GUIDE

How to get maximum value out of remote access

A buyer's guide to remote access management solutions.

secomea

Introduction

The digital transformation of large-scale manufacturers is happening – and it's one of the most profound changes to the industry in decades.

Across sectors, geographies, and sizes of operation, the main focus for manufacturing managers is the combination of IIoT, Data Analytics and Cloud – the pursuit of flexibility and resilience. Right now, the global manufacturing industry is in the midst of the digitalization wave.

Being digital is about removing reliance on physical presence. Being able to virtually monitor and access manufacturing assets is one of the main drivers of investment in industrial digitalization – and with good reason.

When it comes to downtime every minute counts. To exemplify, one German automotive manufacturer estimated that a minute of downtime cost $22,000*. Yet, manufacturers often rely on external technicians due to increasing line-complexity, costing valuable time in travel and coordination.

Digital leaders mitigate this by being able to remotely monitor and identify irregularities, delegating and managing access to production assets. By investing in remote access management, digital leaders are seeing a decrease in downtime, savings on prescriptive maintenance efforts as well as staff and travel-cost, and much higher returns on their investments than their counterparts.

More than 64%** of manufacturers are still in the early phases of digitalization – and have been so for long. The increasing importance of manufacturing as a part of the global supply-chain has led to manufacturing being the single-largest target for cyber attacks, and naturally decision-makers are proceeding with caution.

With regulatory pressure and an increase in security standards and directives like IEC62443 and NIS-2, it can seem almost impossible to enable OT excellence while being compliant.

In general, there is a need to handle remote access management in a secure and user-friendly way that is fit for manufacturing.

In this guide, we seek to address just that. We want to shed some light on **the best practices in identifying, selecting, and evaluating** remote access management systems.

Happy reading!

*Forbes, 2022 | Unplanned Downtime Costs More Than You Think
**PwC study: Digital Factory Transformation Survey 2022

Table of contents

The case for remote

The vast majority of manufacturers are in the very early stages of digitalization and have not yet realized the benefits of being able to centrally manage data and access of their equipment remotely - from anywhere in the world, at any time. So, before looking into features or point- functionality that solves short-term problems, the underlying issue needs to be addressed. This is the case for remote.

Operating in a changing reality

Equipment lifecycle and maintenance is second nature for most manufacturers, but the latter years have shifted the context of both workforce availability and technical possibilities. Being able to access and manage equipment remotely provides new opportunities... but also new requirements.

Widespread supply chain issues, the long-term effects of a global pandemic, increasing raw material prices, and labor shortage is the reality that most manufacturers are facing. The fabric of how we run production has been impacted – yet the boardroom pressure of cost and quality still stands strong.

To meet this increased pressure, manufacturers have invested in digitalization. Last year alone, more than 1.1 trillion USD* were spent to drive digitalization, with maintenance, performance and quality analytics being the main drivers.

Realizing these benefits all starts with a central **overview** of and **access** to your production equipment – an issue that increases with the size and distribution of facilities. Having the remote advantage lets you address the cost and quality challenges of a modern manufacturer.

*PwC study: Digital Factory Transformation Survey 2022

Challenges:

Prevent downtime

Downtime is the single largest revenue-drainer for manufacturers. Not being able to produce the scheduled volume severely impacts the entire value chain, deferring revenue and undertaking costly repairs.

Lower travel costs

In many cases, remote technicians are needed to solve issues in modern production equipment. With technicians being a scarce resource, time-to-service is often being pushed by extended travel time – and hence cost.

Cybersecurity exposure

With an increasing share of production equipment being digitally connected, manufacturers are exposed to new threats. Managing cybersecurity is a MUST for companies to mitigate the risk of connected equipment.

Technician shortage

The demand for skilled technicians is higher than ever – and supply struggles to meet it. More than two-thirds (68%)* of manufacturers rely on OEMs and technology suppliers more frequently as the level of automation increases.

Remote work

The traditional sequential maintenance is labour-intensive and can sometimes be complicated due to health and safety concerns. Finding a way to enable remote work is needed for better yield of OT.

Making sense of data

Modern manufacturers produce enormous amounts of data on each site, and should strive to collect, process, and analyse the data to drive decisions in daily operations and prevent failures before they occur.

*PMMI Report: Automation Timeline: The Drive Toward 4.0 Connectivity in Packaging and Processing

Enabler

Central control and access to data and equipment.

Being remote is about optimizing

Most manufacturers occasionally have to halt production to conduct maintenance. The average manufacturer experiences 800 hours of downtime each year - but not all downtime hits equally. While planned maintenance can be managed, unplanned downtime severely affects the entire value chain. The companies that succeed in optimizing active technician time and the use of data are the ones that succeed in bringing down the amount of downtime.

Maintenance approach

Having remote access to your manufacturing equipment enables you to collect, process, and analyse data to drive decisions in daily operations and prevent failures before they occur – potentially reducing unplanned downtime by up to 35%.

According to IIOT World*, the average unplanned downtime associated with different maintenance approaches are: “reactive” 8.43%, “planned” 7.96% and “data/monitoring” 5.42%.

*IIOT World, 2018 | The actual cost of downtime in the manufacturing industry

Increasing wrench-time

The ability to effectively identify, deploy, and initiate technicians for maintenance is crucial for ensuring quick issue resolution and lowered costs. Being able to delegate access remotely (even to remote technicians) can remove non-value activities and result in 4 times as much ‘wrench-time.’

According to Forbes**, plant maintenance operates with a wrench-time rate between 18% and 74%. Most average around 20-30%, so there is a huge potential for optimization.

**Forbes, 2022 | Unplanned Downtime Costs More Than You Think

Manufactures effectively optimizing maintenance approach and wrench-time can reap upwards of

5-20%

productivity gains via increased uptime and lowered cost.

Setting the vision

Being able to centrally monitor production across multiple sites, countries and types of equipment are central levers to reap productivity gains.

By mastering the data needed for better corrective and predictive maintenance, manufacturers have the core foundation for ensuring the deployment of the right skills at the right time at the right place. Not being forced to have costly on-site visits lets you utilize a global pool of technicians and ensures that downtime can be addressed as fast as possible.

But enabling remote access to your systems challenges your operation in a new way. Having a solid and cross-functional understanding of what you want to achieve is crucial for alignment. A good way of doing this is to map out your change journey. Understanding where we are, where we wish to be and what we want to have changed is central to delivering value.

1 Where are we today?

How many types of remote solutions do you have?
- per factory
- per Machine Supplier
- per central IT

How do you establish remote access?
- Up to the Machine Supplier
- End-users create it themselves
- End-users ask IT to do it

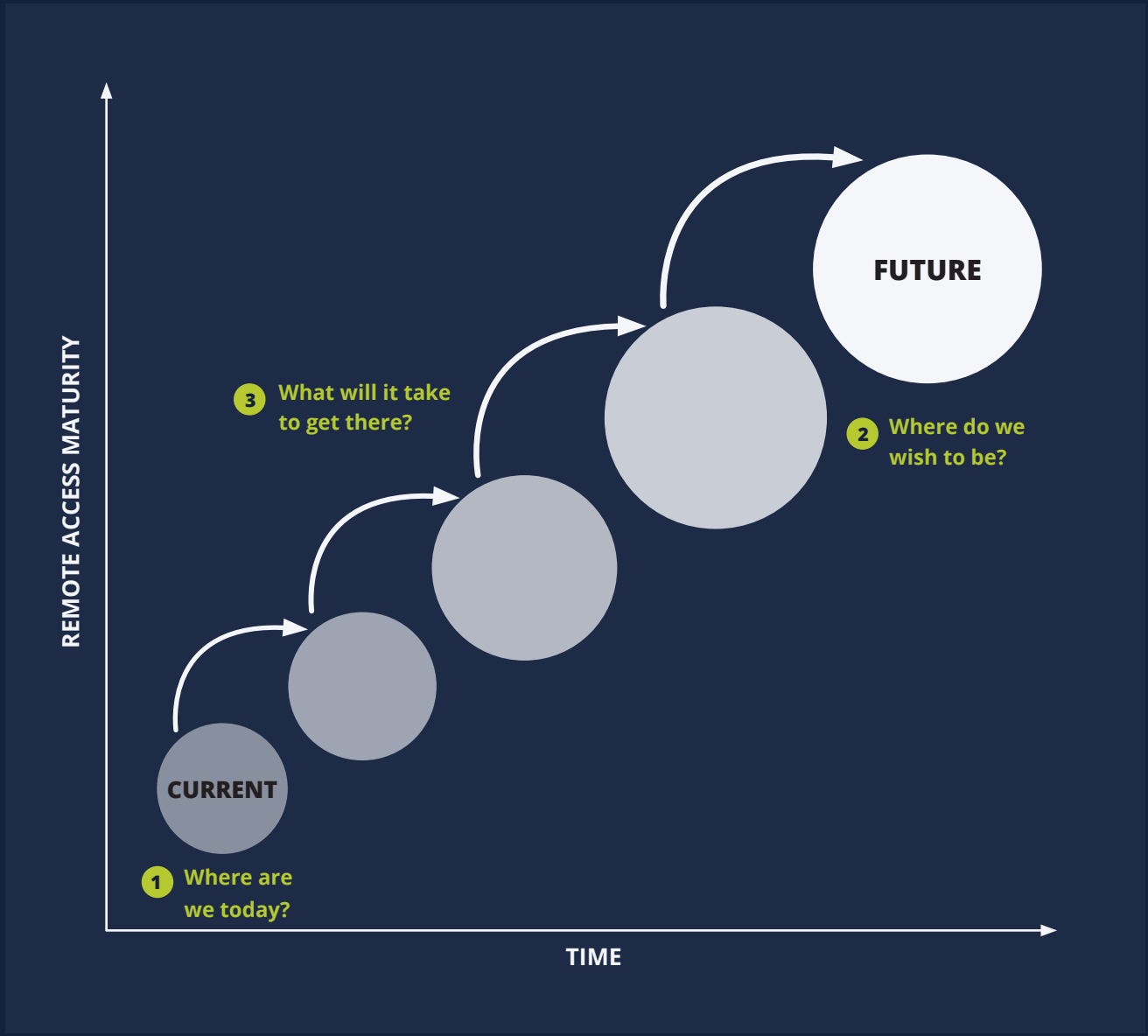
How long time does it take to get a remote connection?
- Instantly
- 1-3 days
- one week
- more than one week

2 Where do we wish to be in e.g., 5 years? What should remote access enable us to do...?

- Mitigate downtime
- Use machine data to conduct predictive and preventative maintenance
- Etc.

3 What will it take to get there? Which specific steps are needed, in relation to

- Timing
- Impact
- Effort



"

Our ability to monitor the performance of our flow-wrap machines, and to adjust or reprogram **remotely** saves time, cuts costs and keeps downtime to the minimum"

Tom Payne, Electrical Manager at Redpack

Redpack PACKAGING MACHINERY

Redpack supplies flow-wrapping machinery for a wide range of manufacturing sectors, with a particularly strong presence in fresh food and pharmaceuticals. Redpack is the UK's leading designer and manufacturer of flow wrapping machines and feeding systems since 1977.

This guide will enable you to get each step of the buying process right

Buying process phase	Outcome	Time to complete
Setting the team	✓ Right stakeholders involved in buying commitee	1 week
Category selection	✓ Remote access category best fit to your needs selected	1 week
Identifying specifications	✓ User specifications identified ✓ Technical specifications identified ✓ Economic specifications identified	2 weeks
Engaging with vendors	✓ RFP created if required by your company ✓ Solutions demoed ✓ POCs completed ✓ Vendors evaluated ✓ Solution selected	4 weeks (early vendor engagement) 4 weeks (POC) 1 week (evaluate offers)
Implementation	✓ Change needs identified ✓ Implementation plan created ✓ Mechanisms in place to support users and onboard new hires	1 week (implementation of 1 site) 8 weeks (hypercare)
		Total: 14 weeks + 8 weeks' hypercare

Setting the team

One of the things we see most often being a barrier to value realization is the dreaded “scope creep”. The single most driving factor of this is not having the right people involved at the right time. Deciding who should be a part of your buying committee and designing the process is one the best ways to enable a fast and reliable value realization.

Different responsibilities at different times

In writing this guide, we have interviewed many companies – both customers and non-customers – that have successfully realized bottom-line improvement from remote access management, but also companies that have failed to do so.

Talking to many stakeholders, and analysing the make of a successful buying experience, we saw a clear pattern across sectors and sizes.

The manufacturers that succeed in:

- **Rapid decision-making**
- **Quick implementation**
- **Speedy ROI**

are the manufacturers that involve all buyer types in their buying committee.

Accross companies we see 4 main buyer types that are all "buying" a different product:

Vision buyer

People buying the "end-destination", focused on change and how to implement change, fast.

Economic buyer

People buying the business case, focused on making the economically right decision.

Technical buyer

People buying the technical solution, focused on security, compliance, maintainability and tech-fit.

User buyer

People buying the functionality and features of the product, focused on usability and performance.

So...who should take part in the buying commitee?

Every manufacturer is different, which is why prescribing the exact setup is difficult. Generally, we see 6 roles that are represented in larger manufacturing buying committees.

Information technology

IT is a central actor in making sure that your remote access systems are in place. Everything from network security to compliance with internal security standards needs to be in place.

Maintenance

Maintenance will be an active end- user of the systems and will be affected by a RAM solution in the everyday work. Making sure that ongoing maintenance work is eased is crucial.

Executive sponsor

The executive sponsor is essential to create the right support and to make sure that the solution is delivering on the overall goals – whether its uptime, security or cost.

Operational technology

OT will be one of the main users of the remote access management system and will be the daily operator of OEM technician access and issue tracking. OT decides the majority of functional requirements.

Project management

As few purchases have such cross-functional impact, a project manager should be involved to oversee the process from A-Z. The PM makes sure that all internal alignment is in place.

Procurement

In most organisations management of running costs is essential. Procurement organisations are typically skilled in managing and facilitating RFP processes. Usually also manages contracts if Legal is not involved.

Category selection

There are many things to consider when finding the right remote access management solution for your company. What is the scale of third-party access needed? Who will access the equipment? What is the distribution and build of the industrial equipment? What do we want out of our data? Before settling on a specific vendor or approach, it is key to identify the most common use cases you will face.

Remote access solutions quickly and securely grant access to defined parts of a network

When a machine unexpectedly breaks down, you often rely on external technical assistance to fix the problem. As every second of downtime is profit lost, your plant manager cannot wait for an onsite visit but is pressed to fix the breakdown at any cost – even at the expense of cyber security.

In essence, the plant manager needs a solution that can connect an external technician to a faulty machine quickly and securely.

The challenge
Providing external connectivity is relatively simple. But, doing so in a secure way that integrates with existing ways of working is more complicated.

Many OEMs provide a remote access solution to fulfil their SLA. While that is good enough for some, these solutions risk noncompliance with your IT policies while adding complexity to an already-complex OT network. For that reason, many manufacturers prefer a standardised solution across all OEMs.

The solution
What your production plants need is a unified remote maintenance solution that:

a) offers documented cybersecurity
b) provides explicit access control
c) is easy to use
d) seamlessly integrates with IT and OT processes
e) gives you full control

Many solutions can fulfil the criteria above to varying degrees. We have outlined the most commonly used remote access categories to the right and described them in detail on the next two pages.

Solution category landscape:

01. Generic industrial firewall/VPN solutions
These solutions connect networks and make individual employees' PCs part of a greater office network.

02. Generic remote access solutions
Generic solutions made for multiple purposes across industries. Generally seen as thin-client screensharing applications.

03. PAM system with remote access capabilities
Privileged Access Management systems control access and permission rights across an IT environment. Remote access is typically one functionality among many.

04. Purpose-built remote access solution for manufacturing
Specifically made to connect remote users to manufacturing equipment, allowing them to view and control interfaces, troubleshoot equipment and install updates.

Remote access category descriptions

GENERIC APPLICATION ← → SPECIFIC APPLICATION

01

Generic industrial firewall/VPN solutions

These solutions exist almost everywhere. Traditional VPN solutions are good for connecting networks and making individual PCs part of a greater office network.

Typically, VPN solutions are 'always available', either with permanent tunnels between site and vendor or client and asset. There are no built-in approval flows for the initiated tunnel/session.

When it comes to fine-grained access policies like granting one person access to one asset on a specific service, these solutions are complicated. The technology itself might be able to solve the task, but it requires deep IT understanding.

02

Generic remote access solutions

Usually seen in the form of screen-sharing software already installed on company PCs, allowing external technicians to overtake control of PC.

External stakeholders are thereby granted unrestricted network access with no central control or transparency, which entails substantial risks to cybersecurity.

These solutions often emerge bottom-up without a management decision to use them. They are typically used in urgent situations, such as downtime, where their speed in use trumps cybersecurity risks – though often without IT/Cybersecurity's awareness or approval.

03

PAM system with remote access capabilities

PAM systems are usually implemented top-down via IT as a suite solution for cybersecurity.

PAM systems are typically deployed across an entire organisation. They can have many functionalities, such as scanning networks for cyber threats and managing which accounts have access to what, including remote access.

PAM systems typically operate through jump host, requiring physical on-premise servers.

Training is required for non-IT users.

04

Purpose-built remote access solution for manufacturing

These solutions are purposely made for industrial manufacturing equipment.
Designed for OT users, they don't require IT skills to operate. Most providers have simple drag-and-drop interfaces, limiting the need for training.

Remote user are typically connected to IIoT device via a hardware gateway placed on the control panel of the machine, even though software-only solutions do exist.

Users and devices are connected through Relay VPN, creating a direct link without access to any other parts of the network. Access can be granted for a specific person to a specific machine at a specific time interval.

Choosing the right remote access category for you

When evaluating remote access categories, four perspectives are central.

- How secure is it?
- How easy is it to implement and get fully operational?
- How easy is it to use in day-to-day life?
- How many resources does it require to buy and operate?

Where companies typically go wrong is trying to answer these questions in silos. Be sure to involve your buying committee and make sure all stakeholders are aligned on the job to be done. Being vigilant about solving the defined need is crucial as companies risk losing sight of the task at hand, and therefore risk ending up with a solution that does many things averagely – instead of a few things well.

Evaluating remote access categories

	Generic industrial firewall/VPN	Generic remote access	PAM system with remote access capabilities	Purpose-built remote access solution for manufacturing
Security against cyber threats	**High**	**Low**	**High**	**High**
Compliance with corporate IT policies	**Medium**	**Low**	**High**	**Medium**
Speed of implementation	**Low**	**High**	**Low**	**High**
Ease of use	**Low**	**High**	**Low**	**High**
Speed of granting access rights	**Low**	**High**	**Low**	**High**
Total cost of ownership	**Medium**	**Low**	**High**	**Medium**
Great for you if you are a ...	**Strong IT knowledge or a small start-up with few machines**	**Small start-up** with few machines with a low risk exposure to cyber attacks	**Large organization** primarily looking for a general cybersecurity solution	**Manufacturer** looking for a purpose- built solution giving global overview

The right approach on paper should also be right in practice

Navigating early category selection can be difficult. Most vendors are good at promoting what they are good at, but typically hide away the downsides of their approach – making it difficult to assess what the right approach for you is. The most often overlooked factors in identifying the right category are:

TIP

If you need more information, ask 1-2 vendors in each category for references of companies similar to yourself. Call the references if needed to get an objective opinion.

Total cost of ownership

The cost of a system is not just the purchase price. To compare apples to apples and avoid unwelcome surprises, make sure to include the following costs in your assessments:

- License cost structure
- Implementation & integration
- Maintenance & service
- Training of existing employees
- Training of new hires
- Hardware – especially if you need on-premise servers
- Expanding solution to other sites
- Onboarding of 3rd parties

Adoptability

If your solution is too technically complex or slow to use in day-to-day life, system users often defer to simple-to-use but unsecure shadow systems.

Apart from wasting money on unused solutions, unauthorised and unmonitored shadow systems can severely compromise security. These include simple screen sharing services, but also physical USB pens and unauthorised account/password sharing.

To avoid shadow systems, make sure your remote access solution can easily be adopted by the users and provide simple and timely interaction.

Future proofing

Your needs constantly evolve – so should your solution. With manufacturing being the #1 target industry for cyberattacks*, security threats and regulations constantly evolve. To maintain a high level of security, your solution must constantly be updated to keep you safe.

Staying on top of new threats and vulnerabilities is generally a difficult task – and is increasing with specialization. Make sure that your remote access solution is focused on your industry and use case and is dedicated to continuous development and improvement.

How to get started with remote access

Typically, the purchasing process of a Remote Access Management system is triggered either by a single person in the organization or by an incident. Both cases call for caution.

To avoid being too silo-focused, you need to 'pause' and expand the perspective. By expanding the discussion through installing a buyer committee, you will have people representing all parts of the value chain that are involved in maintenance – and ensure a holistic view.

From here, the first step is to define the outline of what a solution could look like for you – narrowing down the category of systems right for you.

How to get started

1. Align on your needs by discussing needs in your buying committee (see key questions for inspiration)
2. Assess fit between the categories and your company by comparing your needs with remote access categories
3. Double-check potential "red flags" in relation to TCO, adoption and future-proofing – building a case
4. Choose the category that provides you with secure and quick remote access and best fit for your needs

Key questions to clarify your needs:

- Does the remote access solution need to fulfil many purposes or be focused on specific applications?
- What are the requirements specific to our sector, industry or company that will need to be supported?
- Will we need to give access rights to both internal and external users? At what frequency? At what speed?
- Do we have uncommon characteristics that require a tailored solution?
- How does our end-goal look like?
- Where will the budget come from? Set-up vs. maintenance vs training?
- Who should be able to operate the remote access solution? Non-IT people?

Identifying Specifications

4

Remote access management is much more than just access. Making sure that all user groups are considered is key to finding the optimal solution for you - often covering the entire value chain from maintenance enablement to C-level reporting.

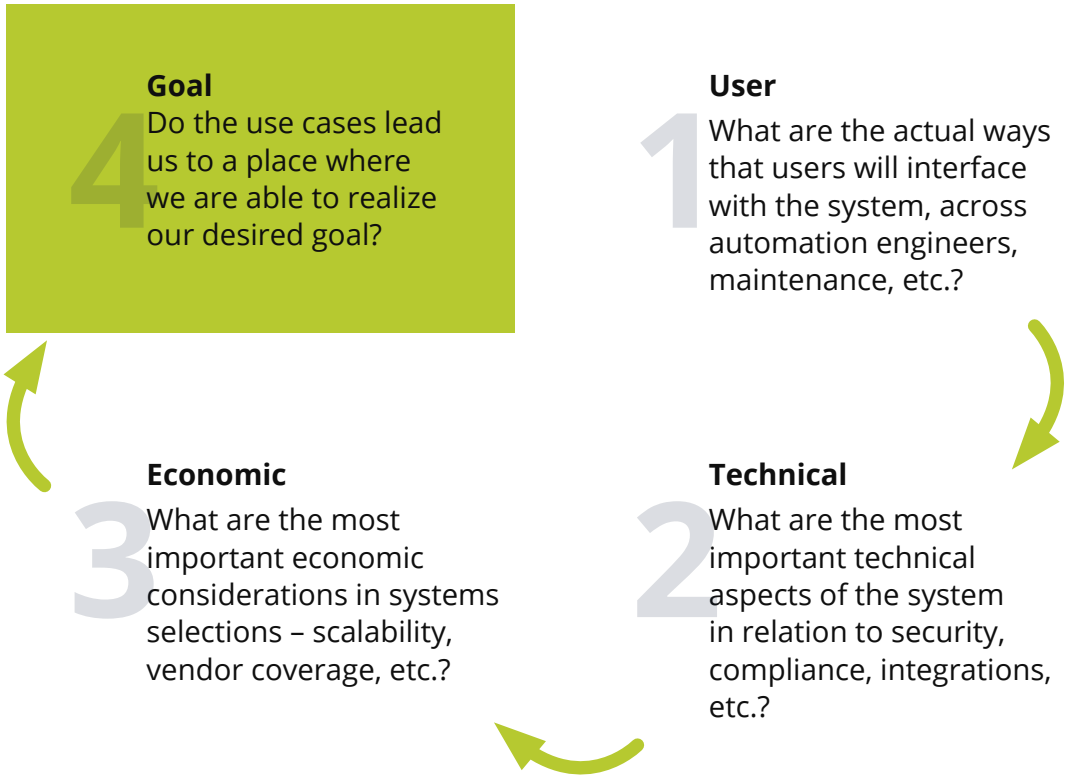
Specifications need to be built from multiple angles

The list of potential specifications can be potentially endless. Often, it can be hard to navigate the list of proprietary features and functionalities, naming conventions, etc., while still being focused on what really matters to you.

To make sure that you set the scene for your buying process, you should define the specifications – or the acceptance criteria for a solution right for you.

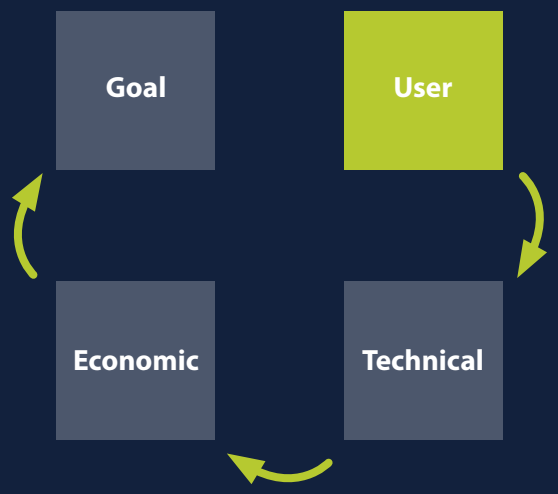
To avoid a long list of mindless features, build your specifications on specific use cases; what you want to be able to do.

Use your buyer profiles as a guide to what you need to cover.



Example of

User specifications



Enable remote work on equipment

We want our service technicians to be able to access, monitor and diagnose our assets remotely

Unify approach to different assets

We want to be able to have ONE system to access, monitor and analyse our assets – across sites and geographies

Global overview, local control

We want to have an easily-searchable global log of accesses and changes to equipment while being able to administer access rights locally

Easy onboarding of new people and assets

We want to ensure that the system is scaling with us – enabling easy on/offboarding of assets and people

Easily delegate access to OEM technicians

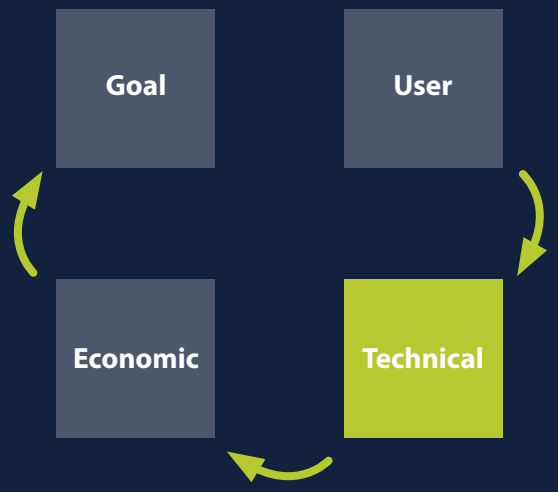
We want to be able to quickly and easily delegate time-restricted access to technicians and ensure frictionless shopfloor approval by OT

Automation of alarms / notifications

We want to be able to define workflows and parameters that will assist us in our day-to-day work

Example of

Technical specifications



Integrate with our SSO and AD set-up

We want to be able to use our existing SSO and AD set-up to manage access to the equipment through existing user groups and MFA

Central audit data gathering

We want to be able to pool the equipment- and access data for analysis. The data needs to be available through APIs to other services

Full flexibility in upgrade / patching

We want to be able to have flexibility in implementation of upgrades/ patches so we can plan a time convenient to us

Low ongoing IT involvement required

We want a RAM system to fit into our existing infrastructure without comprehensive dependencies that place sustained demands on IT resources

Provide overview of cyber vulnerabilities

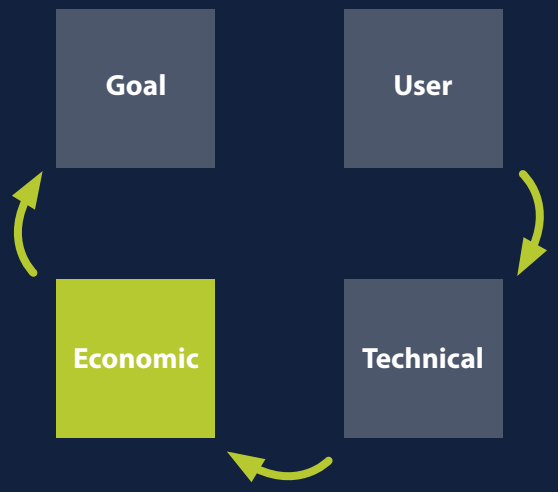
We want the system to ensure security compliance at all times. All vulnerabilities need to be documented and reported

Continuous upgrade of cybersecurity

We want the system to be proactively kept up to date with emerging cyber threats and compliant with future cybersecurity directives like NIS-2 and IEC62443

Example of

Economic specifications



Ensure a speedy time-to-value

We want to start realizing the benefits of the RAM system as fast as possible – ensuring short pay-back time

Enable scalability over time

We want to be able to scale our system over time, and have an easy way to manage the cost of onboarding new sites, equipment and people

Use knowledge for optimization

We want to be able to use usage data to inform us of potential ways to optimize our cost structure

Offer transparent price model

We want to plan and predict the total cost of ownership by having full transparency into the pricing model

Ensure flexibility through pricing model

We want flexible pricing according to our preference for upfront or pay-as-you-go pricing. Further, we want to split the price into a global price and a per-factory price

Be able to handle all support

We want the vendor to be able to handle all and every part of the RAM system lifecycle, from configuration, to support and retirement

Make sure that the use cases support your vision

To make sure that your use cases are all relevant to your overall goals and ambitions, you should evaluate how they contribute to them. When you are comfortable that you have an exhaustive list, you are ready to initiate the buying process.

User specifications

+

Technical specifications

+

Economic specifications

Goals:

Reduce downtime

Lower maintenance cost

Reduce risk of cyberattacks

An important exercise is to assess whether the combination of user, technical, and economic specification will enable you to realize your goals.

If you are not able to draw a line between the specifications and how they will help you achieve your goals you should revisit either your specifications or your goals.

This exercise enables you to have a clear benefit realization plan and also make the purpose of your transformation very salient.

Engaging with vendors

Once there is internal clarification about the goals and the specifications, it is time to engage with potential vendors. There are many ways to go from shortlisting to selection, typically either through a formal process or dialogue with select vendors. In this chapter, we cover what we have learned from providing remote access to more than 9,500 production sites.

Optional: Building a request-for-proposal

Some companies have a policy to formalize needs and requirements in a request-for-proposal (RFP). While this is not considered a necessary step in this guide, writing an RFP for potential vendors can give you clarity on your needs, result in more competitive bids, and allow you to compare vendors based on uniform criteria.

In our experience from working with customers, we see that a simplified process without an RFP is preferable. However, if your company requires you to write an RFP, keep in mind that it should communicate your situation, needs, and vision clearly to make sure vendors get an understanding of your company as an outset.

Secondly, the RFP should clearly communicate what you are trying to achieve and not how you wish to do so. Far too often, RFPs end up being prescriptive, not enabling vendors to challenge and uncover new approaches to achieving your goals.

We suggest structuring your RFP as seen on the next page.

A final requirement should be for vendors to present their RFP and demo their solution during a 1-2 hour meeting. This allows you and your buying committee to ask questions, experience how the solution works, and avoid misunderstandings.

Section	Component	Purpose
Company presentation	Introduction History Business overview Strategy	Give a short introduction to your organisation Illustrate your path to where you are today Explain the composition of your business Enable vendors to see how they can assist you
Background for RFP	Purpose and objective Approach and formats Aim	Make the vendor understand why they are here Explain how you expect the RFP to be delivered Explain what you want to achieve (goals)
Process	Stages Timeline People	Make the overall steps visible Set expectations for your timeline, including milestones and decision gates Give access to stakeholders who are main input-givers
Solution requirements	Implementation Operation Technical References	Gives insight into how the vendor will implement Illustrates how the day-to-day handling is done Explains the technical fit with your set-up Shows what vendor has done for similar companies
Proposal economy	License Configuration Training	Explains vendor's pricing model options Breaks down the different components of cost Details training needs and training process

Shortlisting vendors

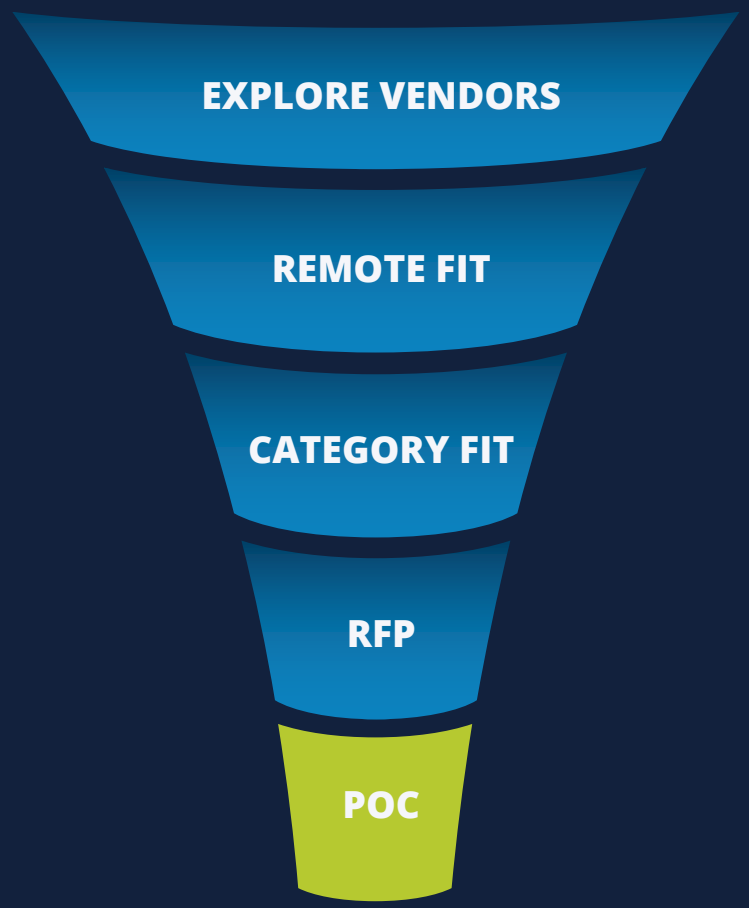
RFP presentations and demos are a great way to get introduced to RAM solutions. They do, however, happen in controlled environments. To evaluate how well a RAM solution is truly going to work for you, you must pilot it in in your unique, live environment with real people, real machines, and real data via a proof-of-concept (POC).

Be razor sharp on who you invite for a POC. They require a resource commitment from both sides, why vendors sometimes charge for them. Here's the process:

First meeting: Engage the 1-2 vendors that performed best in the demo round and set up a meeting to define success criteria for the POC.

POC Implementation should take less than one week. If it takes weeks or even months it's a red flag, especially if you plan to expand to several facilities.

Testing time: Test the solution(s) for a period of 30 days so end- users can get a feeling for the solution and any potential challenges can surface.



Evaluating and selecting

Remote access management is a relatively new category. There are several ways to provide remote access, each with different maturity and slightly different capabilities. This makes it hard for buyers to navigate the solution space and identify which alternative is the right one for them.

When assessing the fit, the importance of soft factors in vendor selection is often overlooked. This includes your relationship with the vendor and how you see it progress over time. Remote access and cybersecurity are rapidly-evolving areas, making advice and support from trusted partners highly valuable.

For a vendor to pass your evaluation, you must trust that the vendor can deliver on a range of must-have capabilities – now and in the future.

	Important for evaluation of:
Ease of use	User specifications
Security	Technical specifications
Configurability	Economic & technical specifications
Implementation	User specifications
Platform scalability	Economic & technical specifications
Continuous development	Economic & technical specifications

Must-have capabilities

Ease of use

Interface and functionality must fit user needs

The value you will get from your remote access solution depends on its adoption and ongoing usage. If the system isn't easy to use and employees cannot grant access rights at the needed speed, you risk employees deferring to shadow systems.

As a buyer, you need to assess whether the user experience fits with the users. The interfaces must be intuitive and the functionality tailored to both technical and administrative roles in your company. Remember that if non-IT people should be able to manage, maintain, and use the remote access solution, the system must be designed to accommodate that.

In essence, you need to ask your buying committee: Do we believe all user groups would be able to efficiently use the remote access solution?

Security

Security is a qualifier – without it we cannot go

Manufacturers are experiencing increasing pressure for cybersecurity readiness. In fact, the manufacturing industry is currently the #1 target for cyberattacks*, with OT as the main target. When evaluating the RAM security, a minimum should be:

- End-to-end encryption
- Access restricted to specific IP endpoints (and not the entire network)
- Ability to grant access to a specific person to a specific device at a specific time interval
- Two-factor authentication
- Audit trails
- Role-based account management
- User authentication is compliant with Corporate IT policies (integration with active directory, MFA, etc.)
- Certified/audited according to relevant certificates for you (e.g. IEC62443)

*X-Force Threat Intelligence Index 2022, IBM

Configurability

The right solution is tailored to you

You need to make sure that the solution you choose can be configured to your specific needs. Many manufacturer organisations have non-negotiable configuration needs that not all remote access solutions can be configured to.

Make sure that the remote access system accommodates your needs:

- Integrate to your own systems/UI or use vendor interface?
- Hosting on-premise, on your own cloud/ network, or on the vendor's servers?
- Remote access through VPN tunnelling, jump host, or web remote desktop via web browser?
- Software-only gateway or hardware gateway across the factory floor?
- Hosting flexibility? Data storage and management?

Must-have capabilities

Implementation

Don't neglect time-to-value

Time-to-value is the lens you should adopt when evaluating remote access solutions' ability to be implemented in your organisation. Implementation can take many shapes and forms, but the time from initial request to being fully operational can differ greatly from solution to solution.

Make sure to pay extra attention to:

- Delta from demo/pilot – what is missing
- References from peers
- Willingness to include implementation time in payment terms
- Load on internal resources
- Ensuring adoption and follow-up

Platform scalability

Select a solution that scales with you

Your business is evolving, and therefore your remote access management solutions should as well. You should be able to scale to new equipment setups without friction.

If not, you risk escalating costs and complexity if you need to expand to additional sites in the future. It's always a good idea to drive a POC or Pilot to test the vendors' ability to swiftly get up and running. Make sure to assess the:

- Reliance on on-premise equipment – and its cost
- Analysis requirement and dependencies of pre- existing infrastructure
- Training requirements
- Number of providers you need to mobilize to supply hardware, software, and hosting
- Set-up cost to operating cost ratio
- Ability to work with legacy equipment

Continuous development

Your solution should fit - today and tomorrow

You should assess the degree to which the remote access solution provider shows a credible commitment to keep your solution updated to fight the latest cyberattacks and develop its functionality according to your needs.

This is an often-overlooked evaluation criterion – and can be harder to assess. Providers that are dedicated to continuous improvement will have more customer feedback, incorporate more global security risks, and be up-to-date on changes in regulation and integration needs that reflect your needs and use cases.

Remote access is an emerging industry. The expected development in functionality is enormous over the next 5-10 years, why you must choose a provider likely to keep evolving your solution without jeopardizing the user experience.

Implementation

After selecting a new vendor, agreeing to the T&Cs and the ink on the paper is dry, your new solution should prove itself. But way too often new components and questions arise, changes to the contracts sneak in, involvement drops, and all of a sudden implementation time drags out. Implementation is a specialization of its own, so in this chapter we will highlight learnings from thousands of implementations to make sure that your value realization will be fast.

Implementation is very much about change management

The buying process can for many organisations be a long-haul that requires significant time investments. Too often we see organisations mistaking the purchase decision for the finish- line – and not just a milestone. As a result, the implementation gets little attention and time-to-value drags out. The organisations that master implementation get more out of their solutions quicker – and they all share the same trait. They are prepared.

Being prepared is not just about planning ahead – but also realizing that the job is not done when the remote access solution is installed. Focusing on "what we are doing differently" with a remote access solution in place is central to ensuring a smooth transition. To do so, you need to have a holistic view on implementation; from having awareness to supporting the "new ways of doing".

As most manufacturers will not have in-depth experience in implementing or changing remote access management systems, your vendor should support across this!

I Make sure that all users of the RAM solution are **I**nformed and aware about what we are changing

B Make it very visible for the users involved how a RAM solution will **B**enefit both the company and them individually

U Give the users the core **U**nderstanding of what they need to change. E.g. new operating procedures, interfaces

P Support the users with actual **P**ractise in using the solution, assisting them in building the needed capability

A Ensure continuous **A**doption and allow for feedback, questions, and iterative learning for maximum coherence and compliance

A structured process ensures that everybody is aligned

No two manufacturers and no two implementations are exactly the same. To avoid costly roll-backs and tasks falling between chairs you should be crystal clear on exactly what both sides need in the implementation – otherwise, the process will drag out wasting time and delaying the value realization. While different vendors have different processes, you should make sure that they at least cover the following aspects:

Implementation phases

PLAN

Align on the scope and plan of implementation. Define who is responsible for what task, and what information/actions are needed when. Build a common implementation plan so everyone has one source of progress

SET-UP

Share the needed data to set up the solution. Typically, this entails:

Administration details, e.g. local administrators, users, access groups, and access rights

Network details, e.g. outbound firewall rules, factory blueprints, and IP settings

Asset details, e.g. IP addresses, names, and locations

TEST

Make sure that you put aside time for testing the different use-cases and specifications needed for your solution. Make sure that your people are actively involved in giving input and signing-off

CONFIGURE

Based on the selection criteria and potential further input from the test, configure the solution to your needs. Our experience show, that this is key for adoption of the system

TRAIN

Once the system is “ready” – instruct and show the users how they operate the solution. The goal is to enable users to handle all features on their own – so make sure that they have the tools to self-identify potential solutions

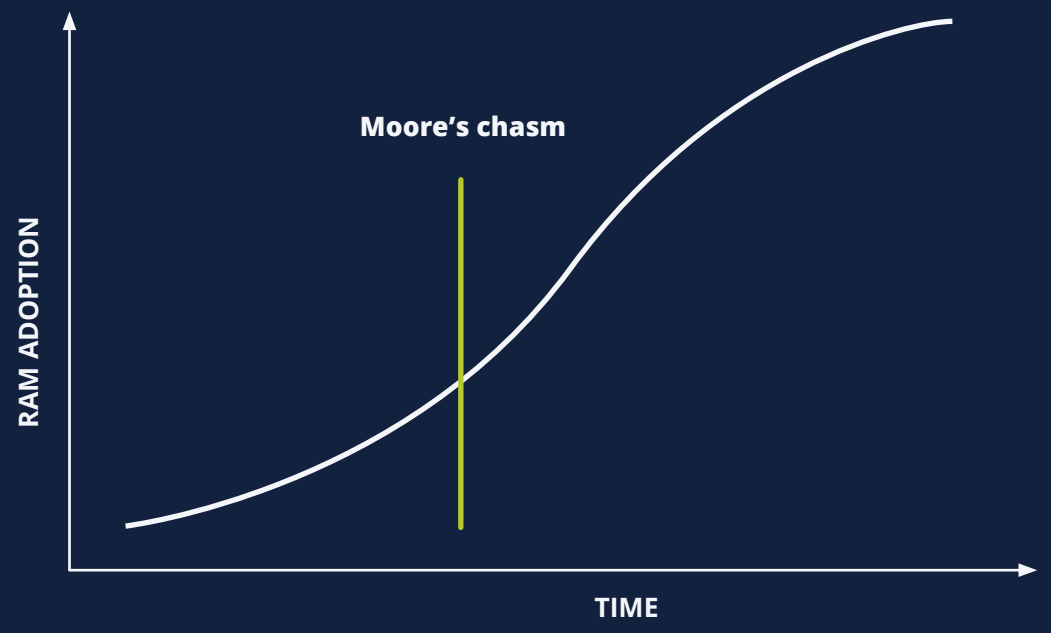
Ensure the right initial support

Once the remote access management solution is implemented and the users are all trained, you will face the true test of adoption; getting users to actually adhere to the solution.

Often companies neglect the importance of the early phase of changing ways of working and risk reverting to status quo; falling victim to Moore's Chasm. To avoid this, it's important to have full attention both internally and from you vendor – a so-called "hypercare" phase.

Apart from making sure the right support and issues handling is in place, the purpose of this phase is to enable you to make an early evaluation on your value-realization. Only once the application of your remote access management solution is stabilized across people, process and technology you can assess IF your solution is meeting your requirements and thereby consider your solution implemented.

Adoption model



Typically, your Hypercare should include:

- Dedicated contact-point for users to address all issues to
- Central aggregation and monitoring of issues
- Centralized mitigation plan – and agreement on ways to address
- Quick escalation of potential issues
- Vendor driven coaching
- De-brief with data on adoption and identified issues as well as ways to address (e.g. new configuration)

Ensure your solution grows with you

Needs for configuration and general support will arise, and you need to address them when they do. But as a manufacturer, the reality you operate in today is most likely vastly different than what it was just 3 or 5 years ago. Therefore, you need a remote access management solution that is able to grow and adapt to your needs.

Anticipating changes to the initial set-up is important to not get surprised with excessive change-costs or problems with scaling. When agreeing on the right vendor, you should make sure that they are able to support your business needs – both today and on a continuous basis.

Common change cases

Assets

You will often need to onboard new, or different assets. Make sure that your solution can handle addition or change of equipment easily.

People

The people using your solution will change over time, and therefore you need to ensure that you can get new people trained.

Sites

Over time, you might want to add/remove sites to your remote access management setup. Make sure that you have a process for doing so.

Configurations

Your ways of working might change, due to security protocols, user rights management or the like. Anticipate changes to your configuration.

New releases

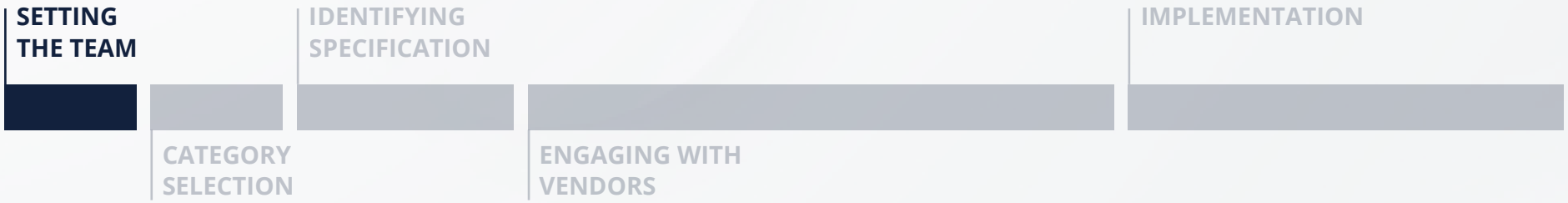
To ensure compliance and longevity of your solution, you need to make sure that you are able to upgrade to new releases and features without hassle.

The A-Z process

Too often, manufacturers find themselves in an unnecessarily long and messy buying process due to unclear solution criteria and missing organisational alignment. The risk of ending in a similar situation can be mitigated by structuring the buying process correctly, involving the right stakeholders, and starting the process by asking the right questions.

In this chapter, you'll find a condensed overview of the key elements and outcomes in each phase of the buying process.

How to drive the buying process



Setting the team

Your buying committee must represent end-users, IT, and OT. If the right stakeholders are not involved, you risk ending up with a solution that:

a) does not match the actual use case

b) is not compliant with security protocols or

c) is not aligned with cybersecurity strategy

To get the right perspectives, your buying committee should typically include:

Buying committee members

- **OT & Service/Maintenance** to ensure that solution features match actual use case
- **IT** to ensure compliance with safety protocols
- **C-level** to provide sponsorship and budget & align with company & data/ cybersecurity strategy
- **Project management** for internal alignment
- **Procurement to manage costs and potentially drive RFP process**

Outcome

✔ Right stakeholders involved in buying committee

Benchmark time requirement

1 week

How to drive the buying process

SETTING THE TEAM | CATEGORY SELECTION | IDENTIFYING SPECIFICATION | ENGAGING WITH VENDORS | IMPLEMENTATION

Category selection

Good category selections begin with your most common use cases. Spend time identifying them before you look at specific solutions. Compare your use cases with the pros and cons of the four main remote access categories.

- **Generic** industrial firewall**/VPN solutions**
- **Generic** remote access solutions
- **PAM system** with remote access capabilities
- **Purpose-built** remote access solution for manufacturing

Remember to look at total cost of ownership, adaptability and future-proofing when evaluating categories.

Category evaluation perspectives

- How secure is it?
- How easy is it to implement and get fully operational?
- How easy is it to use in day-to-day life?
- How many resources does it require to buy and operate?

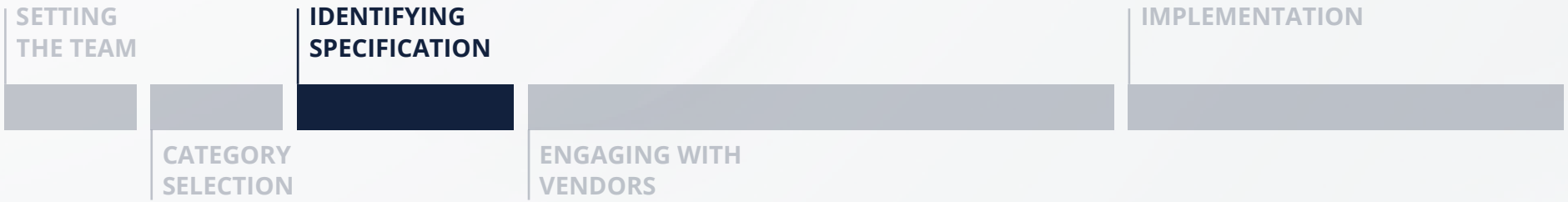
Outcome

✔ Remote access category best fit to your needs chosen

Benchmark time requirement

1 week

How to drive the buying process



Identifying specifications

Your specifications – or acceptance criteria - must be built from multiple angles to ensure that you're enabled to do what really matters to you.

When fulfilled, the specifications should enable you to reach your desired goal for remote access management.

Specification areas

- **User specifications** – What are the actual ways that users will interface with the system, across automation engineers, maintenance, etc.?
- **Technical specifications** – What are the most important technical aspects of the system in relation to security, compliance, integrations, etc.?
- **Economic specifications** - What are the most important economic considerations in systems selections – scalability, vendor coverage, etc.?

Outcome

- ✔ User specifications identified
- ✔ Technical specifications identified
- ✔ Economic specifications identified

Benchmark time requirement

2 weeks

How to drive the buying process

Engaging with vendors

If required by your company: before reaching out to potential vendors, formalize your needs and requirements in an RFP and send to 3-5 vendors. Have them present their RFP and demo their solution to your buying committee to see and feel how the solution works.

Select 1-2 vendors for POC in your unique environment using real machines, real people, and real data.

Test for 30 days to pressure-test the solution and select the best-performing solution based on:

Evaluation criteria

- **Ease of use |** Interface and functionality fit user specifications
- **Security |** Technical solution capabilities match technical specifications and keep us safe from cyberattacks
- **Configurability |** Solution can be configured to our technical and economic specifications
- **Implementation |** Solution provides frictionless implementation and provides fast time-to-value
- **Platform scalability |** Solution has low reliance on hardware, training, and involvement of third parties
- **Continuous development |** Vendor is committed to update and develop your solution for your specific use case over time

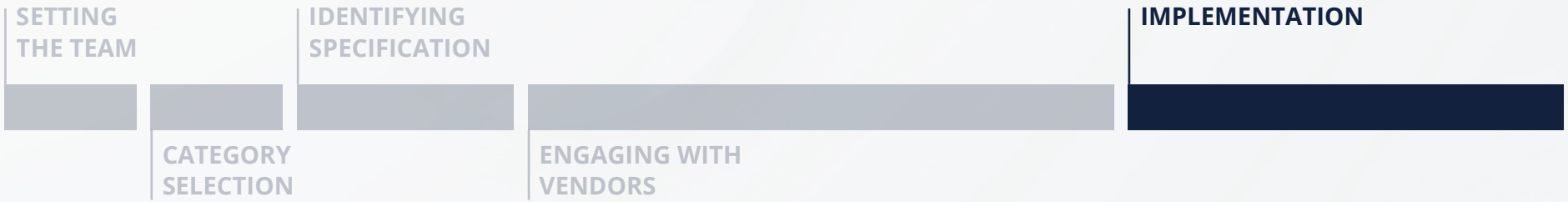
Outcome

- ✔ RFP created
- ✔ Solutions demoed
- ✔ POCs completed
- ✔ Vendors evaluated
- ✔ Solution selected

Benchmark time requirement

4 weeks (early vendor engagement)
4 weeks (POC)
1 week (evaluate offers)

How to drive the buying process



Implementation

The purchase decision is a milestone – not the finish-line. Realising value from your solution relies on successful adoption. Adopt a change management perspective to drive the change in your organisation. Plan to ensure that…

- all users are informed
- the RAM solution benefits are visible
- users understand what they need to do differently
- user practice using the solution
- ensure continuous adoption and allow for feedback

Implementation process

1. **Plan |** Identify change needs and assign responsibility to tasks and actions
2. **Set-up |** Share the data your vendors needs to set up your solution – typically administration-, network-, and asset details
3. **Test |** Test each use case before going live. Get input and sign-off from your people
4. **Configure |** Configure the solution based on your specifications
5. **Train |** Train all user types in how to use the solution

Outcome

✔ Change needs identified

✔ Implementation plan created

✔ Mechanisms in place to support users and onboard new hires

Benchmark time requirement

1 week (implementation of 1 site)

8 weeks (hyper care)

Stakeholder involvement across the buying journey

The required level of involvement of the stakeholder groups represented in your buying committee will shift over the course of the buying process. The highest level of involvement is required at the beginning where the right people need to formulate the needs and vision of your remote access solution. Representatives from IT and OT typically drive the buying process and are heavily involved throughout.

	Setting the team	Category selection	Identifying specifications	Engaging with vendors	Implementation
C-level	○	○			
IT	●	●	●	●	
OT	●	●	●	●	
Maintenance/ service	●	●	●	○	○

○ Limited involvement ● High involvement

Common pitfalls to avoid

01

IT blocks buying process

If IT has not been involved to ensure compliance with IT security protocols, IT can block or veto the decision.

When manufacturers fall into this trap, it is often because an urgent remote access need has arisen in OT or Service/ Maintenance and been driven through a siloed approach.

To avoid it, don't buy in silos - get all the right stakeholders together from the beginning.

02

POC drags out

When the vendor does not have the needed documentation previously described, the POC process cannot proceed.

POC usually takes 30 days but can range from 2 hours to 6 months.

Preparing the right documentation can significantly shorten the POC process and decrease your time-to-value.

03

RAM not used by end users

If the buying process is driven by IT without involvement of end users from OT and Service/Maintenance, it sometimes occurs that the solution does not live up to usability requirements.

When it takes too long to grant an access right to an external technician, for example, end users can feel forced to use shadow systems, compromising cybersecurity.

Again, don't buy in silos - get all the right stakeholders together from the beginning.

Common pitfalls to avoid

04

Hidden costs

Many companies looking for a remote access solution overlook the recurring costs of using it. Employee hours spent on implementation, training and onboarding of new employees, service fees, and hidden price regulations are just some of the largest hidden costs of remote access solutions.

If not taken into consideration, companies risk ending up having to limit roll- out, reducing impact and increasing risk.

05

Missing stakeholder involvement

If not all stakeholders have been involved early in designing the purchasing criteria, you risk having costly roll-backs and breaks in your buying process – sometimes even putting it to a halt.

Make sure to involve relevant stakeholders early, and make their contribution and responsibilities clearly visible.

06

Buying features not systems

Buying too specific on functionally can result in poor solutions either in the form of technical overkill – or the opposite.

Manufacturers buying specific functionality might end up not evaluating the other opportunities for optimization, and therefore overspend on simple functionality.

On the other hand, you might end up with an overcomplicated systems landscape that, if unmanaged, contribute to accelerated security risks.

Tools

We have gathered a selection of relevant tools to help you work with your own buying process. Across manufacturers, the main factor separating the leaders from the laggers are the level of preparedness and alignment through the entire process; from pre- purchase to decision-making and continuous value realization.

01 Business case template

Support your change-vision with a business case – quantifying the benefits you reap in your business.

02 ROI calculator

Estimate the return of your remote management investment – on save increased throughput and lowered risk.

03 RFP Checklist (if required by your company)

Get an overview of the most used and valuable parts and questions of an RFP.

04 TCO Calculator

Make sure your evaluations are supported with a complete picture of the associated cost, with this TCO calculator.

Outro

Remote Access Management solutions are a core enabler of the modern manufacturer. Being able to access and manage your production assets from anywhere and anytime is central to increasing value; from maintenance, technician, equipment and security. In this guide we have outlined the considerations needed, in order to have a smooth buying journey, ensuring cross-operational alignment and fast implementation and realization of value.

If you have any questions or need elaboration or guidance to your buyer journey, feel free to reach out to:

Jesper Nisted Milvertz
Director, Solutions Design

+45 8870 8650
jnm@secomea.com

secomea