Microsoft Security

# 4 Strategies to Address the Biggest Challenges in Data Security

# Contents

Meeting complexity with simplicity ..... 3

1 **Challenge 1:** Protecting data even as company culture shifts ..... 4

2 **Challenge 2:** Knowing your data at a time of exponential data growth ..... 6

3 **Challenge 3:** Defending against identity-based threats ..... 8

4 **Challenge 4:** Reducing complexity in your security stack ..... 11

Four challenges: One answer ..... 13

# Meeting complexity with simplicity

**Businesses rely on data to make decisions, automate processes, and support collaboration. But that data is created and stored across a growing number of places and devices. Hybrid work requires employees to access information outside the office, often on personal devices. IoT transforms physical processes into data streams. Cloud, hybrid, and multicloud ecosystems transfer vast amounts of data across geographies and topologies.**

This rapidly growing universe of diverse information makes data protection more challenging than ever. But many organizations don't even know where all of their data lives, let alone whether it's safe.

That's why managing and protecting data across ever-growing digital estates has become a top priority—even as security talent is scarce and resources become more constrained in the face of global economic uncertainty. With so many pressures, it's not surprising that security teams have adopted a wide range of technologies and approaches. Unfortunately, many organizations have found themselves with unwieldy collections of point solutions that increase complexity, cost, and risk.

An integrated, comprehensive data protection solution can create simplicity by reducing noise and increasing transparency and control. This helps security teams focus on more meaningful and rewarding tasks, such as strategy and sophisticated threats—which can also help with retaining talent.

Many security leaders are looking for fresh strategies to address the scale and urgency of the data protection challenges they're facing. Let's look at some new ways of thinking about these challenges, and how to overcome them.

**A comprehensive solution that integrates security and compliance can simplify data protection challenges. It enables organizations to deploy and manage hybrid, multicloud, and edge architectures, while increasing efficiency, reducing risk, and controlling costs.**

## Challenge 1:

# Protecting data even as company culture shifts

**Remote and hybrid work has risen rapidly just as digital data has grown exponentially. That's brought many changes to company culture, including new policies and norms around productivity, innovation, and when and where we work. But these shifts have created new data protection challenges, including insider risk—that is, the misuse of authorized access to company assets, whether inadvertent or malicious.**

Microsoft's Work Trend Index 2022 found that the number of hybrid employees is up to 38 percent and that 53 percent of people are likely to consider transitioning to hybrid. Those figures align with a trend that's evolved over the last decade, as collaboration gets easier than ever across offices and remote locations.

Hybrid work has also helped enable and motivate the "Great Reshuffle," with more workers changing careers. The Work Trend Index reported that 52 percent of Gen Z and Millennials were likely to consider changing jobs within the next year. That can create challenges both coming and going:

Departing employees might take sensitive data with them (intentionally or not), while new staff might be unfamiliar with an organization's security tools and policies.

Security and compliance professionals know this risk is real: Two-thirds agreed that data theft or data destruction from departing employees is becoming more common, according to a 2022 Microsoft Security report on insider risk.

It's clear that employees will continue to need faster and freer access to data. But organizations need a strategy that doesn't achieve security at the expense of a positive, collaborative company culture.

> **Two-thirds of security and compliance professionals say that data theft or data destruction from departing employees is becoming more common.**

## Strategy 1:

# Implement holistic insider risk management

**Insider risk management is intended to detect and prevent misuse of authorized access—whether that misuse is malicious or unintentional. There are many ways to approach insider risk management, but it's typically most effective as a carefully coordinated, centralized program.**

Insider risk management poses many questions, including:

- How do you mitigate stressors that might lead to disgruntled employees?
- What kind of deterrents should be considered and prioritized?
- How important is training, education, and communication?

A 2022 Microsoft Security report on insider risk asserts that the more often firms deal holistically with the issue of insider risk, the more effective they are at addressing it. The report measured how well organizations integrated their insider risk efforts across four elements:

- **People:** Are they seeking out diverse perspectives to better create cross-organizational buy-in?
- **Process:** Are they taking a balanced approach to insider risk, including prioritizing positive deterrents?
- **Tools:** Do they have integrated tools and technology suitable to address insider risk management needs?
- **Training:** Are their insider risk training programs effective?

The more people focused on and addressed these four elements, the more holistically they were approaching insider risk—and that holistic approach influenced organizational culture, too.

# Key steps to achieve holistic insider risk management

1

Prioritize employee-employer relationships and integrate privacy controls and policies in programs to maintain—and even boost—trust.

2

Attain program buy-in and involvement across the organization, moving beyond IT and security groups to include the perspectives and support of other teams, especially compliance, legal, and human resources.

3

Place a high value on employee data security training and education, relying more on employees as a first line of defense complemented by a strong backing of detection tools.

4

Use positive deterrents more often, such as employee morale events, detailed onboarding, ongoing training, upward feedback, and work-life balance programs.

Integrate tools into the existing security stack and create visibility across the company, maintaining a balance of negative deterrents (by leveraging risk-detection tools) with an equally strong level of positive incentives.

1

2

3

4

## Challenge 2:

# Knowing your data at a time of exponential data growth

**Most organizations recognize the importance of data to successful operations. Yet many still struggle with the basic problem of knowing what data they have.**

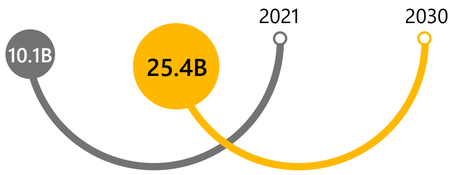
According to ESG's 2022 State of Data Governance and Empowerment Report, 42 percent of organizations say at least half of their data is "dark"—data that's collected but unknown or unused for business purposes. Often, this data simply isn't identified at the point of creation or modification, or it can become dark when a worker switches projects or roles.

The creation and movement of data is now so fast that it's impossible for traditional tools and processes to keep up. The amount of new data created, captured, replicated, and consumed will more than double by 2026, with enterprise data growing more than twice as fast as consumer data. The number of IoT-connected devices alone is expected to reach 25.4 billion in 2030—up from 10.1 billion in 2021.

The reality of hybrid and multicloud ecosystems makes knowing what you have even more difficult. Your data exists on personal devices, in multiple clouds, on IoT devices, and on-premises, to name just a few possibilities.

Discovering and organizing this sprawling wave of digital information while remaining compliant is a mammoth undertaking, especially as ever-smaller IT teams struggle to protect ever-bigger data estates.

**The surge in IoT-connected devices is contributing to rapid data growth.**




## Strategy 2:

# Automate data discovery, classification, and protection

**To govern your data, you need to classify it by sensitivity and business impact. But it's nearly impossible to do this manually over large data stores, especially with more types of data in more locations than ever. That's why it's a good time to evaluate data discovery and classification capabilities—and to look for ways that automation can help.**

Automation that uses artificial intelligence (AI) and machine learning (ML) can recognize and classify sensitive data across locations and do so continuously as more information is created and shared. AI and ML can also increase classification accuracy and review data retroactively. These processes can create a unified map of data across your entire estate and establish the foundation for effective data governance and usage.

To be useful to the people who need it, data classification should also be as intuitive and simple as possible—and it should be integrated with productivity solutions. Data protection leaders in an organization should determine this classification logic, along with workflows that align with day-to-day business activities without impacting productivity.

Automation is the key to increasing efficiency and visibility, so security teams have both the bandwidth and insight to close exposure gaps across your environment. That way, you can know what data you have and keep it safe.

# Key steps to improve data discovery, classification, and protection

1

Automate data classification to make broad governance possible as data proliferates, everywhere it lives, across any clouds.

2

Aim for a holistic, real-time view of key data indicators, including which data gets used and how, so you can discover indicators not only of risk but of value.

3

Maximize the business value of data by creating a unified map to automate and manage metadata from hybrid sources.

4

Make data easily discoverable and understand the origins of your data with interactive data lineage visualization.

## Challenge 3:

# Defending against identity-based threats

**Most employees aren't security professionals, but they're all potential targets of attacks. For example, Microsoft blocks 710 million phishing emails in the average week—a volume that is orders of magnitude greater than all other threats we track and protect against. A Kaspersky Security study highlights this vulnerability as well, finding that 46 percent of cybersecurity incidents involve careless or uninformed staff who inadvertently facilitate the attack. That means if you want to keep your data safe, you need to keep your workers safe.**

Perimeter-based security using firewalls or air gaps has long been insufficient. But that's more true than ever now, as employees work from more places and many organizations have become increasingly reliant on third-party service providers, vendors, and software supply chains.

Organizations need a new approach for this new reality, but the central problem is trust—that is, too much of it. Security that trusts anything inside the perimeter is ripe for exploitation. Cybercriminals have proven adept at silently penetrating perimeters and lurking unseen until the moment comes to strike. An effective approach should help employees access the tools and data they need without relying on trust inherent to any system, process, or user.

**710 million**

**phishing emails blocked by Microsoft per week across our global customer base**

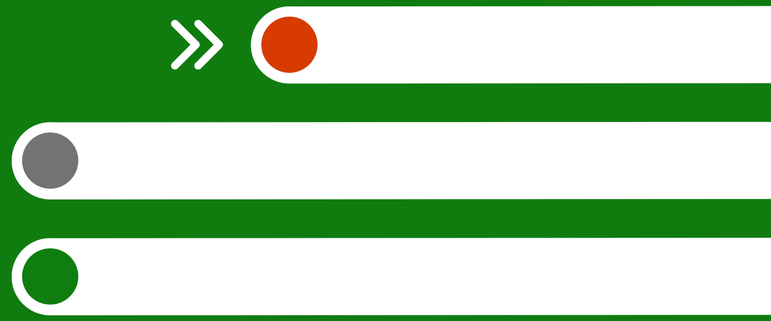
## Strategy 3:

# Implement a Zero Trust framework for more effective security

**As an end-to-end security strategy, Zero Trust relies on three pillars: verify explicitly, use least privileged access, and assume breach. This holistic and integrated approach is relevant to every organization.**

By establishing a solid Zero Trust foundation, organizations can better defend against threats and ensure compliance as they protect and govern sensitive data.

- **Verify explicitly**
- **Use least privileged access**
- **Assume breach**



1

2

3

4

## A Zero Trust framework protects against identity-based threats by detecting and preventing unauthorized access to data at rest, in transit, and across devices and locations of all kinds. It covers six key pillars of enterprise IT:

**Identity and authentication:** Protecting identities against compromise and securing access to resources, including multifactor authentication.

**Applications:** Ensuring applications are available, visible, and protecting your important data.

**Data:** Protecting sensitive data wherever it lives or travels.

**Networks:** Removing implicit trust from the network and preventing lateral movement.

**Infrastructure:** Detecting threats and responding to them in real time.

**Endpoints and devices:** Securing endpoints and allowing only compliant and trusted devices to access data.

## A White House executive order requires federal organizations and their suppliers to implement a Zero Trust architecture. Other industries may not be far behind.

A good first step towards meeting this new standard is adopting a unified, modern identity and authentication system that's capable of supporting multifactor authentication and detecting suspicious activity.

These kinds of systems are a cornerstone of Zero Trust. They enable convenient single sign-on across applications and resources by consolidating identity onto a cloud-based platform.

# Key steps for adopting Zero Trust

1

Follow the three pillars of the Zero Trust end-to-end strategy: verify explicitly, use least privileged access, and assume breach.

2

3

Implement unified, cloud-based identity services to adopt Zero Trust efficiently.

4

Use a Zero Trust framework to support data protection and defend against identity-based threats in a distributed environment.

## Challenge 4:

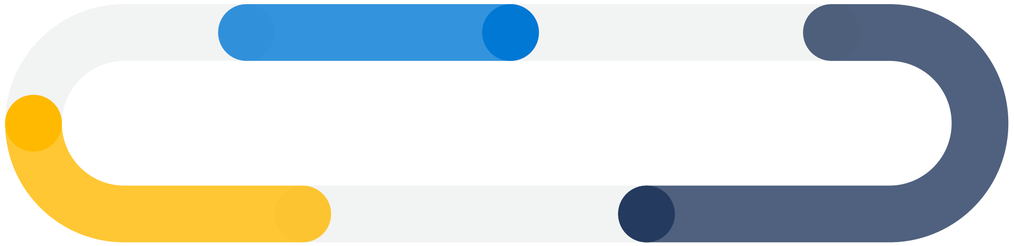
# Reducing complexity in your security stack

**Many organizations default to a patchwork of competing third-party solutions to address basic data protection needs. They're then forced to deploy additional solutions as more gaps appear.**

Enterprise environments are already complex, with many potential blind spots. For example, the average enterprise network has over 3,500 connected devices that aren't protected by an endpoint detection and response (EDR) agent. Layering the complexity of multiple point solutions on top of this only increases the burden of coordinating day-to-day security management, administrator and user training, updates, and compatibility among systems.

Importantly, managing all of these "bolted on" solutions doesn't just take focus away from mitigating complex threats. It also increases costs at a time when security decision-makers are feeling pressure to control budgets and do more with less.[1]

Security teams are already stretched thin. They need to more effectively reduce administrative overhead, complexity, and cost—but without sacrificing protection for efficiency.



[1] March 2022 survey of 501 US Security Decision Makers commissioned by Microsoft from agency Vital Findings. DELL Technologies, 2021.

## Strategy 4:

# Choose a comprehensive solution for data protection

**Many organizations are planning to consolidate their data protection solutions under a single vendor. Vendor consolidation was cited as one of the 7 top cybersecurity trends in 2022 according to a Gartner® survey.[2] In fact, "75% of organizations are pursuing security vendor consolidation in 2022, up from 29% in 2020," according to another Gartner survey.[3]**

The key is choosing the right vendor. An effective and flexible platform can replace multiple point solutions—potentially even dozens in some organizations—and provide coverage across virtually any location or device. A comprehensive solution should increase visibility and go beyond compliance, combining data protection, data governance, compliance, and risk management.

Look for the following characteristics in a solution to maximize protection and efficiency:

- Increased operational efficiency that streamlines IT workloads
- A lower bottom-line cost than a multiple-solution strategy, including by eliminating redundant capabilities
- Easy deployment, maintenance, and governance with familiar systems for faster adoption and easier user training
- AI and automation to reduce threats and help SecOps teams be more productive
- An environment with low or no compatibility issues with existing tools
- "In-place" data management without transfers or access to third parties

[2] Gartner, "7 Top Trends in Cybersecurity for 2022," April 13, 2022. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

[3] Gartner Press Release, "Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022," Sept 13, 2022

# Key steps for choosing a data protection solution

1

Adopt a centralized data protection strategy that meets your organization's goals, such as improving risk posture, reducing complexity, or doing more with less.

2

Select a data protection solution that can scale to protect your entire data estate end to end.

3

Consider the cost of long-term maintenance, future upgrades, and compatibility when weighing your data protection options.

4

# Four challenges:
# One answer

**Microsoft Purview and the advanced security capabilities of Microsoft 365 E5 work together as a unified platform. They're designed to overcome all of the challenges discussed in this e-book.**

1

2

3

4

## Microsoft Purview

Microsoft Purview helps organizations govern and protect data across their multicloud, multiplatform data estates, while meeting compliance requirements. Within Microsoft 365 E5, Purview brings together information protection and advanced compliance capabilities.

### Understand and govern data

It's never been harder to understand and govern an organization's sensitive information. Get visibility into all your data and manage assets across your environment.

### Safeguard data, wherever it lives

Protect sensitive data across apps, clouds, and devices—even if it's not stored on Microsoft platforms.

### Improve risk and compliance posture

Identify data risks and manage regulatory requirements so your organization can stay in compliance.

## Advanced security in Microsoft 365 E5

Microsoft 365 E5 combines best-in-class productivity apps with advanced security, compliance, voice, and analytical capabilities.

The advanced security features in E5 help you extend identity and threat protection with integrated and automated security to help stop damaging attacks. Microsoft 365 E5 also brings together information protection and advanced compliance capabilities to protect and govern data while reducing risk.

## Take on the biggest challenges in data security with Microsoft Purview and the advanced security solutions in Microsoft 365 E5.

Learn more

Microsoft