to Palo Alto Networks. Yet even organizations that pay ransom discover it doesn't guarantee data recovery. Only 1 in 7, or 14% of organizations surveyed for the ESG report, indicated they got all their data back post payment.[5]

Have organizations paid ransoms resulting from successful attacks?



" **More than half** of organizations that have been victimized by a successful ransomware attack at some point admit to having paid a ransom to regain access to data, applications, or systems."

Percentage of data recovered after paying ransom.



[2] Forrester. "Business Resilience Is No Longer Optional," Stephanie Balaouras, 12 May 2020.
[3] Enterprise Strategy Group. "The Long Road Ahead to Ransomware Preparedness," March 2022.
[4] Palo Alto Networks. "2022 Unit 42 Ransomware Threat Report," June 7, 2022.
[5] Enterprise Strategy Group. "The Long Road Ahead to Ransomware Preparedness," March 2022.

Technical leaders can work smarter within existing budgets (and avoid new security budget asks) to address proliferating ransomware by teaming up with industry-leading, data-first companies. Together they can address ransomware protection and recovery through cyber resilience engineering-focused controls and processes. NIST defines resilience engineering as an emerging discipline applied in conjunction with systems security engineering to develop survivable, trustworthy secure systems.

Although data drives digital business and government, there needs to be more focus on data in security strategies. The Data Security Alliance puts data at the center to unify security with management strategies and improve outcomes.

> ""Today's non-stop and increasingly sophisticated cyber threats require an all-hands-on-deck approach. It's not the responsibility of one vendor to solve all cybersecurity challenges, it takes a village to fight the bad guys."
>
> – **Sanjay Poonen,** CEO and president, Cohesity

Ransomware is rising

Ransomware is expected to cause over $30 billion in global damages this year. An attack on a business is predicted every 2 seconds by 2031, up from every 11 seconds in 2022.[6] Why does it get harder each year to contain and stop this growing threat? Organizations striving for cyber resilience confront numerous challenges. Several are listed below.

People challenges

Humans aren't perfect. The most prevalent ransomware attacks happen through phishing emails and stolen credentials—the latter making up 40% of ransomware attacks.[7]

- Organizations lack the time and resources to properly educate and train employees and partners in security awareness to counter attacks (e.g., phishing).
- IT and security roles are siloed. Almost one third of SecOps respondents (31%) recently surveyed believe collaboration with IT is not strong, with 9% of those respondents calling it "weak."[8]

Organizational and process challenges

Although ransomware dwell times have been steadily dropping, studies report lag times between 21 and 11 days still exist. Security workflows and information-sharing processes ill-designed to counter these threats are a primary culprit. For example:

- Patching vulnerable applications and systems is time consuming and costly.
- Legacy systems that can help with defense, such as backup, require IT specialists.
- Attack surfaces are wider, making data everywhere harder to protect.
- Disaster recovery "runbooks" are common, but most don't account for the complexities of ransomware response and recovery.

[6] Cybersecurity Ventures. "Ransomware will strike every 2 seconds by 2031." January 3, 2023.
[7] Verizon. "Data Breach Investigations Report," 2022.
[8] Censuswide for Cohesity survey, June 2022.

Technology challenges

The Global DataSphere is expected to more than double in size from 2022 to 2026 with enterprise organizations driving most of the data growth, according to IDC.[9] Many technology environments, particularly those with a patchwork of best-of-breed products and disparate security and infrastructure platforms, weren't architectured to handle data on-premises, in the cloud, and at the edge at such scale. With data exploding—so many different types, in so many different locations—these environments are buckling under the pressure of ransomware.

- Existing solutions aren't well integrated, resulting in persistent complexity.
- Cloud and hybrid environments introduce new challenges in protecting and recovering from ransomware.
- Economic uncertainty is prompting questions about whether to increase security investments or optimize what currently exists.
- Most technologies aren't able to leverage the efficiency and scaling artificial intelligence and machine learning (AI/ML) help enable.

All hands on deck

Among the prominent signs that ransomware isn't abating and shouldn't be taken lightly, the U.S. National Institute of Standards and Technology (NIST) recently updated "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach" with a focus on cyber resiliency engineering. This emerging specialty systems engineering discipline applied in conjunction with systems security engineering develops survivable, trustworthy secure systems.

Cyber resiliency engineering is geared toward architecting, designing, developing, implementing, maintaining, and sustaining the trustworthiness of systems. They can then anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises that use or are enabled by cyber resources. From a risk management perspective, cyber resiliency is intended to help reduce the mission, business, organizational, enterprise, or sector risk of depending on cyber resources.

This can be a relief to organizations since the talent shortage is impacting collaboration between IT and security teams. In a recent report, 77% of IT decision-makers and 78% of SecOps professionals agreed it's having an impact.[10] This lack of coordination between IT and SecOps, the same report highlights, is leading to respondents believing their organization is more exposed to cyber threats. All respondents particularly fear:

- Loss of data (42%)
- Business disruption (42%)
- Customers will take their business elsewhere (40%)
- Finger-pointing and team blame should mistakes occur (35%)
- Paying ransomware (32%)
- Talent from both teams (IT and SecOps) will be fired (30%).

[9] IDC. "Worldwide IDC Global DataSphere Forecast, 2022–2026," May 2022.

[10] Censuswide for Cohesity survey, June 2022.

One part of the NIST cybersecurity resilience framework approach is a set of guidelines, standards, and best practices designed to help organizations manage and reduce cybersecurity risks. The framework provides a common language and a systematic approach to managing cybersecurity risks across different sectors and industries. It's based on the core functions of identify, protect, detect, respond and recover. These functions help organizations understand their cybersecurity risks, protect their assets, detect and respond to cybersecurity incidents, and recover from them in a timely manner.

At the highest level, a robust cyber resilience framework encompasses two key concepts: withstanding an attack and recovering from an attack.

Modern thinking: Center your security strategy on data

In Formula 1 racing, the car is the focus. How do you maximize its speed? How do you optimize its performance? How do you do it all safely? In business and government, data is the Formula 1 car. It's driving digital business and government. But data is not at the forefront of many security and management strategies. There's too much focus on infrastructure and systems, particularly across clouds.

The mission of the Data Security Alliance is centered on data, specifically to unify data management and data security behind cyber resiliency. The vision is to deliver industry-changing technical integrations and architectures as well as robust data and security collaboration, best practices, and thought leadership around data.

This vision differs from, but is complementary to, that of the Cloud Security Alliance (CSA), which is dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. Organizations are struggling with securing and tracking sensitive data in the cloud. Only 4% believe all their cloud data is sufficiently secured, over a quarter of organizations aren't tracking regulated data, nearly a third aren't tracking confidential or internal data, and 45% aren't tracking unclassified data, according to the State of Cloud Data Security research report by the CSA.

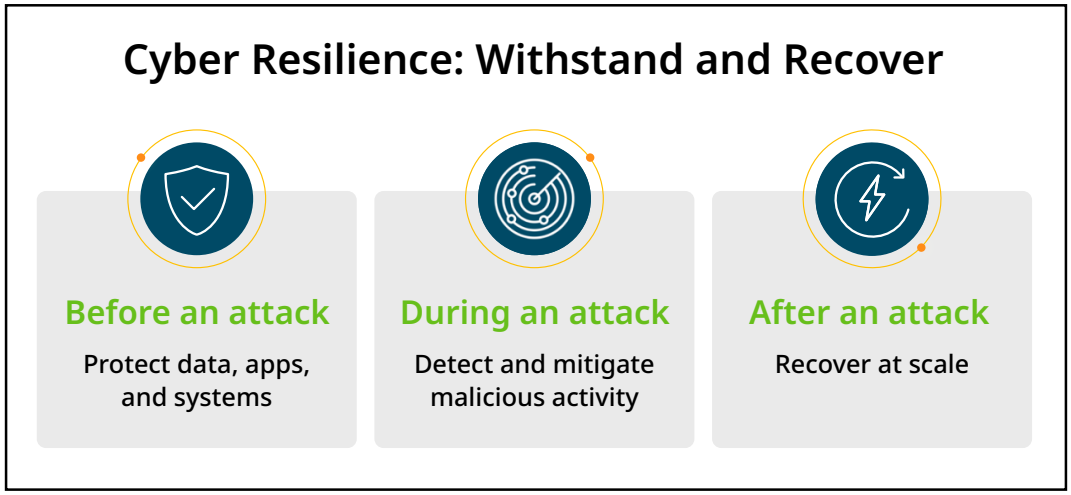
The Data Security Alliance integrations and best practices will help organizations weave a cohesive set of processes and controls together to minimize the impact of cyber incidents. It also will increase organizational confidence in data stored everywhere—across public, private, and hybrid computing environments.

> "Cyber resiliency starts with getting the basics right, especially around your data. It's essential to understand where your sensitive data lives, what it is, who has access to it, and the risks associated. As a Security community, we need to place data at the center of our security strategy."
>
> – **Tyler Young,** BigID CISO

With data at the center of your cybersecurity strategy, your organization can positively:

- Reduce risk
- Drive agility
- Improve resiliency

You can achieve these benefits by proactively staying ahead of threats throughout the distinct phases of the ransomware journey:



Six cyber resilience best practices

When data is your focus, and leading security and data management partners are working as your architectural pit crew, your organization can have the cyber resilience foundation you need for anything. Below find six best practices for building your cyber resilient environment. (They complement the NIST cyber resilience best practices, which include a range of actions—from developing and implementing policies and procedures to regularly testing and updating incident response plans to establishing partnerships with other organizations to share threat intelligence).

1. Stay vigilant: Continuously monitor your security posture

The threat landscape is constantly evolving and organizations struggle to keep up due to limited budgets and resources, resorting to time-consuming manual exporting of data to several spreadsheets and continuously chasing threats rather than anticipating potential attacks or compromises. This leads to unfocused decision-making and inadequate strategic planning at every level of the organization. NIST

advises teams to develop and implement cybersecurity policies and procedures. Yet cybersecurity teams need new approaches to proactively address and manage current and emerging cyber risks. They must more fully understand where to prioritize their efforts, how to objectively measure progress over time, and when to effectively communicate results to stakeholders to mitigate attacks and dramatically reduce the number of incidents they need to respond to quickly.

Preventing cyberattacks means not only implementing the NIST-recommended employee cybersecurity training and awareness, plus implementing access controls and monitoring systems. It also requires full visibility into assets and exposures, extensive context into potential security threats, and clear metrics to objectively measure cyber risk. Organizations that can anticipate cyberattacks and communicate those risks for decision support will be best positioned to defend against emerging threats.

Data is especially challenging, as it's the most dynamic of all assets. Sensitive data grows and proliferates rapidly, and organizations need to know the data's location, its classification, how it's accessed, and other factors to understand its risk and protection needs.

The most successful cyber resiliency plans begin with an assessment. Teams need to not only review cyber strengths, weaknesses, opportunities, and threats but also identify the solutions required to build cybersecurity defenses and respond effectively to cyberattacks. (See the checklist at the end of the document for specifics.) Industry-leading threat experience, coupled with expertise about intelligent data security and data management solutions working onsite and across clouds, help organizations develop more effective cyber readiness programs.

2. Never trust, always verify: Architect with Zero Trust principles

The legacy model of security, centering on the idea of trust but verify is no longer valid in today's business and government environments—because perimeters no longer exist. Best practices for digital business require architecting with Zero Trust principles, including never trust always verify and least privilege to ensure you know who's accessing what information and when.

Compromised sensitive information hurts business reputations and advantage as well as government agility and situational awareness. That's why it's now critical to safeguard every identity—human or machine—across the widest range of devices and environments. A digital identity is the body of information about an individual, organization, or electronic device that exists online. With so many enterprises undergoing digital transformation, a surge of identities with unprecedented access to data has emerged. Today, the number of identities with privileged access and control across multiple devices far outnumbers the number of users, putting the onus on your security team to better safeguard a wider attack surface. Moreover, the use of multiple legacy tools to manage identity security for your data estate creates complexity and inefficiencies that hackers can exploit. Comprehensive role-based access controls coupled with never trust, always verify policies better protect your organization from ransomware and insider threats.

Because data now lives everywhere, your organization must find a way to comprehensively unify data management and data security—from endpoints and cloud workloads; from backup to production; and from identity to data—to stop bad actors. A data-first approach to attack prevention—complementary to NIST's recommendation to implement encryption and other security controls to protect data—requires visibility and control of all your data. With complete visibility, you can minimize data risk across all your cloud and on-prem systems for data security, privacy, compliance, and governance.

3. Know your data: Deepen intelligence

NIST recommends regularly testing and updating incident response plans and conducting regular vulnerability assessments and penetration testing. Doing so is critical because rapid malware detection helps you gain the confidence to refuse to pay ransom. Beyond this guidance for production systems, you can uncover cyber exposures and blind spots within your production environment by running on-demand and automated scans on production data and backup snapshots against known vulnerabilities. These scans also make it easy to assess your risk posture and meet stringent security and compliance requirements without impacting your production environment.

Scan production and backup snaps to assess health and recoverability. Verify backups to ensure no known vulnerabilities get reinjected into the production environment during restores. All of these provide deeper intelligence and a global view of all cyber exposures within your production environment so you can address them before a bad actor exploits them.

Artificial intelligence and machine learning (AI/ML)-powered data classification also accelerates ransomware protection, detection, and response capabilities, keeping you one step ahead of cybercriminals. You can continuously discover sensitive and regulated data, including personal identifiable information (PII), protected health information (PHI), and PCI data, and reduce false positives with ML-based data classification. This data intelligence helps inform the security posture and keep dependent security controls, such as Data Loss Prevention (DLP), up to date as well as helps response teams understand the impact of a ransomware attack or cyber incident.

4. Boost collaboration: Make cyber resilience a team sport

Resilience requires preparation, responsiveness, toughness, and adaptability. In the modern connected world, security leaders must leverage an architecture and processes that are inclusive of on-prem, cloud, and SaaS environments while implementing security processes focused on business continuity. SecOps programs must leverage solutions and processes that deliver prevention to stop adversary actions when possible—but also detect and respond as necessary when prevention isn't possible.

Resiliency is achieved by stopping adversaries before they accomplish their objectives in a target environment. Organizations must implement a strong understanding of their individual threat landscape and attack vectors to support resilience efforts. Both are attainable through understanding refined threat intelligence and attack surfaces, but must be specific to the organization and not generalized. Finally, processes that support business resiliency are a critical security program outcome. Incident response planning and partnerships are key to supporting both the business and your security program's viability.

NIST recommends establishing partnerships and collaborations with other organizations to share threat intelligence and best practices. When you re-engineer and adapt your processes to lean into IT/SecOps collaboration, your organization has a better chance of defending your data against ransomware attackers. Your business leaders will also sleep better at night.

Discover and invest in trusted security products that work seamlessly together to counter ransomware. These include security information and event management (SIEM) and security orchestration, automation and response (SOAR) solutions that accelerate time to discovery, investigation, and remediation of ransomware attacks. Pre-built, integrated workflows that are extensible help enable SecOps to augment

them for automated incident response and unified operations across security, IT, and networking teams. In addition, make sure pre-built integrations are possible using a secure software development kit (SDK) and customizable management APIs that give you the flexibility to operate your environment the way you want to fight cybercrime.

5. Consolidate and simplify: Leverage a modern data security and management platform

Scale and compatibility are additional keys to combating ransomware attacks. Because cyber resilience requires collaboration, it's important to take advantage of an extensible, modern data security and data management platform with an API-rich and API-first architecture that works across locations and covers the widest range of data sources. By consolidating many data management functions in a single platform, you simplify operations. Instead of making copies of data and moving them around, you also have a solution that lets you reuse data in-place, bringing value-add applications to data for routine and more challenging tasks—from virus scanning and data masking to analyzing file audit logs and classifying data. Moreover, a single, extensible platform cuts down your data footprint and the surface available for ransomware to attack.

6. Gain speed and confidence: Integrate backup infrastructure with security infrastructure and operations

Data security and data management complexities can't be solved alone, particularly when a breach happens. To get back to operational readiness as soon as possible—within recovery time and recovery point objectives (RTOs/RPOs)—requires an integrated approach where backup is not siloed but an intrinsic part of security infrastructure and operations.

Organizations investing in data security and data management will benefit from tightly integrated solutions that cover the full spectrum of security frameworks. A popular one is the incident response cycle, or PICERL, from the SANS Institute:

- **Preparation** – Assessments, plans, education, identity management, etc.
- **Identification** – Awareness monitoring, early detection, etc.
- **Containment** – Notification, backups, forensics, etc.
- **Eradication** – Restores, root-cause analysis, malware removal, etc.
- **Recovery** – Vulnerability scanning, return to operations, baseline, etc.
- **Lessons Learned** – Reporting, procedure updates, etc.

Carefully considered integrations give you and your team the speed and confidence to counter attacks all the way from planning to recovery—even using automated AI/ML to detect potential cyberattacks by alerting teams about unusual patterns surrounding your data. When a breach happens, you also have a way to recover clean data—to any point in time and location—that has been vulnerability scanned to avoid system reinfection, reducing downtime.

Cyber resilience capabilities checklist

Key automated and comprehensive features effectively counter ransomware, including the following capabilities:

	Requirements	Key Capabilities
Cybersecurity (withstand)	Strategy	• Advisory, implementation and managed security services to build your cybersecurity defenses and respond effectively to cyberattacks
	Identity management and security	• A platform and services for workforce identity and customer identity • Protection of any identity—human or machine—across the widest range of devices and environments
	Visibility and exposure management	• The ability to inventory all IT assets—hardware, software, applications, data • A platform to assess risk across the attack surface—in the cloud or on premises, from IT to OT and beyond, giving you the visibility and insight needed to prioritize and validate risk posture • Data security posture management (DSPM) to enable a strong data discovery, classification, and intelligence practice—knowing where data lives, what it is, who has access to it, its workflow and risk
	Extended detection and response (XDR)	• A cloud-native solution with XDR capabilities for the entire security infrastructure, speeding detection, response, and recovery • A way to initiate workflows to restore data and workloads when a ransomware attack occurs
	Next-gen Security information and event management (SIEM)	• A solution to defend against advanced threats in today's complex hybrid environments using the most advanced analytics and built on a scalable, flexible cloud-native architecture
	Security orchestration, automation and response (SOAR)	• Automation and flexibility that allows you to manage cyber and ransomware attacks more quickly
	Actionable threat intelligence	• Comprehensive intelligence and expertise, driving dynamic solutions that help you develop more effective programs and instill confidence in your cyber readiness • Visibility and control for all sensitive and critical data to understand and minimize data risk across the cloud and on-prem with a data-first approach—for data security, privacy, compliance, and governance
	Full-stack observability	• An extensible data platform that delivers unified security, full-stack observability, and custom applications
	Zero Trust (ZT) / Perimeter and endpoint protection	• A way to secure the most critical areas of enterprise risk—endpoints, cloud workloads, identity, and data—to stay ahead of adversaries and stop breaches
	Forensics	• Security solutions that help you determine root causes and ransomware signatures for possible prosecution prior to ransomware eradication

	Requirements	Key Capabilities
Cyber resilience (recover)	Backup & recovery	• Comprehensive cyber threat protection, ML-based anomaly detection, rapid ransomware recovery, and hybrid cloud mobility • Data immutability • Data isolation: Separating data is physically and logically for an additional layer of security • Zero Trust principles (such as multifactor authentication [MFA]) • Quorum: Requires multiple people to authorize administrative or configuration changes
	Vulnerability scanning and restoration	• Clean room, staging back into service, additional recoveries of data and/or configurations, application team sign off, possibly data center operations to move systems between environments, security, and network to ensure accessibility to the new operational area
	Threat protection	• Detection of malware and indicators of compromise (IOCs) with ML-based threat intelligence and scanning to identify threats in backup data
	Security integrations	• APIs, SDKs, and integrations to security operations and security controls to accelerate incident response and leverage existing controls and processes

By putting data at the center of your cyber resilience strategy, you can be sure you're architecting for maximum protection and optimal recovery. The Data Security Alliance encourages IT and business decision makers to learn more about cyber resilience at www.cohesity.com/company/data-security-alliance.

About the Data Security Alliance

The mission of the Data Security Alliance is the security and protection of data. The Alliance accomplishes this by holistically unifying data security and management with cybersecurity to improve cyber resiliency, delivering critical technical integrations and architectures, best practices, and thought leadership around a common focus. The Data Security Alliance combines best-in-class solutions from industry leading cybersecurity and services companies with exceptional data security and management expertise from Cohesity. Data Security Alliance members include: BigID, Cisco, Cohesity, CrowdStrike, CyberArk, Okta, Palo Alto Networks, Securonix, Splunk, Tenable, Mandiant, Qualys, Netskope, ServiceNow, Zscaler and PwC.

2000046-001-EN 5-2023