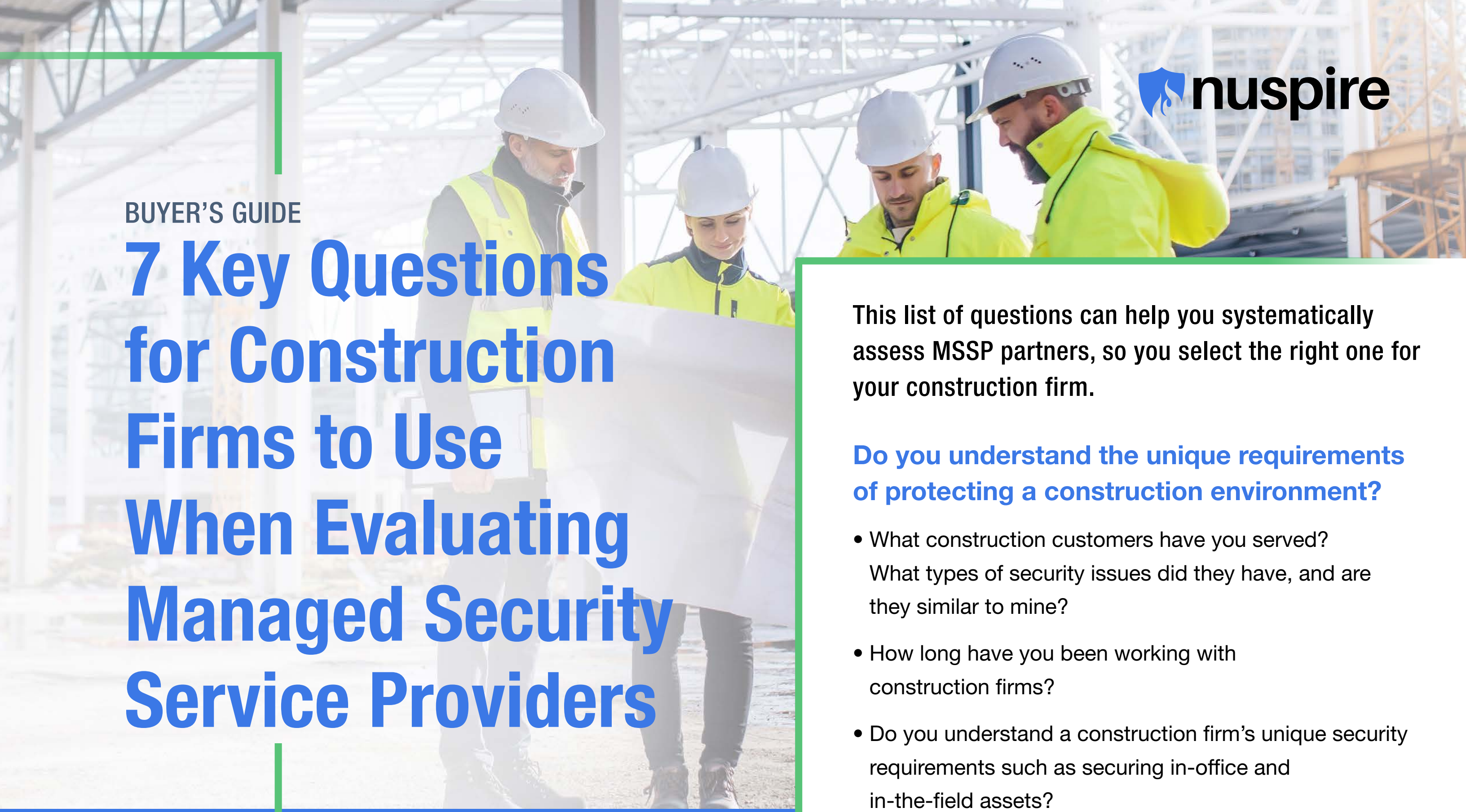

nuspire

BUYER'S GUIDE

7 Key Questions for Construction Firms to Use When Evaluating Managed Security Service Providers

The construction industry's shift to a cloud environment necessitates a new approach to cybersecurity. With the cloud, your data is no longer in one location and more people are accessing it via multiple networks. Cyber attackers know your company deals with a lot of confidential and proprietary information, and that's why the construction industry suffers the most ransomware attacks.

Most construction companies need help protecting their data. Working with a Managed security service provider (MSSP) can be the answer. An MSSP will shoulder the responsibility of securing your defenses while monitoring and managing devices and systems for your firm.

However, with hundreds of MSSPs to choose from, how do you know which one is a good fit for your company? Not all MSSPs are the same, so it's important to be thorough when you're evaluating potential providers.

This list of questions can help you systematically assess MSSP partners, so you select the right one for your construction firm.

Do you understand the unique requirements of protecting a construction environment?

- What construction customers have you served? What types of security issues did they have, and are they similar to mine?
- How long have you been working with construction firms?
- Do you understand a construction firm's unique security requirements such as securing in-office and in-the-field assets?
- How will you make sure the latest patches are installed on potentially vulnerable systems such as our ERP, tool management, CRM and building information modeling (BIM) systems? What is your timeframe for applying the latest patches and updates?
- How do you create a baseline for understanding normal vs. abnormal activity (such as monitoring if someone logs in from an unfamiliar IP address on the weekend)?
- Do you segment the networks of different departments or groups and the IT network from the industrial control systems (ICS) network and industrial demilitarized zones (IDMZ)?
- Do you support identity and access management (IAM), privileged access management (PAM), multi-factor authentication and endpoint detection and response for fixed and mobile devices?
- Will you assess our infrastructure for risks such as insecure Wi-Fi hotspots or USB ports?
- What type of risk assessments do you perform? Can you also include our third-party vendors in the assessment?
- Does your technology support real-time visibility into my construction company's infrastructure so you can quickly remediate existing intruders and block would-be attackers?

How will you customize your approach to my construction environment?

- Do you have a rulebook that will be customized to my construction environment including processes and rules?
- Do you develop an incident response (IR) plan that details how security breaches will be handled?
- Do you create a disaster recovery (DR) plan that will specify what actions to take before, during and after a disaster? Will you document when to shut down and restart our operations in case of a breach?
- Do you run tabletop exercises to test use cases to make sure the team is ready to detect, respond and contain?
- Can dashboards and reports be customized to the needs of different users in my organization?
- Which security framework do you use to protect my systems? Does it include information technology and operational technology network configurations?
- Will your security framework align with my organization's audit requirements? How often do you conduct regular audits?

What is your onboarding process?

- How long will it take you to onboard so you can start supporting my environment?
- How will you help me identify all of our fixed, mobile and Internet of Things (IoT) assets that aren't visible or secured?
- Can you identify gaps in my current security processes and determine where we need to maximize visibility in order to predict potential risk?
- Do you rely on our organization to have a specific technology to integrate with yours, or do I need to replace my current technology stack?
- Do you have a formalized onboarding process that includes a deep discussion about risk, goals, industry and asset inventory? How often is this process repeated and updated?
- How do you incorporate advanced tools like log management, security information and event management (SIEM), use case analytics, behavior analysis, business context and pattern discovery to detect and prioritize threats?
- What types of dashboards, log search, dynamic drill-downs and reports do you offer?

How do you leverage threat intelligence?

- Do you utilize global threat intelligence for correlation and threat discovery from multiple sources?
- How often will your threat detection methods evolve in order to detect when attackers shift tactics?
- Do you provide multiple sources of threat intelligence that are correlated to an actionable step?
- Do you have full visibility of security events and the ability to analyze and investigate each event? How do you correlate and prioritize data?
- Do you have more than one source of threat intelligence?

How do you sift through potential threats and select actionable alerts to send us?

- What type of notification will I receive when there is an alert? What criteria needs to be met in order for you to recommend we act on a threat?
- How long does it take you to respond after an actionable threat is detected?
- Does your security operations center (SOC) team proactively investigate suspicious events without overly relying on system-generated alerts?
- What type of case management and incident tools do you use?
- Do you create customized alerts to reduce false positives based on my business requirements?
- Do you use managed detection and response (MDR) technology to augment your detection and response capabilities?

What is your incident response time?

- What is your process when I have an event that I believe needs to be investigated?
- What is your average time between incident and response?
- Does your SOC have an incident response and forensic team to respond to active malware or known breaches?
- Will you regularly consult with us on new threats, alert trends and how to benefit from their security posture?

Do you deliver 24x7x365 managed security services?

- When are your security analysts available?
- How do you ensure threats are addressed in real-time 24x7?
- How do your security analysts proactively hunt for threats that we may not be aware of?
- Can your security analysts support custom coverage days and times such as 7 p.m. to 7 a.m., weekends only or other models?

How will you protect my endpoints?

- Will you inventory everything that's connected to my network, both internally and externally, including fixed and mobile endpoints and IoT and employee devices?
- Can your technology monitor both endpoints and IoT devices in my environment? How will you monitor traffic that's generated to and from my endpoints?
- How long will it take to identify and register all my endpoints and get them up and running?
- Do you provide detection, response, protection and prevention?