

BEYOND THE OFFICE: FINDING GAPS

*A Practical Guide to Seeing What May Be
Missing Across Your Bigger Security Picture*

The boundaries of your business no longer end at the office. Work moves across locations, platforms, devices, and outside relationships, creating more connections to understand and protect.

In June 2026, Microsoft identified an automated business email compromise campaign that reached more than 67,000 users across more than 42,000 organizations in less than three hours.

EXECUTIVE SUMMARY: THE VISIBILITY GAP

Cybersecurity gaps do not always begin because a safeguard is missing. They can develop as the business changes around protection that was designed for an earlier version of the environment.

A new application adds another place for company information to live. A change in responsibilities can leave permissions behind. A vendor relationship can introduce outside access. A new device can connect employees to resources that once stayed inside the office. Individually, these are ordinary business changes. Together, they can make the bigger security picture more difficult to follow.

That is the visibility gap this guide is designed to explore.



The objective is not to create a longer list of security concerns. It is to create enough visibility for leadership and IT to understand where the picture remains clear and where another look may be worthwhile.

You cannot make confident security decisions until you can see the bigger security picture.

WHAT THIS HELPS YOU EXAMINE

USERS & IDENTITIES

Understand who can access systems and whether permissions match responsibilities.

DEVICES & ENDPOINTS

See which equipment connects to company resources.

CLOUD APPS & DATA

Follow where important information moves.

VENDORS & THIRD PARTIES

Identify outside organizations that connect to systems.

*You cannot make
confident security
decisions until you can
see the bigger security
picture.*

1. YOUR SECURITY PICTURE HAS MORE EDGES THAN IT USED TO

There was a time when business technology had easier boundaries to recognize. Employees worked primarily from company locations, information stayed on systems managed inside the organization, and access to important resources often depended on being connected to a familiar network.

That model has changed. Among U.S. employees with remote-capable jobs, 52% work in a hybrid arrangement and another 26% work exclusively remotely according to Gallup's May 2026 data.

YOUR BUSINESS HAS ONE ADDRESS. YOUR TECHNOLOGY DOES NOT.

The important change is not simply that businesses use more technology. It is that the relationships between people, systems, information, and outside organizations now extend much further.

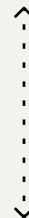
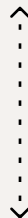
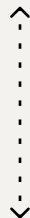
A person may begin the day using a company laptop from home, access a cloud platform, collaborate with a customer, and later continue working from another location.

None of these actions automatically represents a security problem. They represent the connected world in which business now operates.

YOUR CONNECTED BUSINESS



SYSTEMS & COMPANY DATA



Looking at each part separately can tell you whether a safeguard exists. Looking across the environment tells you whether that protection remains visible from one connection to the next.

That difference matters because a cybersecurity gap may not be an obviously unprotected system. It may be a place where access, responsibility, ownership, or visibility becomes less clear as the business changes.

2. WHERE CYBERSECURITY GAPS BEGIN TO FORM

Some gaps are easy to identify because something is obviously absent. An account lacks stronger authentication. A device has fallen behind on updates. A backup process has not been established.

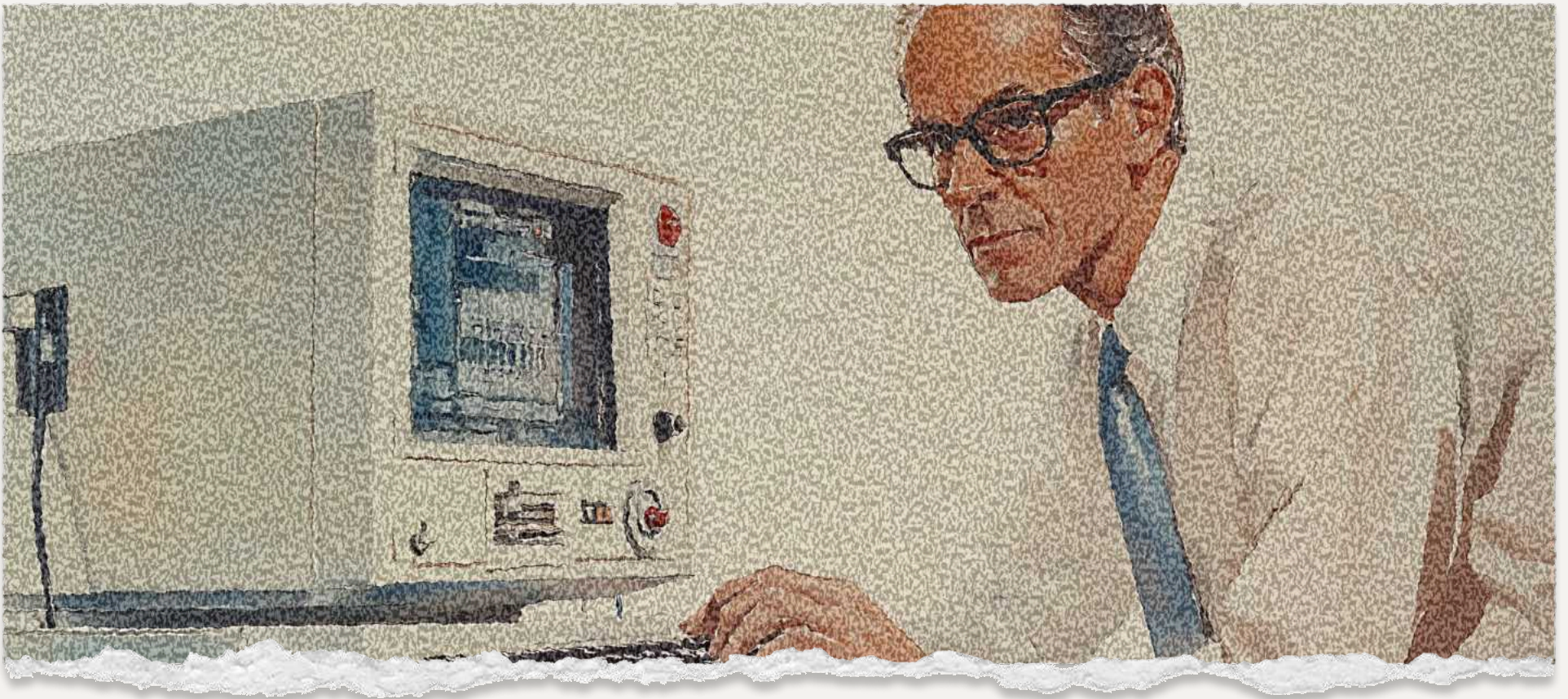
The harder gaps can appear inside environments that already have solid protection. They develop gradually as the organization hires people, changes responsibilities, adopts software, adds vendors, replaces equipment, expands locations, and gives employees new ways to work.

A Gap Can Begin With an Unanswered Question

Each business change may make sense by itself. The difficulty appears when no one steps back to examine how those changes have altered the complete environment.

ASK	WHAT IT MAY REVEAL
Who still has access?	Permissions may remain after an employee changes responsibilities.
Which devices can connect?	Different equipment may be operating under different management standards.
Where does company information live?	New platforms may have introduced additional storage and sharing locations.
Which vendors can enter the environment?	Access established for an earlier project may still be active.
Who owns the security decision?	IT, business departments, and outside providers may each control a different part of the same system.

These situations do not prove that an organization is insecure. They show where context may have become incomplete.



Look for Change Before Looking for Failure

A productive review should therefore begin with business change rather than a search for mistakes. Consider what has happened across the organization since the last time the environment was examined as a whole:

- Have new employees or contractors joined?
- Have people moved into different roles?
- Have teams adopted additional cloud platforms?
- Have vendors gained or changed access?
- Have new locations, devices, or workflows been introduced?
- Has important information begun moving through different systems?

THE QUESTION IS NOT WHETHER THE ORGANIZATION HAS DONE SOMETHING WRONG. IT IS WHETHER THE SECURITY PICTURE HAS KEPT PACE WITH THE WAY THE BUSINESS NOW OPERATES.



FOLLOW THE INFORMATION

Not just the application.

BEFORE INFORMATION MOVES, UNDERSTAND THE DESTINATION

The purpose is not to slow down useful technology. It is to prevent valuable applications from becoming parts of the business that no one can clearly place inside the security picture.

3. USERS & IDENTITIES: FOLLOW THE PERSON, THEN FOLLOW THE ACCESS

People sit at the center of many technology connections. Their identities open applications, provide access to data, connect devices to business resources, and determine what they are allowed to do once they are inside a system.

That means identity security cannot stop at confirming that the correct person signed in. The deeper question is whether the access behind that identity still matches what the person needs today.

Microsoft's own security work illustrates why the distinction matters. In July 2026, the company reported that the most consequential security failures rarely come from one missing control, but from identity gaps, unmanaged assets, and inconsistent configurations that can be chained together into larger attack paths. That makes understanding the access behind an identity just as important as knowing that authentication exists.

Access Changes as People Change

An employee may join one team, take on a new project, move into another department, or receive temporary access to complete a specific responsibility. Each change can add permissions.

Removing permissions can be less visible because the employee may continue working normally even when old access remains.



Look Beyond the Login

Multifactor authentication strengthens identity protection, but it is one part of a larger picture. Leadership and IT should also understand where stronger authentication applies, which accounts hold greater privileges, and whether exceptions still have a valid purpose.

QUESTIONS TO BRING INTO FOCUS

- **Can every active account be explained?** Each identity should connect to a person, system, service, or current business need.
- **Do permissions match current responsibilities?** Access accumulated through earlier roles or projects deserves review.
- **Who has elevated privileges?** Administrative access should have a clear reason behind it.
- **What happens when responsibilities change?** A role transition should change access as deliberately as onboarding created it.
- **Where does stronger authentication apply?** Exceptions should be understood rather than simply inherited.
- **Can unusual use be recognized?** The organization should have a way to notice when an identity is being used outside its expected purpose.

The objective is not simply to count accounts. It is to understand the doors each identity can open and whether those doors still belong in the current security picture.



4. DEVICES & ENDPOINTS: SEE WHAT TRAVELS WITH YOUR PEOPLE

The technology employees use now travels with them. Laptops move between homes, offices, customer locations, and other networks. Mobile devices connect to email and files. Remote employees rely on equipment outside the traditional office perimeter. Specialized hardware may remain in service because an operational process still depends on it.

Each device creates another connection between your people and the systems they need to do their work.

Knowing a Device Exists Is Only the Beginning

An inventory can tell IT what equipment the company owns. A security picture needs to answer more.

Is the device managed? Is it receiving updates? What systems can it access? What information can it store? Does the organization have the same visibility when that device is away from the office?

DIFFERENT DEVICES CREATE DIFFERENT QUESTIONS

Company Managed Laptop	Whether expected protections, policies, and updates remain in place.
Remote Endpoint	Whether visibility continues when the equipment operates away from a company location.
Mobile Device	Which business services and information it can access or synchronize.
Specialized Hardware	Whether older or purpose built equipment can support current safeguards.
Outside Device	What resources it is allowed to reach and under which conditions.

The goal is not to treat every device as a threat. Different devices simply create different levels of visibility and control.

Move Beyond “How Many Devices Do We Own?”

**A BETTER QUESTION IS: CAN WE ACCOUNT FOR THE DEVICES THAT
CAN REACH THE BUSINESS?**

That includes more than laptops purchased by IT. It includes equipment that employees, contractors, locations, applications, or operational processes use to connect to company resources.

If a device can reach the business, it belongs somewhere in the security picture.



5. CLOUD APPLICATIONS & DATA: FOLLOW WHERE INFORMATION GOES

Cloud applications have changed how information moves through an organization. A file may begin in email, move into a collaboration platform, enter another business application, and later be shared with an outside party.

Each step can support legitimate work. Each step can also change who can see the information, who controls access, and where responsibility sits.

Follow the Information, Not Just the Application



AT EACH STEP:

WHO CAN SEE IT?
WHO CAN SHARE IT?
WHO CONTROLS ACCESS?

When a team adopts a new cloud service, attention naturally focuses on what the application allows them to accomplish. Security introduces a different set of questions.

Before Information Moves, Understand the Destination

- **What information will enter the platform?** Not every application handles the same type of business data.
- **Who can access it?** Internal users, administrators, outside collaborators, and vendors may have different levels of visibility.
- **Can information be shared externally?** Sharing settings can expand the audience beyond the organization.
- **Who controls configuration?** Responsibility may sit with IT, a department, or the software provider.
- **What happens when the service is no longer needed?** The business should understand what remains and where it goes.

The purpose is not to slow down useful technology. It is to prevent valuable applications from becoming parts of the business that no one can clearly place inside the security picture.

Start With the Information That Matters

Trying to map every file would create noise. Begin instead with information that supports important business activity.

That may include customer records, financial information, employee documents, contracts, intellectual property, operational files, or credentials.

Then trace the route:

- **Where does the information begin?**
- **Which systems process it?**
- **Where is it stored?**
- **Who can share or download it?**
- **Which outside organizations receive it?**
- **Where does responsibility change?**

When you know where important information travels, you gain a better view of where protection needs to travel with it.

The Visibility Gap

ORDINARY BUSINESS CHANGES

TOGETHER, THEY CAN MAKE THE BIGGER SECURITY PICTURE
MORE DIFFICULT TO FOLLOW.

6. VENDORS & THIRD PARTIES: SEE WHO ELSE CONNECTS

Your organization is not the only one interacting with its technology. Software providers, consultants, support companies, professional services firms, contractors, and other partners may need legitimate access to systems or information.

Those relationships are part of how businesses operate, but they also expand the number of connections the security program needs to understand. A 2026 study published by Elsevier examined 161 documented software supply chain incidents and identified 19 distinct types of attacks across those environments. The finding points to something broader than software alone: outside relationships can introduce different paths into the same business environment, making visibility into access and dependencies increasingly important.

Every Outside Connection Needs Context



A provider responsible for infrastructure may need broader access than a contractor working inside one application. A consultant supporting a temporary project may need permissions for a defined period rather than indefinitely.

The important point is not that every outside connection creates a problem. It is that every connection should have a reason, a boundary, and an owner.

FOUR QUESTIONS CAN BRING THIRD PARTY ACCESS INTO FOCUS

- **Who has access?** Know which outside organizations and individuals can reach systems or information.
- **Why do they have it?** The permission should connect to an active business purpose.
- **What can they reach?** The organization should understand how far that access extends.
- **When was it last reviewed?** Access that once made sense may no longer match the relationship today.

Application integrations deserve the same attention. Two systems can exchange data automatically for years without a person actively signing in. That connection may be invisible during day to day work but still belong in the security picture.

If another organization can reach your systems, applications, or information, it is already part of your connected world. The question is whether you can see that relationship clearly.

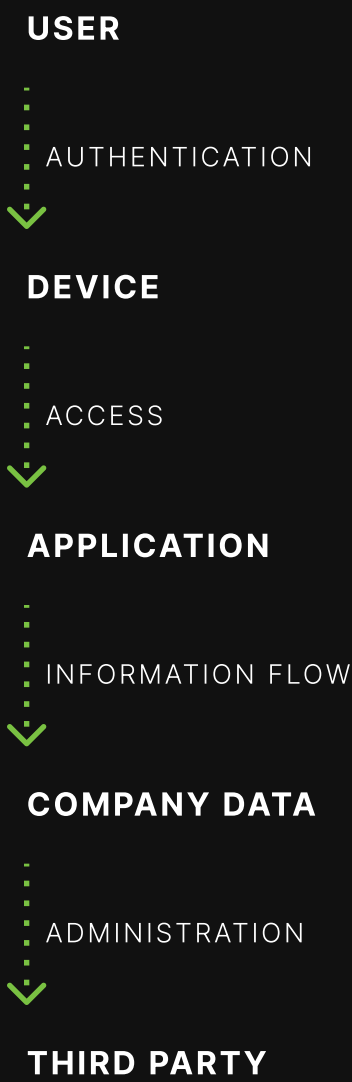
7. THE SPACE BETWEEN THE CONNECTIONS

Users. Devices. Applications. Data. Vendors.

Each can be examined separately. But the gaps that are hardest to recognize often appear where those pieces meet.

A user signs in from a device. That identity opens an application. The application contains company information. A vendor may administer part of the platform. Every individual component may have its own safeguard while questions remain in the handoff between them.

Protection Can Exist While the Connection Remains Unclear



That is why reviewing cybersecurity product by product can miss part of the story.

A company may use multifactor authentication, but not every application may follow the same access path. A laptop may be carefully managed while information from that device can still move into another platform with different sharing rules. A vendor may have legitimate access even though the original permission level has not been reconsidered recently.

None of these situations requires a complete security failure. They require the organization to look across the handoffs.



ASK A BIGGER QUESTION

INSTEAD OF ASKING ONLY...	ASK...
Do we have endpoint protection?	What can this device reach after someone signs in?
Do we use MFA?	Where does stronger authentication apply and where are the exceptions?
Do we protect cloud applications?	What changes as information moves between platforms?
Do we review vendors?	What can each outside party reach today?
Do we have security tools?	Can we see how those tools connect across the environment?

Cybersecurity tools solve specific problems. The bigger security picture shows whether those protections remain clear as one connection becomes another.

8. BUILD YOUR CONNECTED BUSINESS SECURITY PICTURE

You do not need to begin by buying another security product or replacing technology that already works. Begin with the environment the business already has.

Bring the major connections into one view, then work outward from the people, systems, and information the organization depends on.

The Connected Business Security Check

AREA	LOOK AT	ASK
People & Identity	Employees, administrators, contractors, accounts, and permissions	Does access still reflect current responsibilities?
Devices	Company equipment, remote endpoints, mobile devices, and specialized hardware	Can we account for what connects and how each device is managed?
Applications	Core platforms, cloud services, department software, and integrations	Do we know which systems are part of the environment and who controls them?
Data	Important information and the places through which it moves	Can we follow where information is stored, shared, and accessed?
Third Parties	Vendors, consultants, partners, and external integrations	Do we understand why each outside connection exists and what it can reach?
Connections	The places where people, devices, applications, data, and outside access meet	Does protection remain visible from one part of the environment to the next?

Use the Check to Create a Shared View

The purpose of this exercise is not to produce an engineering diagram of every technical dependency. It is to give leadership and IT a common view of the environment.

Technology teams can explain how systems work, why access exists, and where technical limitations may apply. Business leaders can add the context behind customer requirements, operational priorities, growth plans, and important business processes.

Together, those perspectives turn isolated technical observations into a clearer understanding of the environment.

Once the connections are visible, the organization is in a stronger position to ask what deserves a closer look.

9. GIVE YOUR IT TEAM MORE BEHIND THEM

An experienced internal IT team carries context that an outside provider cannot replace. They know the systems employees depend on, the reasons behind earlier technology decisions, the projects already underway, and the operational realities that do not appear on a network diagram.

That knowledge should remain central to the security conversation. Additional cybersecurity expertise should strengthen it, not work around it.

More Expertise Can Add a Different View

Internal technology teams balance user support, infrastructure, projects, vendors, systems, and business requests alongside cybersecurity responsibilities. Some security questions require additional depth or dedicated attention that may be difficult to maintain while all of those responsibilities continue.

That is where added cybersecurity expertise can become useful.

WHAT MORE BEHIND YOUR IT TEAM CAN LOOK LIKE

MORE PERSPECTIVE	MORE DEPTH	MORE CAPACITY
Another experienced view can help examine assumptions and connections that are difficult to evaluate from inside the environment every day.	Specialized cybersecurity knowledge can support questions involving identity, monitoring, cloud environments, incident readiness, and risk requirements.	Internal IT can gain additional resources for security work while continuing to support users, systems, projects, and operational priorities.

The Goal Is Not More Technology for Its Own Sake

A security partner should first understand what is already in place.

That means asking:

- Which safeguards are already working well?
- Where does the internal team already have strong visibility?
- Which areas require deeper expertise?
- Where does responsibility become less clear?
- Which questions are difficult to answer with the information available today?

For IT, this creates more support behind work already in motion. For leadership, it brings another layer of context to future security decisions.

The starting point is not assuming what needs to change. It is understanding enough of the environment to know where another look is worthwhile.



10. SEE THE BIGGER SECURITY PICTURE

Your business operates in a connected world shaped by people, technology, information, and relationships that extend far beyond a single location. You may already have strong safeguards across much of that environment, supported by people who understand your business and systems well.

The next opportunity is to see how those protections connect.

Follow the people who access your systems. Account for the devices they use. Trace important information as it moves between applications. Understand which vendors enter the environment and why. Then look at the spaces where those connections meet.

The Journey From Visibility to Better Decisions

SEE THE CONNECTIONS



ASK BETTER QUESTIONS



FIND THE GAPS



UNDERSTAND THE
BIGGER PICTURE



DECIDE WHAT
DESERVES ATTENTION

A clearer security picture does not mean that every finding demands action. It gives leadership and IT the context to separate what is already working from what may deserve more examination.

That leads naturally to the next question in the journey:

WHICH CYBERSECURITY RISKS DESERVE ATTENTION FIRST?

The answer begins with visibility. Before deciding where to invest, strengthen, or change, the organization needs to understand what is already in place and how well that protection reflects the world the business operates in now.

BRING YOUR SECURITY PICTURE INTO FOCUS

SinglePoint Global works alongside business leaders and technology teams that already have systems, safeguards, internal expertise, and priorities in motion. Our role is to help bring those pieces into a clearer security picture, examine where protection may become less visible, and add cybersecurity expertise behind the teams already responsible for the environment.

The conversation begins with what you already have and the questions that remain around it. What is working well? What has changed? Where has the business extended beyond the environment you last reviewed? Which connections deserve another look?

Understanding those answers creates a stronger starting point for every security decision that follows.

**SEE THE BIGGER SECURITY
PICTURE**

LANDING PAGE



**TALK WITH A
SINGLEPOINT GLOBAL
SECURITY ADVISOR**

CONTACT US



ONE WORLD. COUNTLESS THREATS. ONE SECURITY PARTNER.

