TECHNICAL VALIDATION

Architect and Execute Resilience with Fenix24

Ensure a fast recovery from ransomware attacks

By Justin Boyer, Senior Validation Analyst
Omdia

MAY 2026

Contents

Introduction

This Technical Validation by Omdia details our examination of Fenix24 and its cyber recovery services and software. We examined how Fenix24 helps organizations recover from ransomware attacks and architect recovery and resilience before an attack happens, with the help of its Argos99 software.

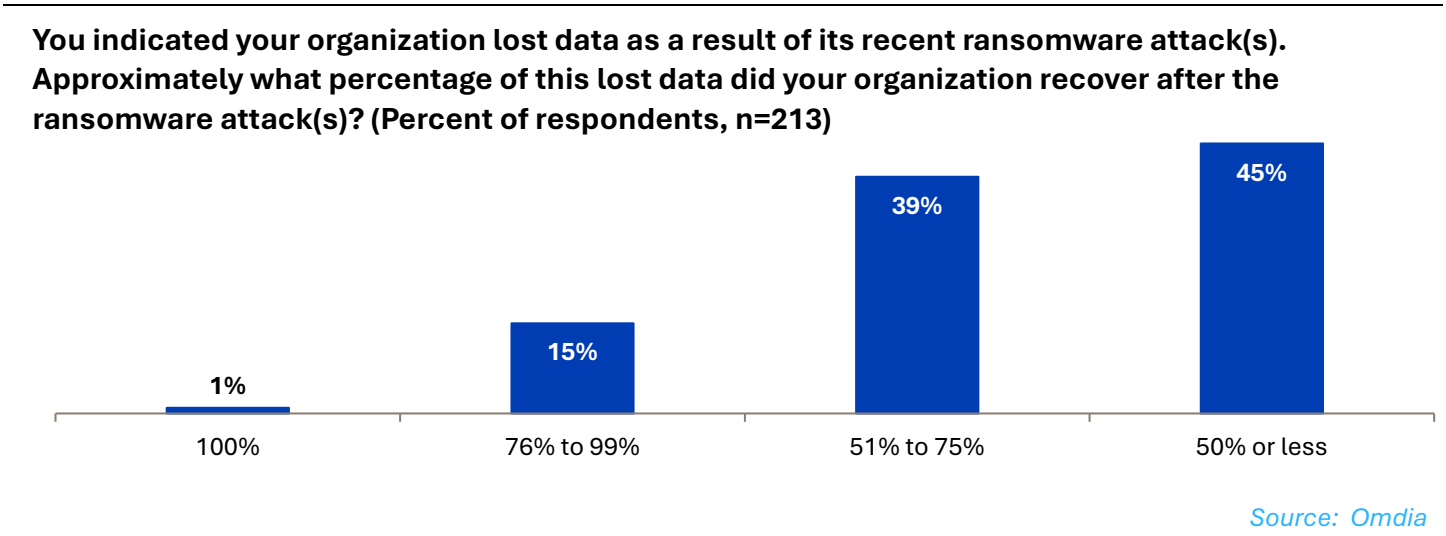
Cyber recovery challenges

Many organizations focus on prevention of cyberattacks, but recovery can be left behind in the process. Organizations spend their budget on firewalls, endpoint protection, and identity controls, all tools used to prevent ransomware attacks. However, building cyber resiliency, the ability to recover quickly from a ransomware attack, is often underfunded and under-supported. Additionally, the rise of powerful AI models, such as Mythos, has given attackers the tools they need to find vulnerabilities anywhere. It's no longer realistic or practical to pretend breaches can't happen. Organizations must switch to a different mindset: what happens **when** an attack occurs, not if.

Traditional disaster recovery planning and compliance frameworks were designed around physical disasters (fire, flood, hardware failure, human error). As a result, organizations enter a ransomware event with recovery architectures that were never designed to withstand or rapidly recover from a contemporary ransomware attack, leading to the destruction of data backups and critical infrastructure.

Omdia research has uncovered several concerns organizations have regarding ransomware attacks and recovery. More than half (57%) of survey respondents indicated that their organizations have experienced attempted ransomware attacks at least weekly, with 22% experiencing them daily.[1] When ransomware attacks are successful, they are incredibly costly, indicated by 55% of respondents reporting that successful attacks cost their organizations at least $1m. A further 45% indicated that, when their organization fell victim to a ransomware attack, they could only retrieve 50% or less of their data (see **Figure 1**).

Figure 1. Most organizations do not get all their data back from ransomware



Source: Omdia

[1] Source: Omdia Research Report, *The Ransomware Reality: Cyber Reslience, Data Resilience, and Data Protection*, November 2025. All Omdia research references and charts in this Technical Validation have been taken from this report.

Unfortunately, even those organizations that have not been hit with a successful ransomware attack do not feel comfortable in their ability to protect their data if one does occur. The majority (81%) of survey respondents reported that they are concerned that their data protection copies could become infected or corrupted by ransomware attacks. When backups and critical infrastructure are not protected ahead of time, recovery from successful attacks will cost organizations much more.

Organizations may spend money on tools and technology designed to help prevent or recover from ransomware attacks. However, if they lack an understanding of what happens during ransomware attacks and do not plan accordingly, they will suffer from permanent data loss; interruption of business operations; and slow, incomplete, and expensive recovery periods.

Fenix24

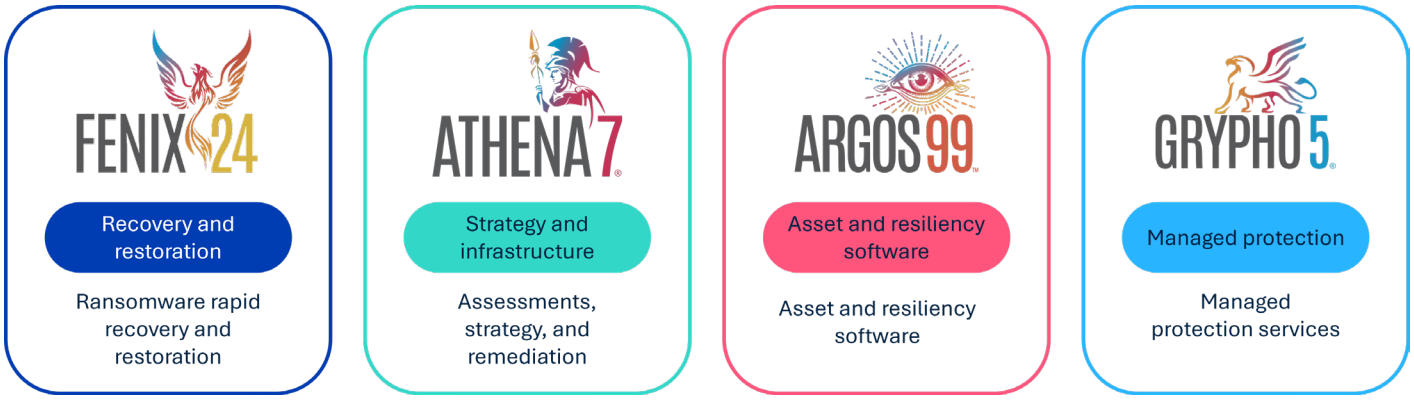
Fenix24 is an industry-leading post-ransomware recovery company that organizations turn to when hit by a cyberattack such as ransomware. Having worked through more than 500 breach events, Fenix24 has accumulated a deep understanding of how threat actors behave: what they target, how they move laterally, and how they maximize destruction of both backups and infrastructure. Through this experience, Fenix24 has also built expertise in the resiliency posture an organization needs to have in place to recover from an attack quickly.

Using advanced techniques, Fenix24 prioritizes accelerating recovery through teamwork with forensics experts, automation, and processes. Doing so, the company works to get organizations back up and running as quickly as possible without a focus on billable hours.

Instead of only focusing on recovery efforts for clients, Fenix24 worked to reverse engineer ransomware attack patterns to define what organizations need to ensure a path for assured rapid recovery. Therefore, in addition to "wartime" recovery during a crisis, Fenix24 takes the lessons learned and applies them to "peacetime," working to architect recovery strategies for organizations before they get hit with a successful attack, focusing on resiliency and recoverability.

To operationalize these insights at scale, Fenix24 developed the Argos99 platform to help assist in recovery. Argos99, which began as a set of bespoke tools that Fenix24's recovery teams used in the field, has now developed into an enterprise-grade software solution. It ingests and cross-correlates data from over 60 sources—endpoint detection and response (EDR), firewalls, cloud and on-premises directories, and telemetry—to create a reliable, real-time view of an organization's assets, servers, policies, domains, virtual machines, and business-critical applications with all their dependencies. This critical information provides the foundation for rapid recovery in wartime, and genuine preparation in peacetime.

Figure 2. Fenix24 services from recovery



Source: Fenix24 and Omdia

Omdia Technical Validation

Omdia reviewed through detailed briefings and remote demonstrations how Fenix24's approach to cyber resilience and recovery enables organizations to recover from ransomware attacks quickly and completely. We specifically examined its outcome-focused approach to recovery, its ability to architect recovery before an attack happens, and the Argos99 software platform that underpins all its services.

Outcome-focused recovery from ransomware attacks

Omdia reviewed Fenix24's philosophy on fast recovery from ransomware attacks. We examined how Fenix24's methodology leads to efficient operations and restoration with a focus on client outcomes, not billable hours.

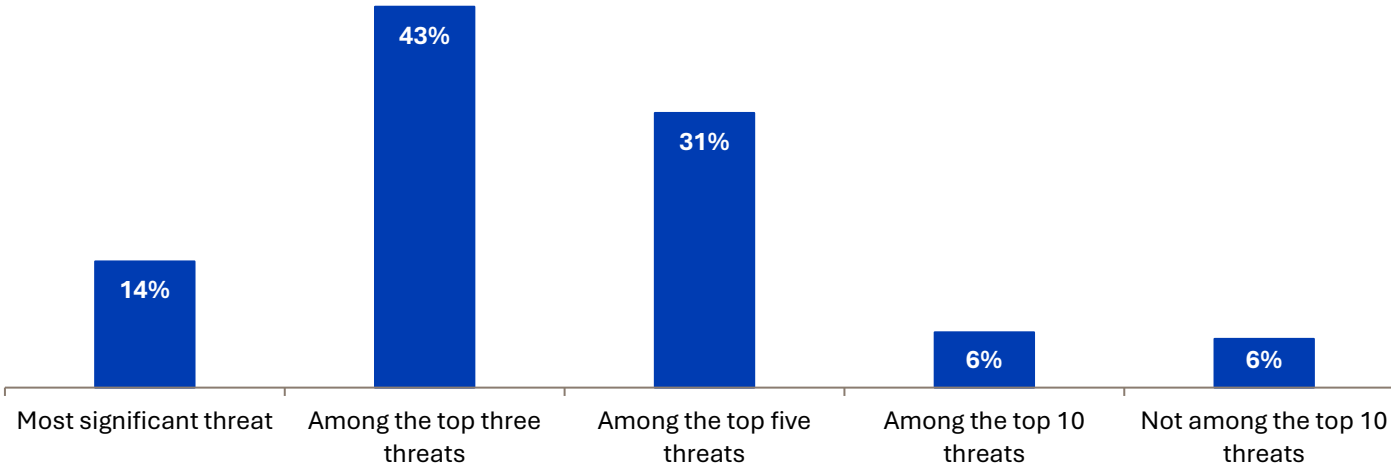
Omdia analysis

Ransomware attacks can be devastating to their victims. They do not only encrypt data; they destroy it, if possible. They target backups to prevent organizations from recovering. They damage or destroy critical infrastructure that organizations need to function properly, such as Active Directory, essentially bringing business operations to a halt. Without the ability to bring critical infrastructure and applications back online, organizations potentially lose millions of dollars in revenue in addition to the cost of recovery itself.

Because of the potentially catastrophic damage ransomware can cause, organizations are rightly concerned about the threat it poses. According to Omdia research, 88% of surveyed respondents indicated that ransomware is at least a top five threat to the health of their organization, including 57% that said ransomware is at least a top three concern for them (see **Figure 3**). However, despite this focus, ransomware attacks still succeed, and organizations may find themselves in need of fast help when they do.

Figure 3. Organizations see ransomware as a serious threat

As an overall threat to the health of your organization compared with all other potential risks, where would you rank ransomware? (Percent of respondents, N=400)



Source: Omdia

Fenix24 helps organizations quickly recover from ransomware attacks by concentrating on three critical philosophies.

- **Focus on recovery.** Traditional recovery methods often feature a staff augmentation model, where recovery services personnel travel to the ransomware victim's site to begin recovering systems and data. Traditional staff augmentation increases customer costs and forces them to wait until help arrives to start recovery efforts. Fenix24 focuses on recovery first, not billable hours. By establishing remote access to the environment as soon as possible, Fenix24's team can begin working to recover data immediately and can leverage Argos99 to accelerate asset and dependency mapping, which are required for a faster recovery.
- **Brownfield recovery.** Fenix24 embraces brownfield recovery, facilitating a safe recovery within the customer's existing environment. This rapid recovery model leverages Argos99 to immediately understand and map the environment to mitigate risk while facilitating a significantly faster return to operations. The Fenix24 rapid recovery model contrasts with many services that recommend organizations deploy new infrastructure, software, and devices (greenfield) instead of the faster path of managing technical risk while resuming rapid recovery with the brownfield model. Using the existing infrastructure, Fenix24 can recover much faster than traditional methods.
- **Experienced and thorough recovery process.** Fenix24 works quickly to lock down the environment, evict pervasive threat actors, prevent further compromise, and stop the attack progression. It then works to identify business-critical applications and the required core infrastructure for the organization to operate—such as Active Directory, hypervisors, and Domain Name System (DNS)—and determine dependencies so critical business functions can be reestablished and the organization can resume business operations as quickly as possible. Fenix24 works closely with forensics teams to accelerate forensic capture and focus systematically on accelerating recovery of critical applications with laser

focus while establishing a "safe date" from which data restoration can begin. A "follow the sun" model, with teams across multiple time zones, ensures 24/7 recovery operations.

Through a tight focus on accessing the customer's environment and beginning recovery efforts as soon as possible, Fenix24 provides the skill and expertise organizations can depend on to fight the threat of ransomware.

Why this matters

Ransomware has become a scourge on multiple industries. Its rise has led to many organizations losing their data, losing access to critical applications, and suffering potentially millions of dollars in damages. When an attack is successful, organizations are challenged to find the skills and expertise necessary to recover their environment as quickly and cost-effectively as possible.

Omdia validated that Fenix24's approach to ransomware recovery helps organizations quickly recover from successful ransomware attacks. Instead of using traditional staff augmentation models that slow down recovery, Fenix24's recovery specialists prioritize gaining quick remote access to the customers' environment so data recovery can begin immediately. Fenix24 works to restore critical applications and infrastructure within the customer's existing environment, instead of requiring the installation of new appliances, working to recover core infrastructure, such as Active Directory, hypervisors, and DNS, while also restoring critical business applications.

Any delay in recovery efforts after a successful ransomware attack can potentially mean hundreds of thousands, or even millions, of dollars in losses due to business disruptions. Fenix24 maintains a tight focus on getting its customers' critical systems and applications restored as quickly as possible. This fast recovery helps organizations reduce downtime and restore business operations, helping to mitigate the financial impact from a successful attack.

Architect recovery before an attack

Omdia validated Fenix24's approach to building resiliency into its customers' infrastructure to ensure fast recovery in the event of a successful ransomware attack.

Omdia analysis

Despite the concern organizations have for the threat of ransomware, many businesses primarily focus on prevention. They purchase appliances and software geared to prevent malicious actors from gaining access to their environment, train employees to look for phishing emails, and invest in risk and vulnerability management programs to plug security holes. However, many organizations underinvest in recovery in the case of a successful attack. They do not take the time to ensure that, if an attack is successful, they can quickly restore operations without paying the ransom and minimize losses. Fenix24 applies the lessons from hundreds of live ransomware recovery engagements to help organizations architect recovery solutions that will hold up against attacks occurring in the wild—not theoretical scenarios.

- **True immutability.** Many organizations believe they have immutable backups (i.e., backups incapable of being altered by anyone for a defined period of time), only to discover during an attack that those backups are vulnerable. Fenix24 ensures that data backups are genuinely immutable.

- **Preventing backup integrity issues.** Fenix24 ensures backup integrity is handled in a way that makes backups usable when it matters, which requires significant backup testing, manual restore exercises, and architecting sufficient storage for forensics and rebuilding, as well as the bandwidth necessary for data transfer back into production systems.
- **Asset and dependency mapping.** Argos99 maps out assets and their dependencies, enabling a clear, sequenced plan for restoring critical functions in their entirety. While organizations may know their business-critical applications, they may also lack visibility into the dependencies, databases, and infrastructure required to bring any particular application back online. Attempting to construct that map in the chaos of an active breach adds days—and sometimes weeks—to business interruption. And a lack of understanding those assets and dependencies in peacetime means the organization cannot architect a path to assured recoverability within defined recovery time and point objectives (RTOs/RPOs). Organizations cannot protect what they do not understand.

Why this matters

Organizations often work hard to prevent successful ransomware attacks. However, many do not put forth the effort required to recover from an attack if one is successful. Omdia research shows a distinct lack of confidence in the safety of the very data backups organizations need to recover, with 81% of survey respondents reporting that they are at least somewhat concerned that their data backups are vulnerable to a ransomware attack. If recovery is not planned for or carefully architected, organizations face potentially catastrophic damage to their systems.

Omdia examined Fenix24's methodology to see how it can help organizations make the necessary changes to ensure a fast recovery from a successful attack. Fenix24's Athena7 service works during "peacetime," before an attack happens, to architect a recovery plan. It does this by ensuring data backup immutability, preventing data backup integrity issues, and mapping out dependencies with Argos99. This increased understanding of its customers' infrastructure and business applications enables Fenix24 to ensure a safe and fast recovery.

Ransomware attacks are happening on a constant basis. While protective measures are important to prevent ransomware from getting in, sufficient attention must be given to how an organization will recover if the worst happens. With the help of Fenix24, organizations can architect recovery and have confidence that, if a successful attack occurs, they can recover quickly and greatly reduce business disruption and the resulting lost revenue.

Argos99 platform

Omdia validated how Fenix24 uses its Argos99 platform to provide the foundation for recovery architecture and planning.

Omdia analysis

IT systems architecture can be challenging to track. Changes happen often, and documentation is not always up to date. If a successful attack occurs, organizations need to know exactly how they interact and which depend on each other to effectively recover without unnecessary business disruption. Argos99 is the platform Fenix24 developed to give organizations rapid, comprehensive visibility into their technology estate—with the

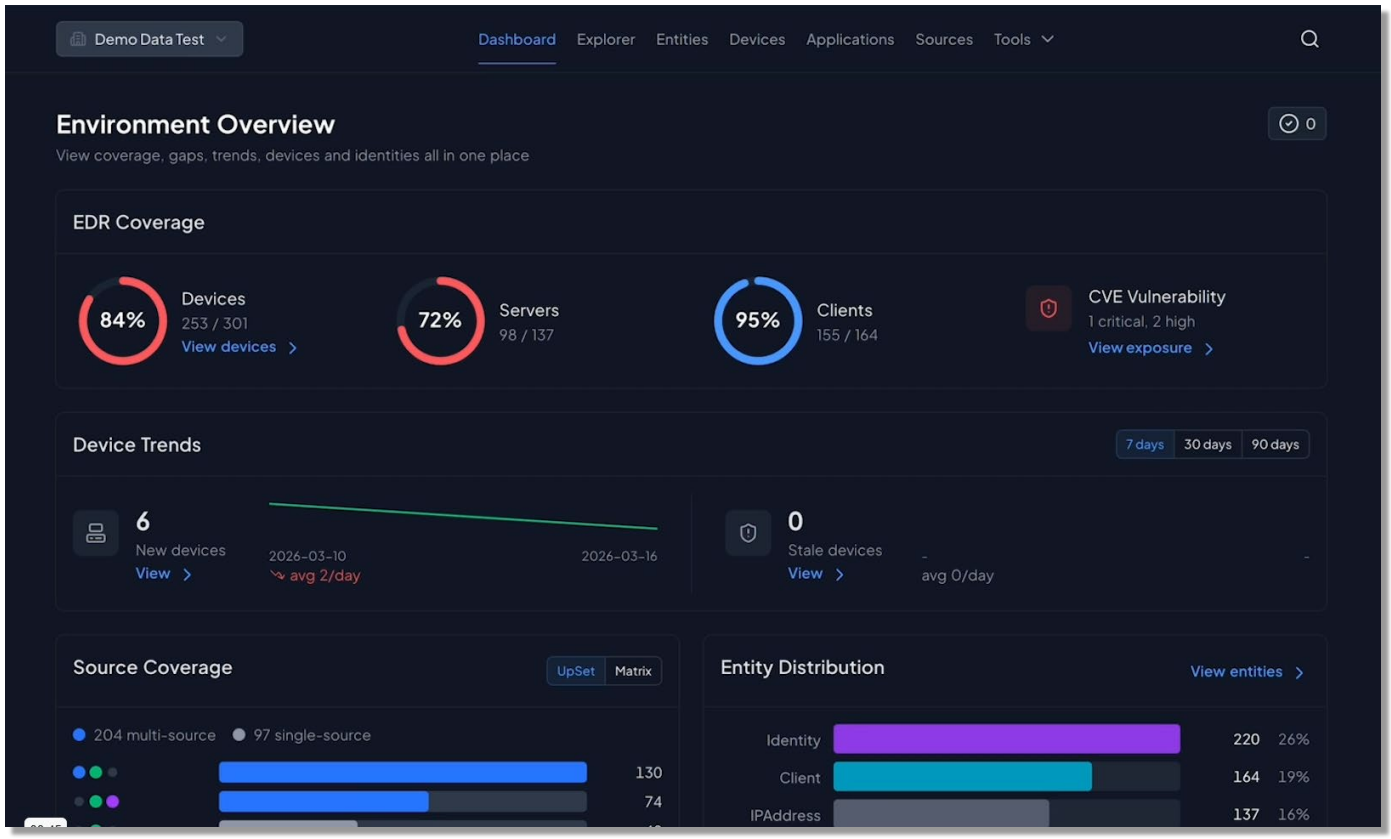
full context needed to leverage that data for rapid recovery in wartime or to architect true resiliency in peacetime.

Argos99 is an enterprise-grade SaaS platform built on a simple premise: Organizations cannot recover what they cannot see. Asset Intelligence—a continuous, correlated view of every asset, identity, configuration, and data repository across the environment—is the platform's foundation. Application Dependency Mapping is built on top of that foundation, turning raw asset data into actionable recovery intelligence. Originally built as bespoke internal tooling to support Fenix24's own recovery operations, Argos99 has since been developed into the enterprise-quality software available today as a fully standalone product, independent of any Fenix24 services engagement.

By ingesting and cross-correlating data from over 60 sources—spanning EDR, firewalls, cloud and on-premises directories, and telemetry—Argos99 delivers a transparent, reliable, real-time view of what assets exist in an organization, how they are configured and protected, and how they depend on each other. That dependency intelligence is the foundation for answering the questions that matter when planning for business continuity and disaster recovery (BC/DR): What breaks if this goes down, what's the blast radius, and what needs to come back online first?

Omdia reviewed several key use cases for Argos99. In its current enterprise-grade form, it can provide several benefits across the organization. We began by examining the Argos99 Asset Intelligence Dashboard. This dashboard provides an overview of the environment, including key data that can help with higher-level decision making. The data presented comes from live telemetry, not based on documentation or what people think is happening. In our demonstration, Argos99 was pulling data from Active Directory, CrowdStrike, and VMware vCenter. Using this dashboard, we were able to quickly ascertain EDR coverage gaps showing all endpoints not protected by CrowdStrike. We next viewed common vulnerabilities and exposures (CVE) data, showing CVE vulnerabilities along with how long these vulnerabilities have been in the environment (see **Figure 4**).

Figure 4. Asset Intelligence Dashboard



Source: Omdia

We next reviewed the asset intelligence capabilities by navigating to the Assets view and clicking on a specific asset. In the Asset view, multiple sources are brought together into one record for a complete picture of an asset and its makeup. Argos99 correlates data from various sources and organizes it by entities, such as identity, servers, IP addresses, network interfaces, and hypervisors. The data can be from native attributes and user-defined attributes such as tags. In this view, we also saw a graphical representation of connections, installed software, and whether the data is part of a larger application architecture (see **Figure 5**).

Figure 5. Server connections shown as a graph

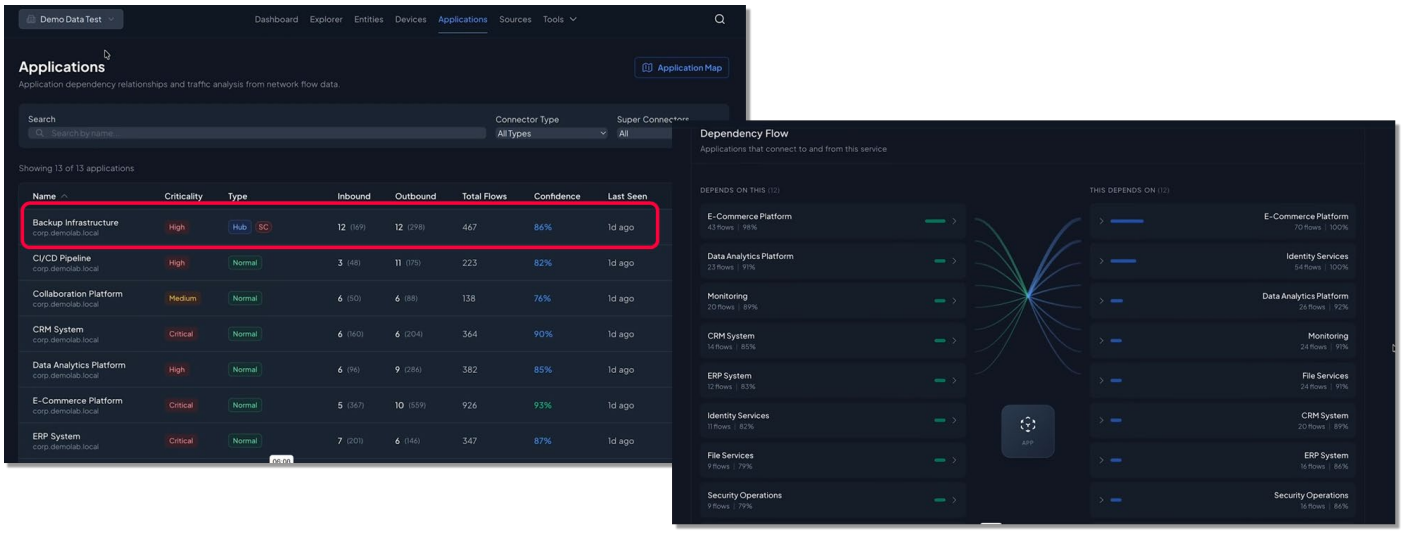
Source: Omdia

Argos99 builds a comprehensive repository of business applications. These create a clear view of complete business applications, their criticality, and the various assets that comprise them. Argos99 separates itself from conventional asset and security posture tools by showing organizations not only what exists but also what breaks when something goes down and what has to come back first. This view is critical in recovery planning to ensure all dependencies for an application can be brought back online together in a reasonable timeframe.

Omdia reviewed the application view where we could see which applications depend on other applications to function properly. Organizations can use application grouping and dependency mapping to ensure the chain of critical functions are brought back completely in the event of a successful attack. Application dependency mapping also lays the groundwork for organizations to properly architect an effective recovery plan to ensure applications are brought back online within an acceptable time frame. Knowing recovery order and identifying "hub" applications that others depend on means organizations can define realistic RTOs and RPOs, not just aspirational ones.

In our scenario, we navigated to the application view, where all applications are listed along with key attributes, such as criticality, inbound and outbound dependencies, and whether they stand alone or if other applications depend on them to function (known as “hub” applications in Argos99). We clicked on backup infrastructure, where we were presented with the detail page for the backup infrastructure application. This view also featured a detailed listing of inbound and outbound dependencies, enabling us to continue drilling down into different assets to find more details about the overall environment (see **Figure 6**).

Figure 6. Application dependencies



Source: Omdia

Why this matters

Without a complete picture of their data, applications, and server infrastructure, organizations cannot hope to recover quickly from a successful attack. Unfortunately, such data is often siloed, outdated, and suffering from conflicting sources. If a successful ransomware attack strikes, a poor or outdated view of the environment greatly slows down recovery efforts, costing the organization more in downtime and potential revenue losses. Organizations usually know their critical applications, but they may not know the order in which those applications need to come back online—and that gap is where recovery plans fail.

Omdia validated how Argos99 helps Fenix24 to better understand an organization's overall asset inventory, along with dependencies and applications. This information feeds into both "wartime" recovery efforts after an attack succeeds and "peacetime" efforts to help plan a recovery. Argos99 fills a critical need of providing an accurate, real-time picture of all assets and their dependencies, based on telemetry data from various sources, not on potentially outdated documentation. That picture directly answers the questions a recovery plan depends on: What applications are critical, what do they rely on, and in what order does everything need to come back? Together, these capabilities enable organizations to define recovery order with confidence, set realistic RTOs and RPOs, and walk into a BC/DR planning exercise knowing the plan reflects how the environment works, not how it was documented.

No recovery effort can succeed without a clear view of the environment. Fenix24 has created Argos99 to provide such a view, in keeping with its brownfield recovery model, to help both before and after an attack. Argos99 creates the solid foundation organizations need to safely and quickly recover from ransomware attacks.

Conclusion

Traditional disaster recovery planning and compliance frameworks were designed around physical disasters (fire, flood, hardware failure, human error). Organizations tend to focus on firewalls, endpoint protection, and identity controls, all tools used to prevent ransomware attacks. As a result, organizations may enter a ransomware event with recovery architectures that were never designed to withstand or rapidly recover from a contemporary ransomware attack. According to Omdia research, over half (55%) of surveyed organizations reported successful ransomware attacks costing them over $1m. Despite the high cost of a successful attack, building cyber resiliency (i.e., the ability to recover quickly from a ransomware attack) is often underfunded and under-supported. If organizations lack an understanding of what happens during ransomware attacks and do not plan accordingly, they may suffer from permanent data loss; interruption of business operations; and slow, incomplete, and expensive recovery periods.

Omdia validated that Fenix24 offers robust and efficient recovery services when organizations are hit by a ransomware attack. The company acts quickly to get into the environment within the first few hours and works to quickly recover data in an outcome-focused strategy. It also helps organizations prepare to recover by helping them architect a recovery plan using Argos99 and proprietary techniques. By combining its outcome-based approach with automation, hardware, and software, Fenix24 guarantees recovery within defined timelines and data recovery objectives.

If your organization needs to build a recovery plan and infrastructure that works while ensuring strong support, skill, and expertise when the worst-case scenario happens, we recommend that you seriously consider engaging with Fenix24.

Get in touch: www.omdia.com askananalyst@omdia.com