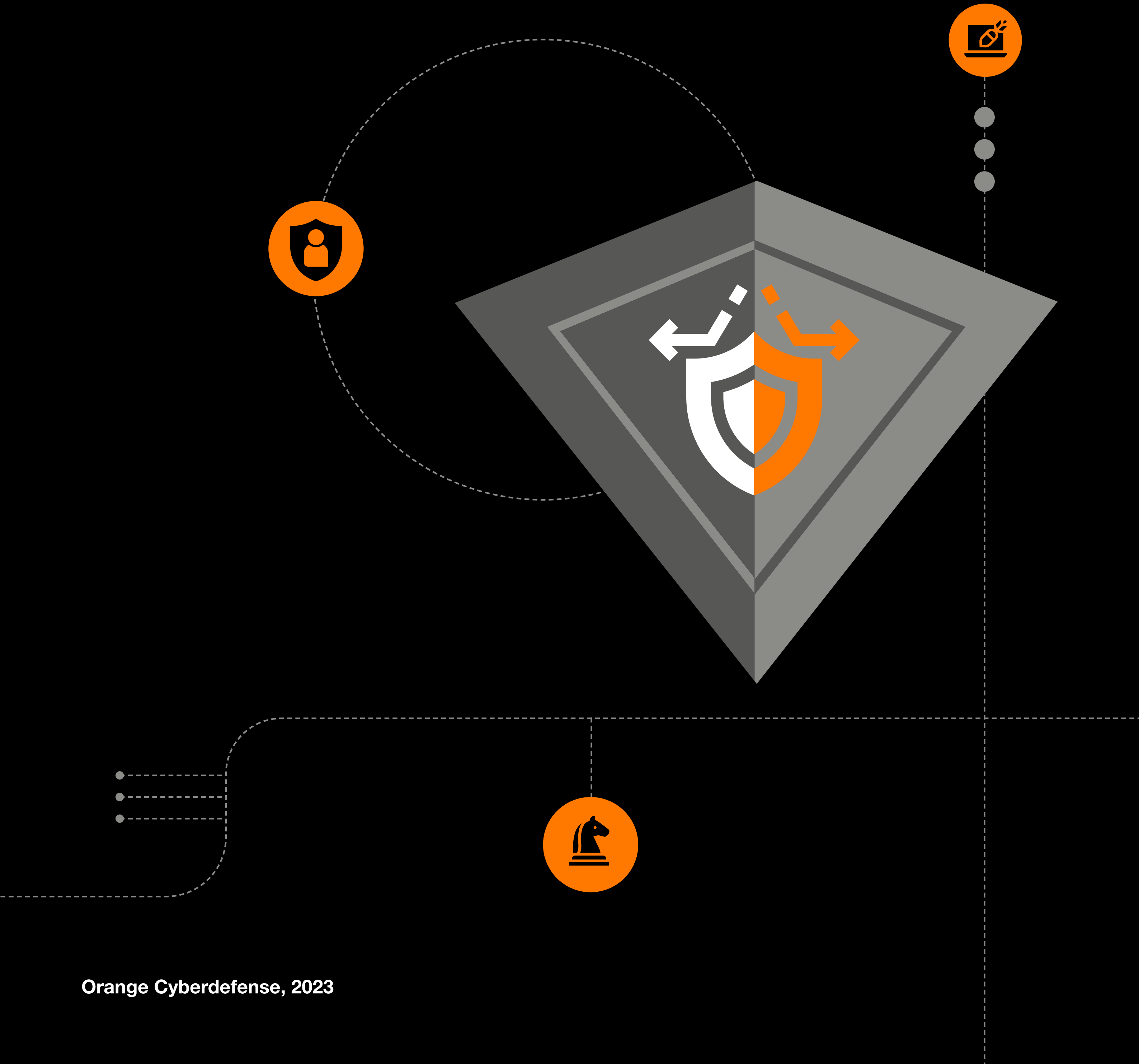
orange™ Cyberdefense

Optimizing your Microsoft Security

Maximize the value of your Microsoft Security technology
with a strategy that's right for your organization



Orange Cyberdefense, 2023

Introduction

Microsoft is a global technology corporation and a leader in many areas of cybersecurity. The possibility of obtaining their security technology through enterprise agreements is now tempting organizations to use as much Microsoft Security technology as possible.

But a sound security strategy is not just about the technology. You also need to pay attention to strategy, the skills shortage, and processes and operations that will enable you to get the maximum value out of your chosen solutions.

Here, we offer an informed, independent viewpoint on these issues and provide a guide for security leaders with regards to Microsoft Security, so you can adopt an approach that is both effective and cost-efficient.

The pros and cons of a Microsoft Enterprise Agreement that includes security technology

A Microsoft Enterprise Agreement is primarily targeted at large commercial organizations with 500 or more users/devices or government organizations with 250 or more users/devices which want to license software and cloud over a 3-year period or more. These contracts give organizations the ability to add and adjust products and services over time and reconcile changes through an annual 'true-up' process. Enterprise agreements include a subscription option that lowers the initial licensing cost and allows you to increase or decrease subscriptions counts on an annual basis.

There are three reasons why companies are attracted to a Microsoft Enterprise Agreement:

- The possibility of maximizing the value of investments in Microsoft technology by getting the best pricing.
- The flexibility to adopt new technology as it comes along and adjust volume levels as required.
- The ability to streamline license management and consolidate the number of vendors.

The Microsoft range of enterprise licenses goes from E1 to E5 (where E stands for Enterprise), with E5 including Microsoft Security technologies and advanced capabilities for compliance and analytics and F1 to F5 license models are for organizations employing frontline workers.

Server and cloud enrollment is an option under the Microsoft Enterprise Agreement by which organizations can commit to one or more key server and cloud technologies from Microsoft, including related security products. Products such as Defender for Cloud, Microsoft Sentinel, and network security such as Azure Firewall are consumption based.

How to maximize the value of your Microsoft Enterprise Agreement

Despite the obvious advantages of enterprise agreements, there are a few potential pitfalls of relying solely on enterprise agreements to source your security technology.

One risk is that the enterprise agreement may include products that your organization could benefit from but lacks the skills or maturity to use.

Another risk is that your organization may be buying technology without a clear security strategy and the right processes in place. Before you start with any implementation of security products, you first need to have a clear security strategy that suits your organization's needs.

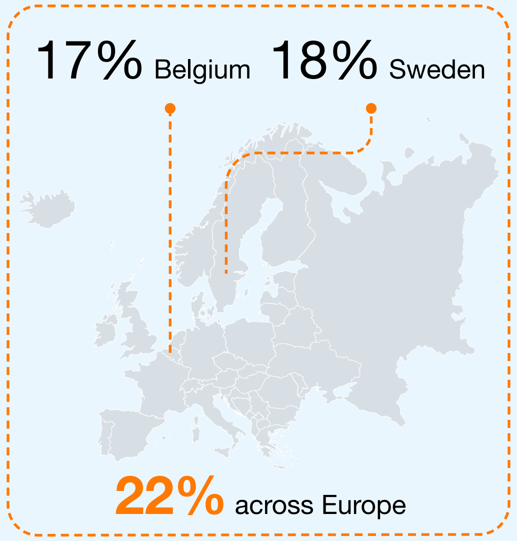
> Finally, to maximize the value of your enterprise agreement, you need to complement technology with services, such as security consultancy, security strategy, vulnerability assessments, penetration testing/ethical hacking, managed detection and response services, or security operations services.

The shortage of skills around security technology

In 2022, the scale of the global cybersecurity workforce gap was 3.4 million people.[1]
In EMEA, the shortfall was 317,000, a figure which had increased 59% on the previous year. 74% of cybersecurity teams with staff shortages believe the skills shortage puts their organization at moderate or extreme risk of attack.

Microsoft's own research[2] found that the demand for cybersecurity skills grew by 22% across Europe, by 17% in Belgium, and 18% in Sweden between 2021 and 2022. Europe's cyber-skilling efforts have not been keeping pace with the growing demand for cybersecurity professionals, highlighting an urgent need for both public and private organizations to step up and help bridge the gap.

Demand for Cybersecurity Skills
(Between 2021-22)



With cyber threats increasing in both frequency and complexity, Europe's accelerating shift to a digital-first economy, and the increasing cybersecurity requirements in European legislation, the need for skilled security staff has never been higher. Microsoft have made a lot of good training available to customers, partners, and service providers to upskill security professionals on their security technology.

Microsoft are investing in a skills initiative in Europe and are working closely with local education institutions, non-profits, governments, and businesses to develop a cybersecurity skills program that fits the unique needs of the market. In this journey, diversity is an area where further progress is needed, and special efforts are being made to overcome the low percentage of women in cybersecurity.

> *In this situation, using Microsoft Security products is an advantage over a multi-vendor approach where you need separate skills in each vendor's technology. The Microsoft platform has the advantage of a consistent management interface, which makes it easier to maintain multiple Microsoft solutions with fewer resources.*

It's not only on-prem anymore, it's multi-cloud

Today, organizations don't just use on-prem and SaaS services; many use multiple cloud vendors, SaaS platforms, and on-prem data centers at the same time. These multi-venue environments are more complex to secure. You have to know how to secure each element involved, so you have to train in securing all your providers' cloud, SaaS, and on-prem solutions – which is a longer development path than if you were training in generic security technology.

> The upside of this, however, is that training in all the underlying technology and the security that overlays it makes you a more rounded security professional – and because you understand that underlying technology, you can secure it more effectively.

Strategies for overcoming the skills shortage

Broadly speaking, there are four ways to deal with a skills shortage: hiring new people, training existing people, using contractors, and outsourcing.

1. Hiring new people is difficult because of the scarcity of qualified professionals, competition for their skills, and the high salaries they command.

2. Training existing people is an effective and cheap way forward. As long as there is a skills shortage, there will be a risk that they will be poached by someone else, but this risk is mitigated by investing in your people.

3. Contractors and freelancers can be a good route. People with in-demand skills tend to operate this way because they can earn more. But this makes them even more expensive than similarly-skilled employees – and they can move on quickly to the next project.

4. Outsourcing is a real option. As with anything where skills demand outstrips supply, it makes the skills shortage someone else's problem. It is a faster route to extracting value from your Microsoft Security products than hiring or training.

Outsourcing can be the quickest and cheapest way of getting access to Microsoft Security skills and the wider security skills you need – if you choose the right provider. You need to be confident of the credibility of the managed service provider. Are they actually a security expert, or just a Microsoft expert? – there's a big difference.

They may have been a Microsoft partner for 20 years, but you need to verify that they have the security skillsets and capabilities you need. Experience in putting security software on people's laptops is a world away from tracking a sophisticated attack across your hybrid cloud environment and mitigating it in real time.

Becoming accredited in Microsoft Security technology is a smart career path for an up-and-coming security professional. It's a fast way to become a valued member of the cybersecurity profession. But expertise in Microsoft should be balanced with more general security skillsets through organizations such as the SANS Institute, in order to become a rounded security professional.

> Whatever route you take to mitigate the skills shortage, remember that what you need is not simply a certain number of certified professionals. You also need the organization and processes to deliver consistent security outcomes, such as reducing your attack surface or analyzing security event data to detect and respond to intrusions.

The importance of taking a strategic approach to security

In general, most enterprises have a security strategy, but the maturity of that strategy and its implementation vary widely. Inevitably, there is also a lot of reactive, tactical activity in response to particular threats. If you suffer a ransomware attack, you can't just ignore it and stick to your strategy – you have to react.

Organizations that have been predominantly reactive in their approach to security will have acquired a great many tools.[3] The average enterprise now uses 76 security tools . Often, these tools don't work together, which makes security operations unnecessarily complex and inefficient.

Strategy is more than technology

But, it's not just a question of technology. Organizations without a proper security strategy will have inconsistent processes. They might do some things very well, but others not at all. Key processes, such as incident response, may be undocumented and untested, so when an incident does happen, they're not ready for it.

From a people perspective, an insufficiently strategic approach may result in unclear roles within the security and IT departments. Roles may be out of date and no longer in sync with technology developments. Security may not be a formal part of a person's job description and if that person leaves, re-hiring against their job description could leave you with a competency gap.

If companies don't follow a strategic approach to security, the most common result is that they fall victim to a ransomware attack which leaves them unable to operate for days or even weeks. It kills their revenue, harms their reputation, and leads to massive costs of recovery – not just the cost of recovering data, but rebuilding networks, and implementing measures to make sure it doesn't happen again. Not to mention the cost of the ransom itself.

> " The average cost of a ransomware attack (excluding the cost of the ransom) was $4.5 million in 2022[4], a figure which far outweighs the cost of taking a strategic approach to security. Of course, there is a cost in developing a robust security strategy, but it's far less in the long run than having to recover from a major incident.

Orange Cyberdefense, 2023

What does a strategic approach look like?

A good security strategy is really an exercise in risk management and covers people, process, and technology. The first step is to get visibility of your risks; then you can make a strategic decision about how much risk you're prepared to accept. We'd all like to shut down all risks to the business, but, realistically, no-one ever has the budget, people, processes, or time to reduce risk to zero.

A very large part of an effective security strategy is not about technology.
Technology is just an enabler. You need to decide on your risk appetite, establish your policies, and set up the governance for enforcing them. You need people with skills and experience, documented and tested processes, and the organizational capabilities to operate the technology you have.

Automation is useful – if you do it strategically

There's currently a lot of buzz in the market about automation and AI in security, and they certainly play an important part in increasing efficiency. But they're not a substitute for strategy.

If a piecemeal approach to security has left you with a critical gap in your processes, no amount of AI-powered automation will make up for it.

Coming up with an effective cybersecurity strategy is a balance between complexity and time. The larger the organization, the more complex it is likely to be, the broader its digital footprint, and the greater its risks. With the luxury of time, it would be possible for such an organization to develop an effective security strategy on its own. But who has the luxury of time, when advanced persistent threats are getting more sophisticated on a daily basis?

Most chief information security officers are not deep technical experts in all areas; their focus is on enabling teams and maintaining oversight. Even the best, in the largest organizations, generally need some help putting together and implementing their security strategy, given its complexity and the fact that time is against them.

You can tell the difference between an enterprise that has a sound security strategy and one which doesn't by how well they handle a big public breach. Organizations that haven't invested in security (to name no names) fail to communicate openly with their customers and suffer severe damage to the brand. Those that do, know what to say and what not to say, maintain their customers' confidence, and suffer less damage overall, even if the extent of the breach is greater.

Conclusion

In summary, if you want an effective security strategy, you can't rely just on one vendor:

- Before sourcing any technology, make sure you have a clear security strategy.
- You may be able to get a lot of the technology you need through your enterprise agreement.
- You will probably also need to get some technology from other vendors – but try to keep the number of vendors down.
- And not everything that makes up a sound security strategy is technology – policies, people, and processes are also essential.

In general terms, the best way for an enterprise to go about getting the most out of the security technologies they get with their Microsoft Enterprise Agreement, is to involve an experienced, independent security service provider.

This will enable them to avoid ending up with overlaps, gaps, or sub-optimal utilization of technology. It will help them deal with the scarcity of skills in cybersecurity in general. And it will provide them with a comprehensive, robust security strategy – and the ability to implement it.

We can help customers to reduce the number of vendors, minimize security detection gaps, and protect your organization 24/7.

To find out more about how Orange Cyberdefense can help with Microsoft Security, visit Security for Microsoft or get in touch with a Microsoft Security specialist via info@orangecyberdefense.com.

1. (ISC)^2 Cybersecurity Workforce Study 2022
2. The urgency of tackling Europe's cybersecurity skills shortage, March 23, 2022
3. Panaseer 2022 Security Leaders Peer Report
4. Cost of a data breach report, IBM, 2022

orange™ Cyberdefense