WHITEPAPER

The Journey to XDR: Practical Questions to Ask

LevelBlue

Everyone in cybersecurity has heard the hype about extended detection and response (XDR), and many companies are interested in exploring this approach. But what should organizations be focused on as they research the growing number of solutions in the market?

This whitepaper looks at the problems XDR addresses and discusses what security practitioners should consider as they plan their journey.

What is XDR?

Extended detection and response, or XDR, is a holistic approach to threat detection and response. It tackles the long-standing problem of siloed security by using different technologies to collect, correlate, and centralize network, endpoint, and cloud telemetry from across the attack surface.

For years, vendors have promised to address the need for better visibility and better data sharing between tools. With the move toward edge computing, and as businesses expand their digital footprints, security and operational complexities increase. Hybrid architectures, the accelerating adoption of cloud computing, a vanishing network perimeter, and a growing remote workforce are just some of the challenges organizations face when trying to secure their IT environments.

XDR extends the capabilities of the security information and event management (SIEM) platform. It improves how data is collected and correlated, and it gives that data context. With XDR, security practitioners get the expanded visibility, advanced security analytics, continually updated threat intelligence, and automated or orchestrated detection and response capabilities they need to detect and respond to threats in real time.

The XDR market is still emerging. Opinions vary on where the technology came from. But focusing on how XDR came together is not as important as understanding the outcomes it drives: more efficient IT operations and the ability to identify, hunt, and remediate threats before they become security incidents.

Focusing on how XDR came together is not as important as understanding its outcomes: more efficient operations and the ability to identify, hunt, and remediate threats before they become security incidents.

Two Approaches

Some vendors are entering the XDR market through acquisition. They are driving toward single-vendor, or native, solutions that offer a unified suite of security tools from one vendor on a centralized management platform. Other vendors are choosing not to provide all components of their XDR solutions in-house. Instead, they offer open solutions with one central management console that integrates with multiple third-party security products.

The Need to Evolve Threat Detection and Response

To understand why security practitioners should care about XDR, it is important to understand the ongoing security and operational challenges it helps them address. XDR is essentially a convergence of the

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 027WP 09-2024

capabilities of different security products. This convergence has been driven by the need for:

- Increased telemetry from multiple sources and better, centralized visibility across an increasingly diverse and distributed attack surface
- Advanced analytics and machine learning to sort through the influx of data and provide context
- Better use of automation and orchestration to enable faster and more efficient threat detection and response

Why XDR . . . and Why Now?

Expand Telemetry from Multiple Sources

→ Get increased visibility and information gathering

Boost Threat Intelligence and Improve Security Analytics

→ Improve time to detect and the accuracy of detections

Automate and Orchestrate Workflows

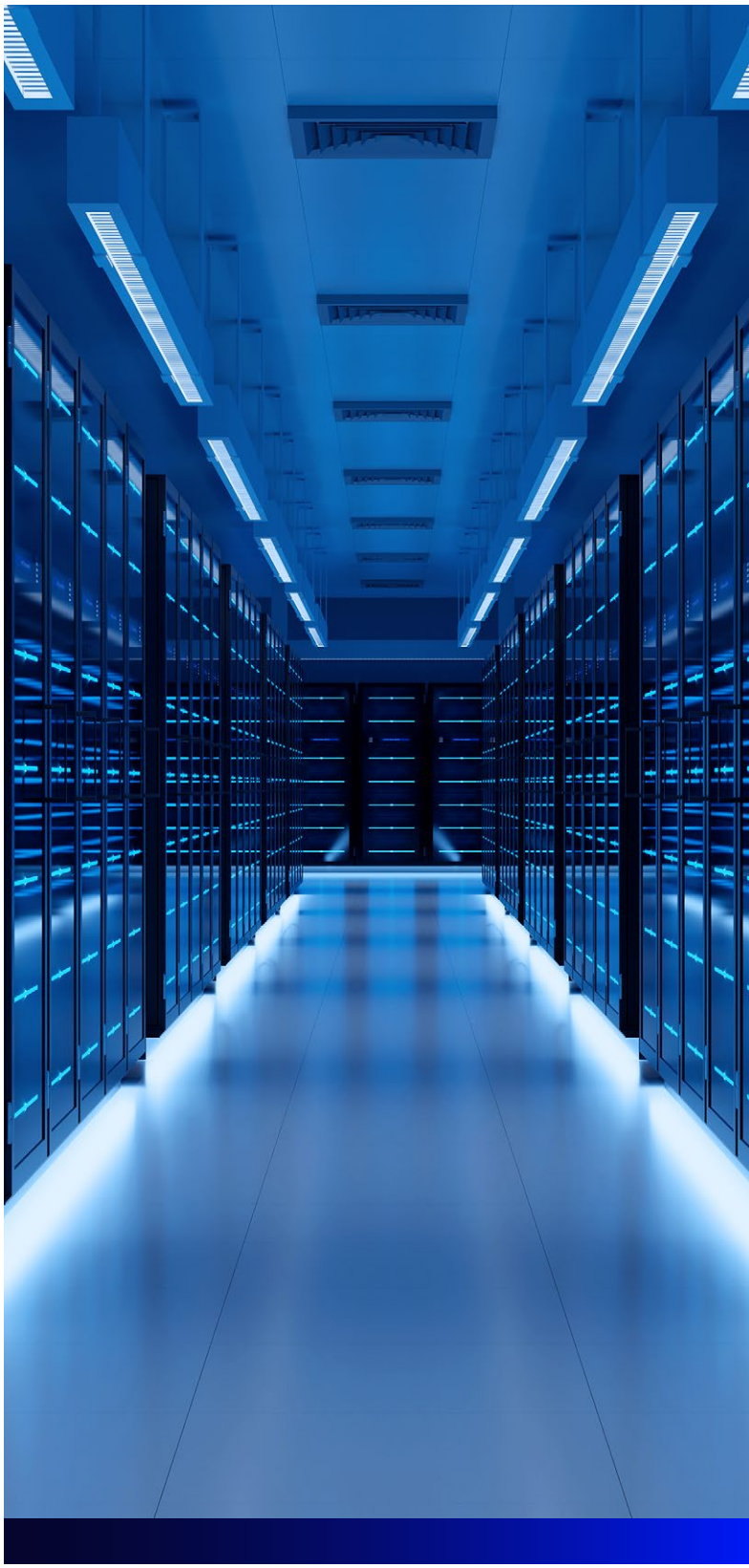
→ Accelerate response speed and recovery time

XDR Outcomes

Better Visibility and More Context

Effective threat detection and response requires visibility across the IT infrastructure because, as cybersecurity professionals like to say, "You can't protect what you can't see."

Security practitioners need to be able to monitor their entire attack surface—including across endpoints, network infrastructure, cloud workloads, applications, and more—to connect the dots and understand when an attack is occurring in their



© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 027WP 09-2024

environment. Without context, ongoing attacks can be missed. One phishing email can lead to an infected endpoint. That can lead to an attacker moving laterally within the network to establish persistence. Once the hacker has established a beachhead in your network, they can eventually deliver a payload, whether that be encryption for ransomware, spying, data exfiltration, or another objective.

XDR provides the security practitioner with visibility in the form of robust telemetry. This is gathered by different security tools from across the organization's network, endpoints, servers, cloud workloads, and email. The security team can see all this data in one centralized view, so they can respond to threats quickly and effectively.

Breaking Down the Silos

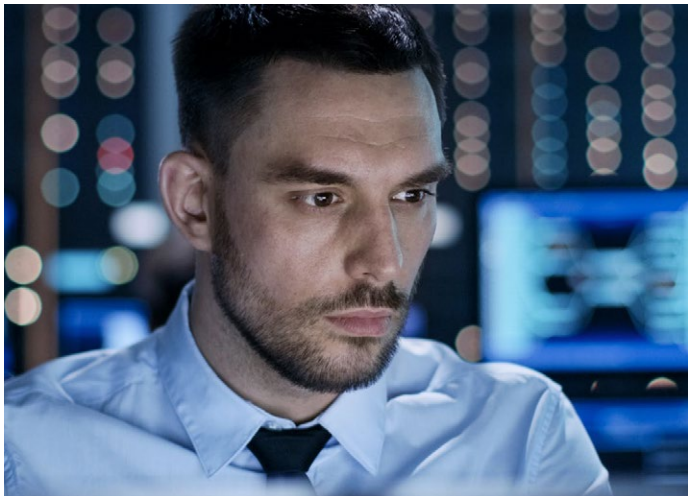
The lack of communication between the many different security tools found in the typical security operations center (SOC) has long made the life of the security practitioner difficult. And while the capabilities found in XDR have been available in some of these tools, it has been up to the security practitioner to integrate these tools in-house and then look across multiple dashboards to understand when attacks are underway.

XDR addresses this problem of siloed information by bringing together the different tools in a centralized platform for the end user. With XDR, the security practitioner can view events, investigate alarms, and respond to threats from a single pane of glass. And regardless of whether an XDR solution is the result of a native or open integration, it is the vendor that takes on the responsibility of integrating the products and systems—not the security practitioner.

Threat Intelligence Provides More Context

Through advanced analytics and machine learning that assesses and correlates the data, XDR can profile behaviors to detect anomalies and predictively identify advanced threats, such as fileless malware, zero-day attacks, and polymorphic attacks.

XDR solutions use continuously updated threat intelligence and enhanced security analytics to increase the accuracy of detections and improve time to detect. This includes mapping correlations and detections to the MITRE ATT&CK® framework,



which is a knowledge base of adversary tactics and techniques. The threat intelligence provides additional context for the data and helps the security practitioner triage responses.

Workflows for Automation and Orchestration

With so much data coming into the SOC, manual processes for validation and correlation are a drain on resources and increase the chance of true threats going undetected. While some analysis is automated on the backend, security practitioners require better use of automation to help them sort and prioritize information.

XDR simplifies day-to-day operations by allowing the security practitioner to automate select workflows and processes. This includes investigating slow network connections, reviewing logs for unusual activity on missing or destroyed devices, or identifying devices.

With this automation, XDR speeds up investigations and helps facilitate faster, more scalable incident response. For example, it provides automated root-cause analysis, so the security practitioner has the context and relevant information they need to take the appropriate response actions. And with XDR, orchestrated response actions can be activated by the security practitioner across all tools with just the click of a button.

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 027WP 09-2024

Planning and Preparation

For the security leader seeking to lighten the load for their security teams and evolve their organization's current threat detection and response capabilities, XDR's promise is immensely appealing: greater efficiency in security operations and more agile security. But there are already multiple offerings available in this emerging market, so where should the security leader start?

Understand Desired Outcomes

Decision-makers should begin by understanding the specific objectives they seek for their organization. Based on those, they can evaluate how an XDR vendor's background can help them meet these objectives.

For example, if an organization is in a highly regulated industry, such as healthcare, manufacturing, or financial services, it will have strict reporting and compliance requirements. This organization would want an XDR vendor with strong SIEM capabilities. Why? So the organization will have the deep analytics and strong data log collection and long-term data retention capabilities it requires.

Network architecture and use cases will also drive considerations. For example, an organization that has an IT estate focused heavily on Internet of Things (IoT) devices will not have the same visibility requirements as the organization that has few IoT devices but many endpoints. On the other hand, XDR vendors coming from the endpoint detection and response (EDR) space are likely to be weaker on analytics but stronger at providing actionable response on the endpoint. Organizations with large numbers of endpoints that need to be monitored (and potentially restored in the event of an attack) will want to partner with these vendors.

Determining the Best Approach

As discussed earlier, vendors are implementing XDR in one of two ways: either by integrating security tools from one vendor's portfolio (commonly referred to as a "native" platform), or by utilizing third-party integrations (commonly referred to as an "open" platform).

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 027WP 09-2024

The organization that purchases a native XDR solution, in theory, will not have to implement and manage integrations with technologies from other vendors. However, it will have to rip and replace what it has in its technology stack to lock in with a single preferred security provider—typically a costly and complex undertaking. And while the simplicity of this approach is attractive, it may preclude the organization from deploying more innovative solutions from other vendors as they emerge in the market.

Since vendor-agnostic, or open, solutions use third-party integrations, customers can deploy them without having to replace tools they have already invested in. An important factor to consider with these solutions is whether the vendor has a large enough ecosystem for integration.

Organizations that deploy tools from multiple vendors are probably better off choosing an open platform or working with a managed security service provider to leverage those investments.

Key Considerations

As organizations assess who to partner with for their XDR implementation, the following items are key:

- Current security stack
- IT and network infrastructure, including future plans
- Potential gaps in current detection and response capabilities
- Loyalty to current vendors
- End-of-life contracts
- Vendor roadmaps for XDR
- Level of experience and expertise in the organization
- Regulatory / reporting requirements

Current Controls

Security practitioners should evaluate the organization's current security technologies and understand where they have gaps in their detection and response capabilities that will need to be addressed either through deployment of additional tools or by making changes to the current stack.

Since the organization's network is its attack surface, it will be critical for security leaders not only to review their current network roadmap but also to understand how their network and infrastructure will change over the next three to five years (for example with the rollout of an edge initiative). If the organization anticipates an increase in the number of endpoints on the network, then it should focus more on vendors with strong EDR capabilities. Alternatively, if the organization prioritizes advanced analytics, broad visibility into the network, and automated workflows, then it should look to vendors with a strong SIEM component.

If there is an incentive to reduce the number of vendors in the organization's technology stack, it will make sense for the organization to look at native platforms and lock in with a particular vendor. However, if the organization has recently onboarded a vendor (for its endpoint security needs, as an example), it may not be feasible to switch to a different vendor's native platform. This is because ripping out the current endpoint solution and implementing a new tool will likely involve considerable time, training, and expense. In this case, the organization may be better off choosing an open platform or working with a managed security service provider so it does not have to rip and replace.

If the organization has contracts that are reaching end-of-life, this would be a good time to evaluate making changes. Alternatively, the organization may be in a situation where the security practitioners want to make a change but are not able to do so in the immediate future because they're locked into a contract for several more years and instead will need to create a roadmap for that change.

Loyalty to current providers will also be a factor. Does the organization intend to stay with its current SIEM platform? Does its current endpoint security provider check all the boxes? As organizations evaluate XDR solutions, many will remain loyal to their existing SIEM and EDR vendors. A customer that is already using an effective EDR solution is unlikely to switch to a product its security practitioners are not familiar with. However, if vendors fail to deliver on their promised outcomes, then organizations will be more willing to make changes.

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 027WP 09-2024

Vendor Roadmaps Are Key

Take care to review vendor roadmaps for integration, including scale and scope. Ascertain whether vendors are planning any integrations. If they are, understand how they plan to achieve them. Whether a vendor approaches XDR through acquisition (i.e., as a native platform) or through partnerships (i.e., as an open platform), integration is key.

If the vendor is partnering for its integrations, understand what that roadmap looks like in terms of the scale and scope of the integrations. Determine the vendor's openness for integration with other vendors, not only for XDR capabilities, but also for other security controls (for example, vulnerability management).

For native XDR vendors, review acquisition roadmaps to understand which capabilities have truly been integrated. When vendors bring together multiple platforms through acquisition, integrations are not always complete. Often, not all features are ported over, and some capabilities are prioritized over others.

Even if a vendor has acquired other technologies and is now positioning its platform as native, the platform will not be truly native until the vendor's engineers have fully integrated the new technology into it. And stitching together different technologies is not a trivial task. For example, the SIEM provider that touts XDR capabilities should be able to demonstrate that its platform has the advanced analytical capabilities, machine learning, and workflow capabilities to process correlations and alarms from multiple sources.

Further, these capabilities should be integrated to the point that it is a seamless experience for the SOC analyst. Can the analyst view data from multiple sources from a single dashboard and act with the click of a button? Or will they need to toggle between multiple dashboards to access different features?

In-House Capabilities vs. Managed Security Services

Understanding what expertise and experience the organization has available in-house is also key. Whether the organization opts for an open platform or a native platform, it will need skilled security professionals to research, deploy, and manage a complex solution that can be challenging to roll out. Not only will staff need to know how to perform the integration during the deployment, but they'll also need to know how to fine-tune the platform and handle its day-to-day management.

The organization may have a SOC in place to deploy and manage its XDR, but if not, this capability will need to be outsourced. While an in-house SOC gives an organization greater control and allows it to tailor security operations to its specific needs, this may not be an option. The annual costs of building and staffing a full-time SOC are not trivial. According to a report from Forrester Research, SOCs can easily cost more than $1 million USD and take 8–12 months to build.[1]

If the organization does not have the requisite expertise and experience in-house, then it may find significant value in working with a managed security service provider (MSSP) or managed detection and response (MDR) provider. These providers can help ask the right questions, perform an assessment to identify gaps in current detection and response capabilities, and help the organization work through how to roadmap from its existing technology stack to an XDR implementation.

If the organization does have the in-house capabilities to handle day-to-day management of the solution and does not plan to work with an MSSP or MDR provider, consider retaining the services of a consulting or professional services company or investing in a product support services retainer. This will ensure the SOC team has access to on-call support when troubleshooting issues.

1 Recruiting The Right Managed Security Service Providers, Forrester Research, Jan 2021, p. 10

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 027WP 09-2024

Next Steps

Assess the Current Security Stack

Review the organization's platforms and technologies to identify where XDR capabilities currently exist and where there are gaps, both in feature sets and in integrations within the organization's current portfolio. Look at the current network roadmap, and also understand how the organization's network will change over the next 3–5 years.

Determine Internal Expertise

Understand the experience and expertise of the organization's current security team. Analyze whether it has the knowledge and experience to deploy and manage the platform.

If the organization does not have these capabilities in-house, consider an MSSP or a consulting or professional services company. These providers offer different levels of support, ranging from initial deployment and fine-tuning of the platform to day-to-day management, or a combination thereof.

Evaluate Vendors

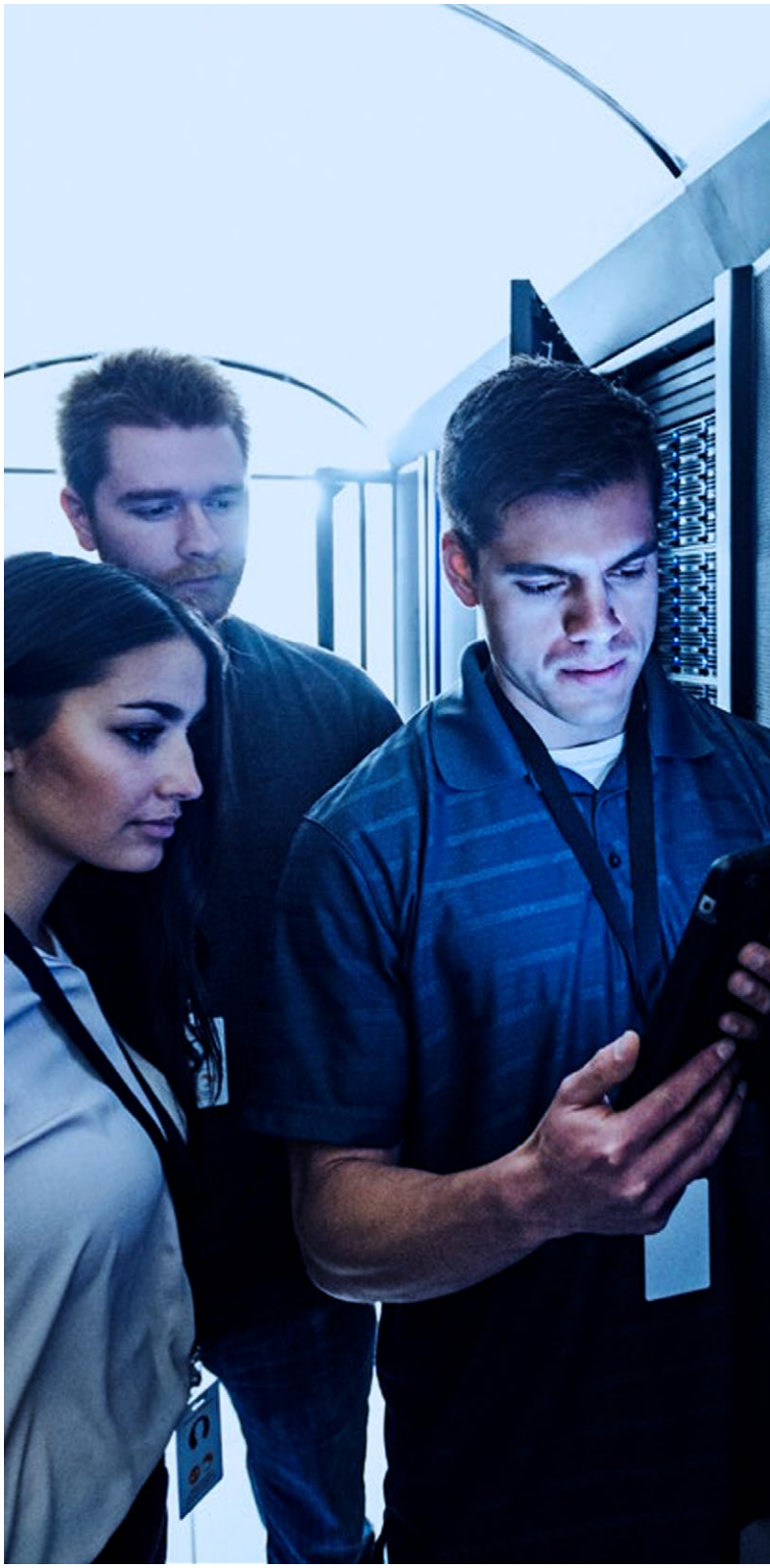
Perform detailed research on the vendors and their capabilities. Either conduct online research or set up inquiries with analysts from research firms.

Conclusion

The need for organizations to defend their data has never been higher, and that need will only intensify. According to the 2023 Cybersecurity Almanac, global cybercrime costs are forecast to grow by 15% per year, hitting $10.5 trillion USD per year by 2025. This is up from $3 trillion USD in 2015.[2]

XDR helps organizations fortify their networks by providing better visibility into threats, more context, and automated workflows to facilitate faster and more efficient incident response.

However, while the benefits of this holistic approach to threat detection and response are clear, not all XDR solutions are alike. Before making any investment decisions, security practitioners should consider several key factors, such as organizational objectives and current technology capabilities, to ensure they select the solution that will best suit their needs.



2 https://cybersecurityventures.com/cybersecurity-almanac-2023/

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 027WP 09-2024

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 027WP 09-2024