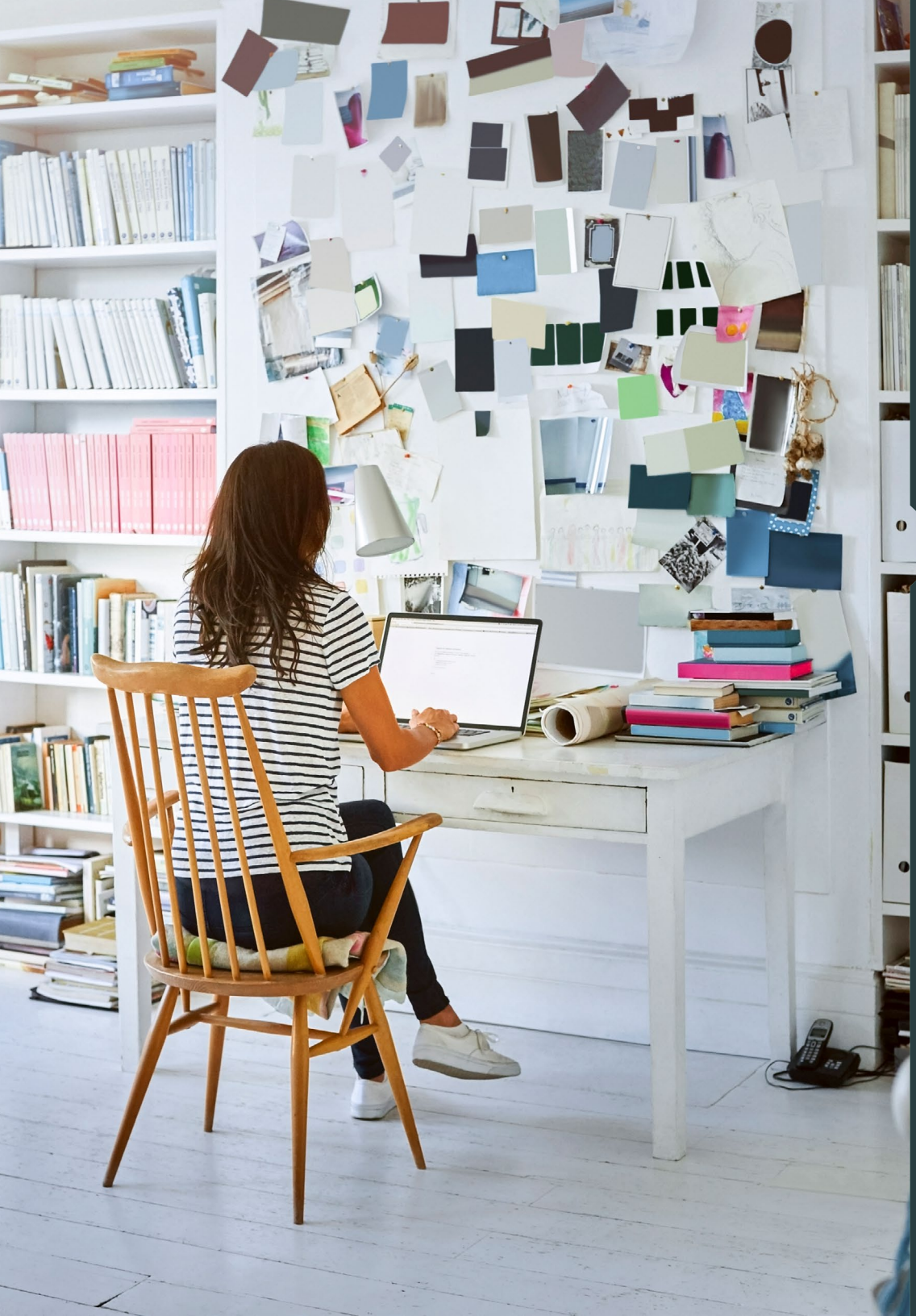


servicenow

All together now

How IT and security teams can collaborate better to drive operational resilience.

START ⟫

servicenow

The perfect storm

In 2020, security just got a whole lot harder. Cybercriminals ramped up activity, eager to capitalize on confusion and profit from the pandemic.

Phishing emails disguised as urgent messages about COVID-19 increased by almost 6,654% over a two-month period. Since January, there were over 100,000 coronavirus-related domains registered globally – with a 50% higher chance that these domains could host malware.

That's on top of longstanding threats like ransomware, which is forecast to make more than $1.3 billion for cybercriminals this year, and business email compromise scams which cost victims over $1.7 billion in 2019.

Not only have the threats increased in volume and velocity, but the majority of organizations have responded to the crisis by enabling their people to work from home, creating the "perfect storm". With a distributed workforce, the traditional network perimeter all but vanished. From an operational perspective, it was an essential move, but from a security perspective, it created a much larger surface area to protect.

The need to act fast and respond to risks and threats has never been greater. And time is a luxury that security teams don't have: it takes on average 73 days to contain a breach, and the average total cost is $3.92 million.

servicenow

You can't fix what you can't see

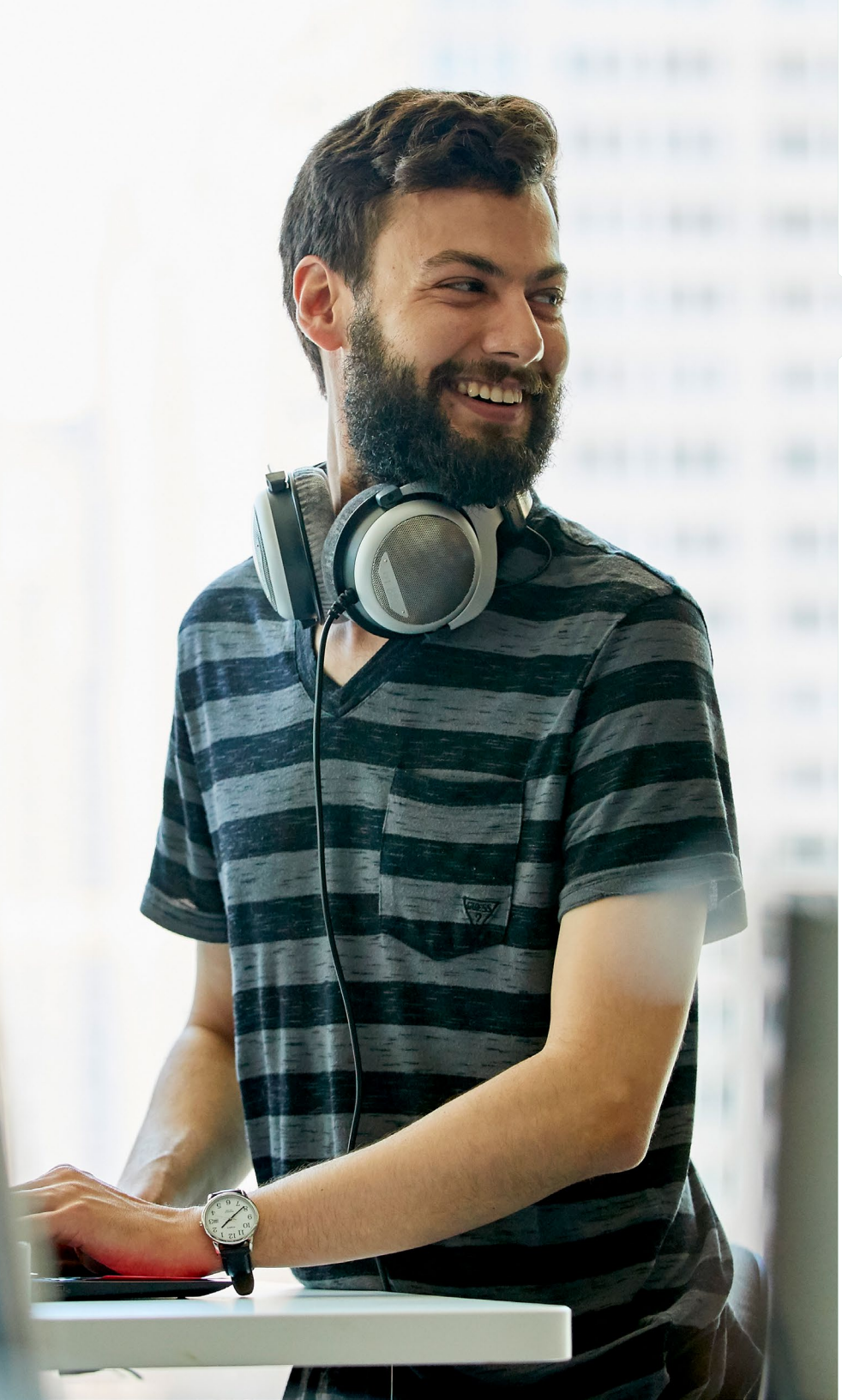
Securing and protecting an organization's most important assets, and reducing the risk of financial loss and reputational impact, is more critical than ever. But in order to prioritize actions and respond effectively, IT and security teams need visibility into the incidents and the business context.

Many organizations are hindered by ongoing issues including:

- Siloed data
- A lack of resources
- Not patching known vulnerabilities
- Reliance on manual processes
- Minimal cooperation between security and IT teams.

These roadblocks reduce the speed of response to new threats that are emerging all the time, further compounding the problem:

- An incomplete understanding of their threat landscape
- An inability to prioritize threats quickly and accurately
- A response that's too slow and too siloed to prevent impact to the business



servicenow

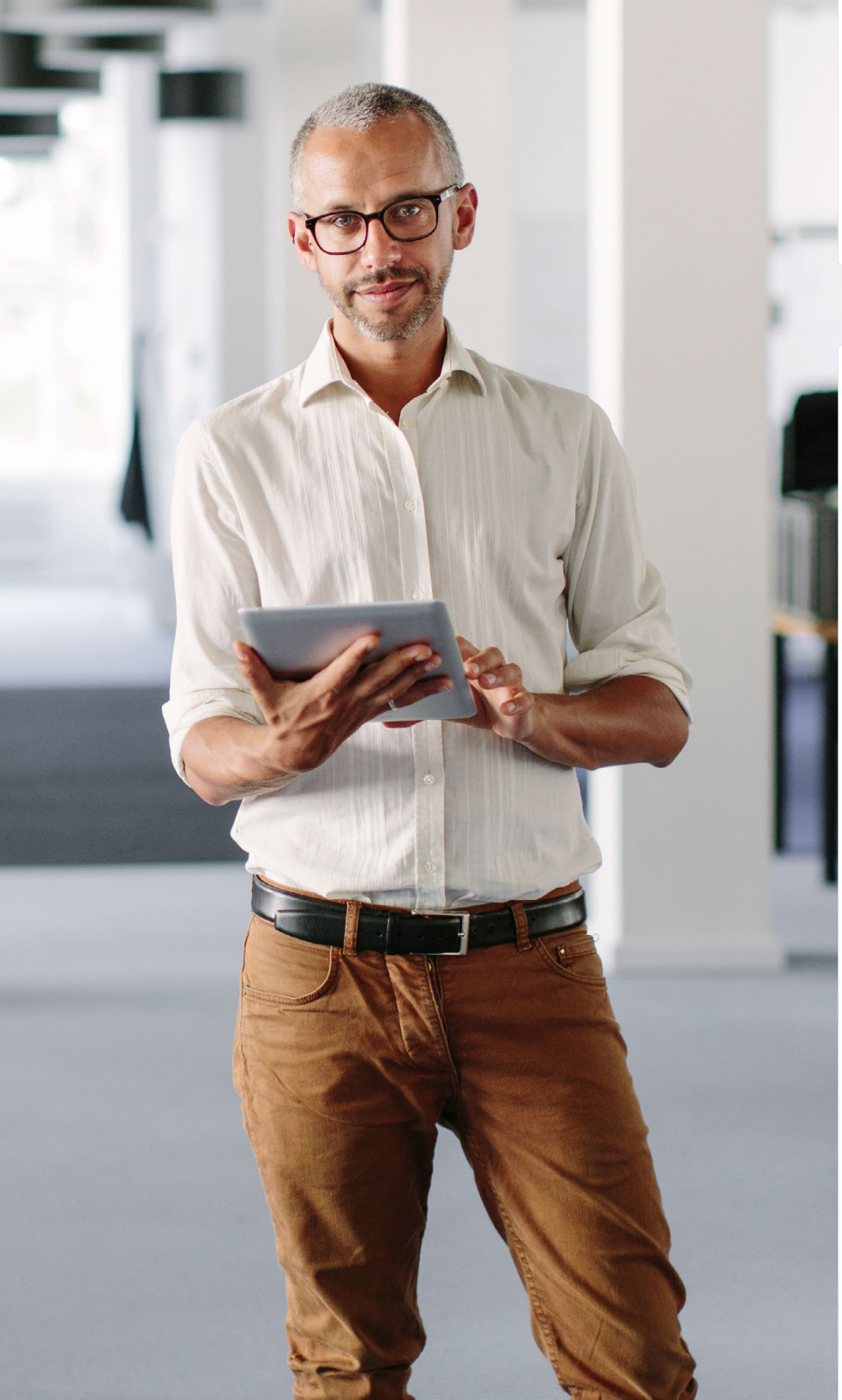
Remove the roadblocks to resilience

As you start building a more resilient organization, you need confidence at every stage of the journey. This calls for closer collaboration between security and IT teams to maximize productivity and minimize risks.

That's where the closed loop approach comes in. It's a way to create a truly resilient organization that can protect itself, regardless of what's happening in the wider environment. It's a four-step approach that lets you:

- Gain visibility of incidents to control them better
- Plan and prioritize essential tasks by importance
- Optimise and collaborate on risks and threats to the organization
- Enable productivity between teams across the enterprise.

We'll cover each of these four core aspects in the following pages. But first, let's look at the concept that ties them all together.



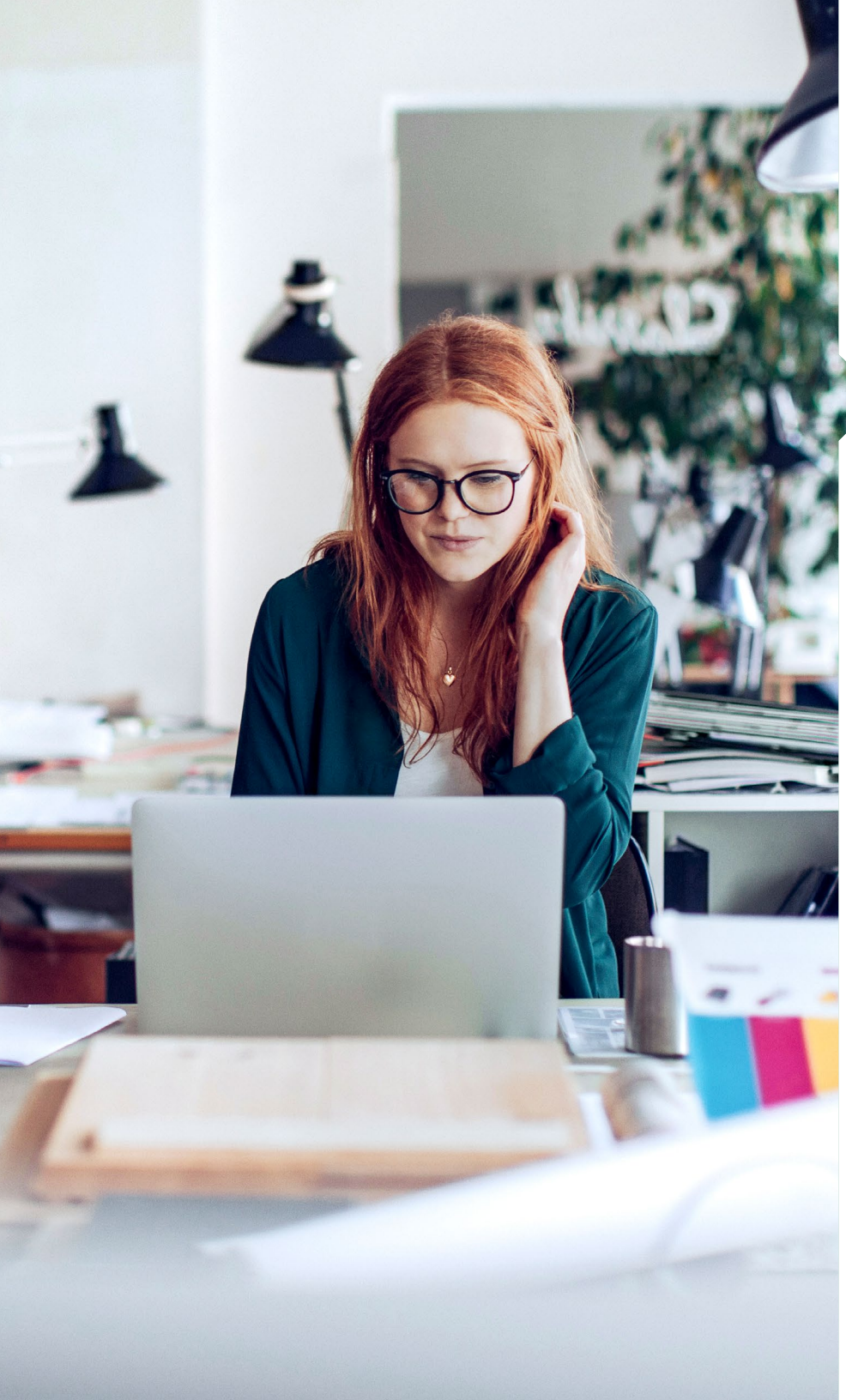
servicenow

Responses at machine speed

Organizations rightly worry about the financial cost of a data breach. When you're stuck with manual processes and insular workflows, it's much harder to react fast, and it's harder to know what worked so you can repeat it the next time.

That's where automated security solutions that leverage artificial intelligence, machine learning, security analytics, and orchestrated incident response can help. They minimize the need for human intervention and are proven to reduce the costs associated with a security incident or data breach.

Automating workflows together with sharing data and actions between security and IT teams, helps ensure that threats to your business are resolved before they can impact the business.



servicenow

Time is money

Automation and collaboration drives efficiency of response and builds operational resilience: 80% of organizations with automation report that they can respond to vulnerabilities in a shorter timeframe.

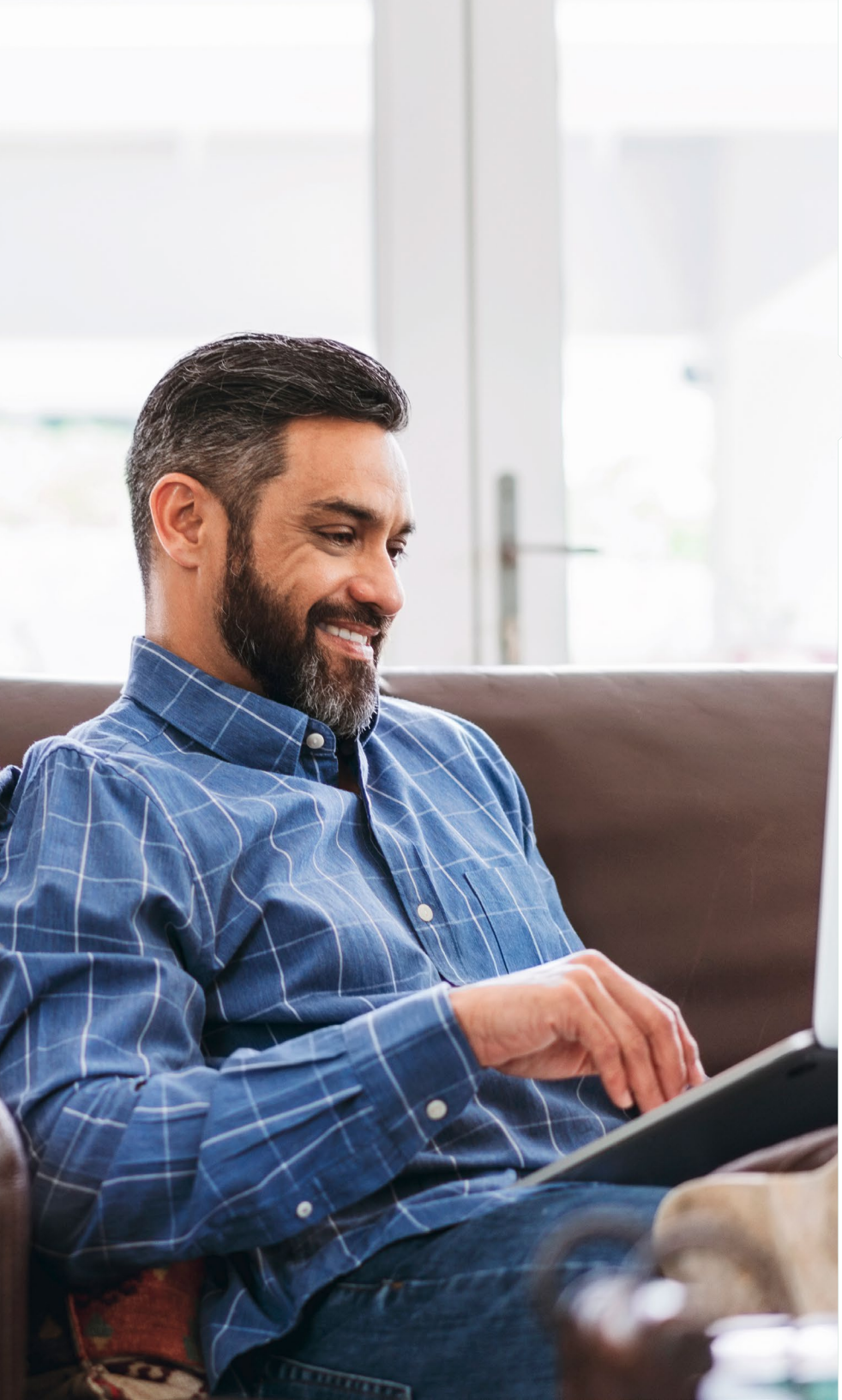
For organizations with no security automation, breach costs were dramatically higher than for organizations with fully-deployed automation ($5.16 million average total cost of a breach without automation vs. $2.65 million for fully-deployed automation).

And the trends are only going one way: average breach costs at organizations with no automation were higher in 2019 than in 2018 (up more than 16% from $4.43 million to $5.16 million).

Breaches at organizations with fully deployed automation decreased in cost from 2018 to 2019. Those breaches decreased in cost by 8 percent, from an average of $2.88 million in 2018 to $2.65 million in 2019.

Challenge	Solution	Tools
Siloed data **76% of organizations have no common view of assets and applications across security and IT** Some of the biggest security threats exploit known vulnerabilities. But when the average SOC contains 75 different tools, all generating alerts, it's hard to distinguish the signals from the noise, and harder still to escalate issues to the right people to take action quickly and reduce the risk of downtime.	**Plan and prioritize essential tasks by importance** With complete visibility, security teams know their security posture and gain the business context they need to identify high-impact threats amongst all the noise happening at the moment, to keep operations running smoothly.	**Security Incident Response** Simplifies identification of critical incidents and provides workflow and automation tools to speed up remediation. It connects the workflow and systems management capabilities of the Now Platform™ with security data from leading vendors to give your teams a single platform for response that can be shared between security and IT. **Vulnerability Response** Efficiently prioritize patching efforts by linking them to business impact. With orchestration, automation, and better visibility, teams can respond more efficiently, reducing business risk.
Lack of resources **82% of employers say they lack sufficient cybersecurity skills.** Manual processes are holding back the ability to continuously monitor changes to threats and vulnerabilities and new ones as they arise. With security talent in high demand, many organizations don't even have the luxury of throwing more bodies at the problem.	**Continuously monitor** By using automation, you can identify security changes in real time and respond at machine speed in order to prioritize the most pressing threats and vulnerabilities – making the best use of the resources you already have.	**Security Incident Response** Simplifies identification of critical incidents and provides workflow and automation tools to speed up remediation. It connects the workflow and systems management capabilities of the Now Platform™ with security data from leading vendors to give your teams a single platform for response that can be shared between security and IT. With orchestration, automation, and better visibility, teams can respond more efficiently, reducing business risk. **Integrated Risk Management** Enable fine-grained business impact analysis and appropriately prioritize and respond to risks. **Vulnerability Management** Systems scan your assets to identify vulnerabilities, or weaknesses that can be exploited and potentially lead to a breach.

Challenge	Solution	Tools
Cross-department collaboration 62% of breached organizations were unaware that they were vulnerable to a data breach. With many teams now geographically dispersed due to new working norms, the opportunity for closer collaboration isn't there. The siloed nature of departments hinders efforts of security and IT to collaborate and share information.	**Optimise and collaborate on risks and threats** Create open workflows across security and IT teams, enabling faster response by reducing cumbersome processes and manual handoffs during response and remediation.	**Security Incident Response** Simplifies identification of critical incidents and provides workflow and automation tools to speed up remediation. It connects the workflow and systems management capabilities of the Now Platform™ with security data from leading vendors to give your teams a single platform for response that can be shared between security and IT. **Vulnerability Response** Efficiently prioritize patching efforts by linking them to business impact. With orchestration, automation, and better visibility, teams can respond more efficiently, reducing business risk and scaling team capacity.
Over-reliance on manual processes 56% of organizations say events slip through the cracks because they use emails and spreadsheets for incident response. An inability to identify the root cause of past events to improve controls, policies and strengthen operations. This results in the same risks and threats recurring, which means repetitive, manual work required from security teams.	**Smarter, repeatable response measures** Automate cross-functional workflows and evidence collection, and put an end to time-consuming and error-prone processes: email, spreadsheets, and phone calls.	**Security Incident Response** Simplifies identification and response of critical incidents and provides workflow and automation tools to speed up remediation. It connects the workflow and systems management capabilities of the Now Platform™ with security data from leading vendors to give your teams a single platform for response that can be shared between security and IT. **Vulnerability Response** Efficiently prioritize patching efforts by linking them to business impact. With orchestration, automation, and better visibility, teams can respond more efficiently, reducing business risk and scaling team resources.

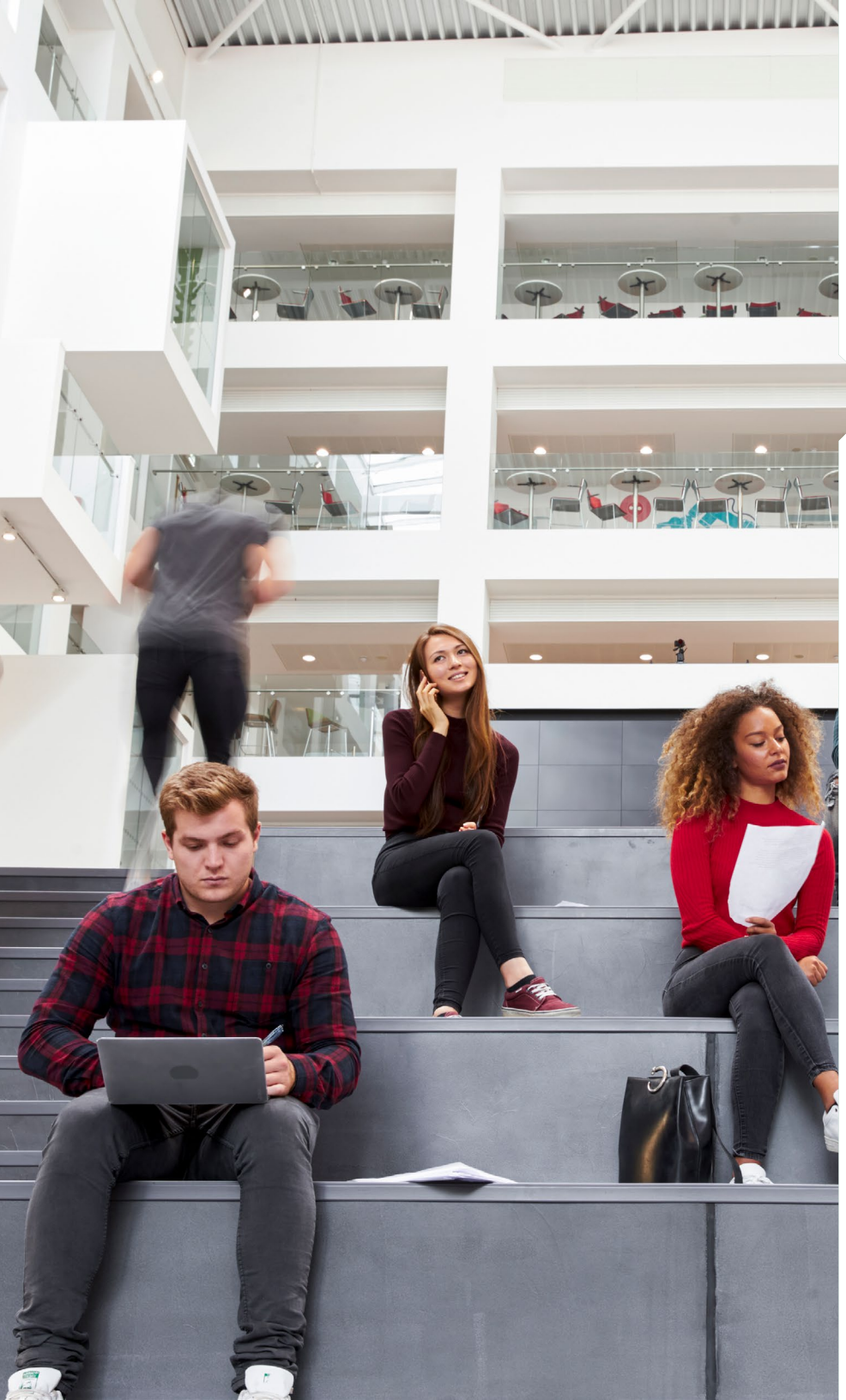


We can work it out

When security and IT are working in harmony, they're able to drive continuous improvement so the business can always stay one step ahead of the latest threats.

Use accurate and repeatable processes to customize playbooks and policies for smarter, automated responses that unlock new efficiencies. This creates a culture that never stops learning, adapting and reporting, which ultimately leads to stronger, futureproofed security operations.

You can be secure in the knowledge that by pairing human action with AI and automation, you've got all angles covered, no matter what the threats are, or where your teams happen to be.



Automation in action: real-world success stories

Reduced response times

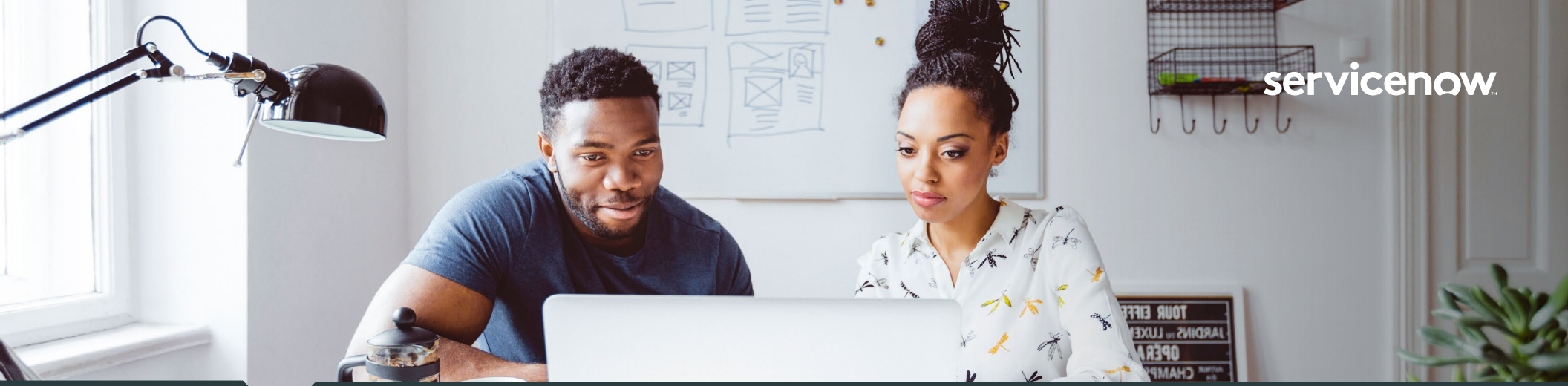
AMP, an Australian financial services company, partnered with ServiceNow for a security operations solution that led to a 60% reduction in time to respond to and patch vulnerabilities.

Faster security investigation

With Threat Intelligence, international IT services company DXC halved the time needed to investigate security incidents.

Increased efficiency

Using the automation in its own products, ServiceNow helped its security team to handle 50% more cases.



Getting better all the time

ServiceNow delivers business context and problem severity insights on a single platform, so you get a rapid, accurate assessment of the problem. This helps you:

- **Focus** your efforts on the incidents with the biggest potential impact
- **Prioritize** security incidents and vulnerabilities by business criticality
- **Improve** decision making for faster and more effective response efforts
- **Align** the right data with the right people
- **Track** incidents and assigns tasks to the correct responders
- **Ensure** tasks are completed on-time

NOW's Security Operations is a single integrated platform that enables your teams to quickly correlate security events, identify dependencies across systems and automate tasks and system workflow interaction across the enterprise to prioritize and align responses to threats and vulnerabilities before your business is impacted.

By leveraging the power of Security Operations and IT solutions together, teams can respond faster and more efficiently, reducing business risk.

Technology isn't about replacing humans in security; it's about empowering them to work better.

View Now

« BACK