CONNECTING YOUR SECURITY TOOLS TO ENHANCE VISIBILITY, STRENGTHEN PROTECTION AND UNLOCK VALUE

YOUR JOURNEY TO A HEALTHY ECOSYSTEM

GUIDE
Getting the best from budgets

Although over half of organisations plan to increase cyber budgets in 2021, only 38% are very confident their cyber budget is allocated to the most significant cyber risks.²

And this lack of confidence may not be entirely misplaced. Despite today’s organisations spending more on security solutions than ever before, industry survey and breach rates show that there’s an opportunity to increase the effectiveness of standalone tools.

Heightening security needs a different approach. One that moves away from siloed solutions and independent technologies towards a more aligned, merged structure.
A SHIFT IN SECURITY MANAGEMENT

The changing landscape has had an impact on managing security, too. This is down to:

- **Evolving incident types**
  From a rise in home working to cloud adoption, working environments changed rapidly in spring 2020, and cyber criminals were quick to take advantage of gaps with new tactics, including timely social engineering.

- **Retaining talent**
  A widening skills gap leads to a stretched IT team with less resource for ongoing security management and threat response.

- **An expansive vendor landscape**
  Point solutions supported by different vendors create fragmented visibility and manual workflows.
SECURITY THAT RELEASES YOUR POTENTIAL

With challenges come opportunities, and among your security infrastructure there’s even more value to be found. But it requires aligning technologies to merge visibility and security coverage. Or, in other words, creating an integrated security ecosystem.

An integrated security ecosystem will help optimise cyber spend, increase efficacy and maximise your current investments. You’ll gain stronger, more accurate data and insights across your whole environment – enabling you to strengthen your security posture, better respond to threats and release greater value.

“While attackers are finding new, innovative ways to threaten the security of an organisation, holistic and complete security will give enterprises a chance to fight against any attack and protect their data.”

Forbes³

66% say security budgets have risen in the last year⁴

56% plan to increase cyber budgets in 2021²

64% aren’t very confident that they’re getting the best return on their cyber spend²

43% of breaches involved small businesses⁵

37% of UK companies have reported a data breach in the past 12 months¹
WHAT IS AN INTEGRATED SECURITY ECOSYSTEM?

An ecosystem is a group of technologies that work together to provide an outcome greater than the sum of its parts. Technology, all in harmony.

Implementing an integrated, reactive system enables your different component parts to detect, react to and contain an incident, and recover your network, on a single security platform, with less latency.

Disparate tools and solutions:

- HARD TO MANAGE
- MISSING A SECURITY INCIDENT
- MORE COSTLY
- REQUIRE ADDITIONAL TIME TO INTERROGATE DATA AND EXPLORE TRENDS
WHAT YOU CAN EXPECT

These are some of the elements that you’re likely to come across and benefit from on your journey to an integrated ecosystem.

ACCENTUATE
You’ll no doubt have already put many security measures in place at your organisation, and this approach will allow you to make the most of what you have to date.
By consolidating data points across systems, you can:
• Maximise what you already have in place
• Improve overall security
• Minimise human intervention

PRIORITISE
By joining the dots on your security assets, you can increase visibility of potential security incident levels and enhance your ability to respond to them. This leads to smarter threat prioritisation and decision making, based on real insights and data.

DELIVER
This is around identifying your mechanism for prioritisation and will depend on your requirements and status.
• Best of breed
  Technology that’s built by separate vendors and represents a deep specialism in a specific area or technology. These vendors focus on being experts in their chosen area
• Best of brand
  Technology that’s built by the same vendor and represents a wide range of areas, so you gain a broader set of tools within the same platform
• Best of both
  Technology that’s built by separate vendors and represents a deep specialism but acts and functions as an integrated platform
Your business is your world and every measure you’ve taken to protect it is a step in the right direction. What’s important now is keeping up that momentum. That means creating a balance between your changing business needs and existing security environment. Understand where you are now and prioritise what’s next for your business.

Take the five steps on your own individual path to a healthy ecosystem.

1. START YOUR BUILD

Deciding that an integrated security ecosystem is right for you sets you off to a great start.

Ask yourself:

- Where are you today?
- What’s important to your organisation?
- Where are you going?
- Where do you want to be?

Think of it like a security-based spring clean. Before making decisions about what to keep, you need to know what you have.

That means, you’ll want to understand the technology you have already deployed. Be self-critical and analytical about how well you’re using that technology – and don’t be shy about seeking guidance and input from your broader team.

This is an opportunity for you to consolidate and optimise, so it’s important you have a real and true overview of what’s in place and your priorities.

2. DECIDE YOUR PRIORITIES

Determine what you want your security ecosystem to look like and what outcomes you want to achieve.

- Are you trying to remove a number of different vendors?
- Do you want to eliminate the biggest and most complicated solution?
- Are you looking to retain the most valuable and remove the cheaper options?

Answering these questions will help you to work out your criteria for your consolidation. It’s a case of figuring out what brings the most benefits and keeps employees secure, compared with what only contributes to the clutter. Or, in other words, what ‘brings you joy’ when it comes to security.

There is no right or wrong answer here – your ecosystem will be as unique as your business.
3. GET GROUPING

Among your technologies, you might have some duplication of capabilities. This can lead to unnecessary spend, more complicated and time-consuming management processes and an overlap of data. The more siloed vendors, the harder it is to identify alerts.

Consider your spring clean, if you have two of the same things, you’ll likely want to remove the second item.

Look to where you can group technologies, depending on their purpose or features. This can help you to identify duplication and, in turn, spot opportunities to consolidate and streamline the platforms, vendors and consoles you’re working with. It’ll simplify how you detect and respond to incidents.

4. IDENTIFY TECHNOLOGIES

Now you’ve had a clear out, you might have noticed some spaces or functions that need to be filled.

If a new technology doesn’t natively integrate with what you already have, it’ll create siloed visibility and impact on your ability to detect security events – something you’ll have already worked to reduce in the last three steps. You’ll want to consider vendors and technologies that naturally integrate together and get the best from each solution’s capabilities.

There’s no one-size-fits-all with this. It’s entirely down to your unique business needs and priorities. Working with a vendor-neutral partner can help identify the right technologies.

5. KEEP AN EYE ON THINGS

Staying organised is an ongoing job. Define your roadmap and always check your progress. Once you’ve got your roadmap in place, you can measure yourself against it and monitor whether the right things have changed. And if they have, by how much.

You can share this progress with the wider business to support future funding, build more trust and get backing for any projects further down the line.

ONLY 31% of UK organisations have done a cyber risk assessment in the last 12 months. 
SECURITY THAT PROTECTS YOUR WORLD

A cybersecurity approach to call your own.

An integrated security ecosystem makes it possible to optimise your existing investments and do more with less, while prioritising what’s important to your organisation. And with Softcat, creating this perfect balance means taking a personal approach that’s realistic and relevant to you.

By really getting to know your business, we can review, analyse, streamline, plan and support your security measures. That’s how we’re able to wrap a protective layer around your exact business, its users, devices and digital workspaces.

Why Softcat?
Real, relevant value. That’s what you get with us.
Here’s what we do:

- **Better choice**
  Our diverse portfolio makes us best placed to advise on what technology integrates well, and our services and skillset mean we can help deploy those capabilities.

- **Dedicated expertise**
  The power of our scale and network means we can share all insight and learnings with you. You’ll be backed by a team that’s dedicated to security and an account manager that supports your individual requirements. We want to make it easy to work with us.

- **Vendor-neutral**
  We look for the best solution within our portfolio – without being restricted to just one vendor option.

- **Cost effective**
  We can help you lower total cost of ownership by providing comparative analysis, which helps you review different options, and informed guidance based on our detailed knowledge of all the different software packages available.

- **Work closely together**
  to make any necessary improvements

- **Invest in real partnerships**
  to build on the progress you’ve made and create better security environments

- **Be on hand with help, advice and deep expertise**
  so you always feel confident

- **Set you on a path**
  to joined-up protection around your business
SECURITY THAT’S GOT YOU COVERED

**Softcat assessments** can help you understand your current status and what’s next for your organisation. We’ll support you with:

**Cyber assessment services**
We offer an ongoing programme to help mature and improve your cyber security over time. Tailored and flexible, it will evaluate your security posture to:

- Deliver a baseline of current state
- Form a desired state
- Deliver the required commercial and technology efficiencies to achieve your goals

**Commercial assessment**
We work with you to understand where your security posture is today and the commercial efficiency of your tools. Once we have this information, we:

- Analyse the data to understand how your tech is being used
- Report on current and potential utilisation
- Look at best practice negotiations for agreements and vendor consolidations
- Issue recommendations for improvements

Release longer-term value and connect independent technologies and make sure your security environment can always go one better.

Protect your world with Softcat.

To find out more about how we can help you secure your organisation, contact your Softcat Account Manager.
CONTRIBUTOR OVERVIEW

To help inform this guide, we’ve held in-depth conversations with two of our experts to talk about the key areas that organisations need to consider when building an effective Cyber Security Ecosystem. Both offer a wealth of experience within the security space.

ADAM LOUCA
Chief Technologist – Security
Softcat

Adam focuses on developing, engaging and transforming Softcat’s strategic customers’ cyber security approach. In addition, he also runs Softcat’s cyber assessment services business, which helps customers understand and improve their cyber security.

TREVOR HIGHLEY
Specialist Sales Manager
Softcat

Trevor has over two decades of experience partnering with customers to help them build long-term strategies that deliver a security approach that both protects their business and simultaneously ensures that their employees are able to work in an agile and productive manner. He has spent time working with key vendors in various go to market leadership roles and is now responsible for Softcat’s go to market cyber customer strategy, which is designed to help customers in a practical manner.

Sources: 1 CSO online  2 PwC  3 Forbes  4 CSO online  5 Verizon  6 gov.uk