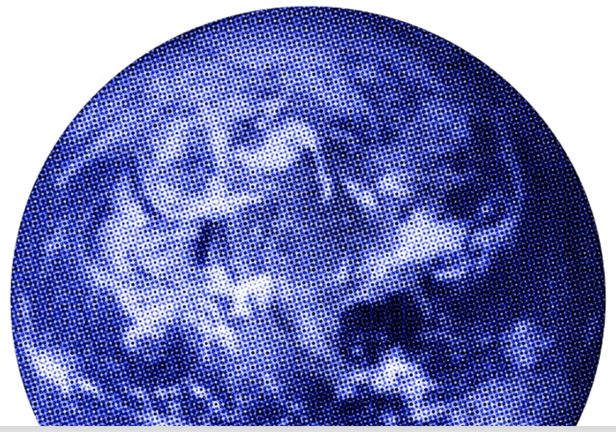
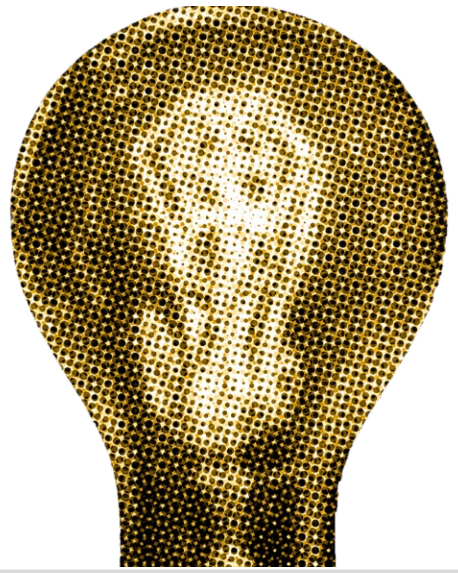
IT All Falls Apart: Modern IT's Losing Battle with Complexity

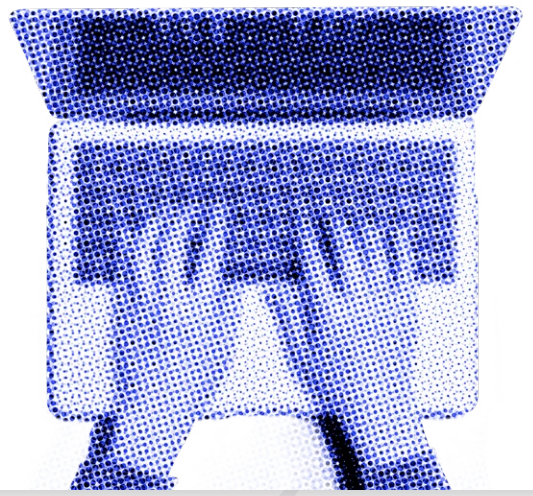
And how to seize the future
with a secure cloud

zix | appriver

Table of Contents







About this report:

This report was compiled by Zix, the leader in software for modernizing IT, making employees more productive, and protecting the business. **Learn more at Zix.com.**

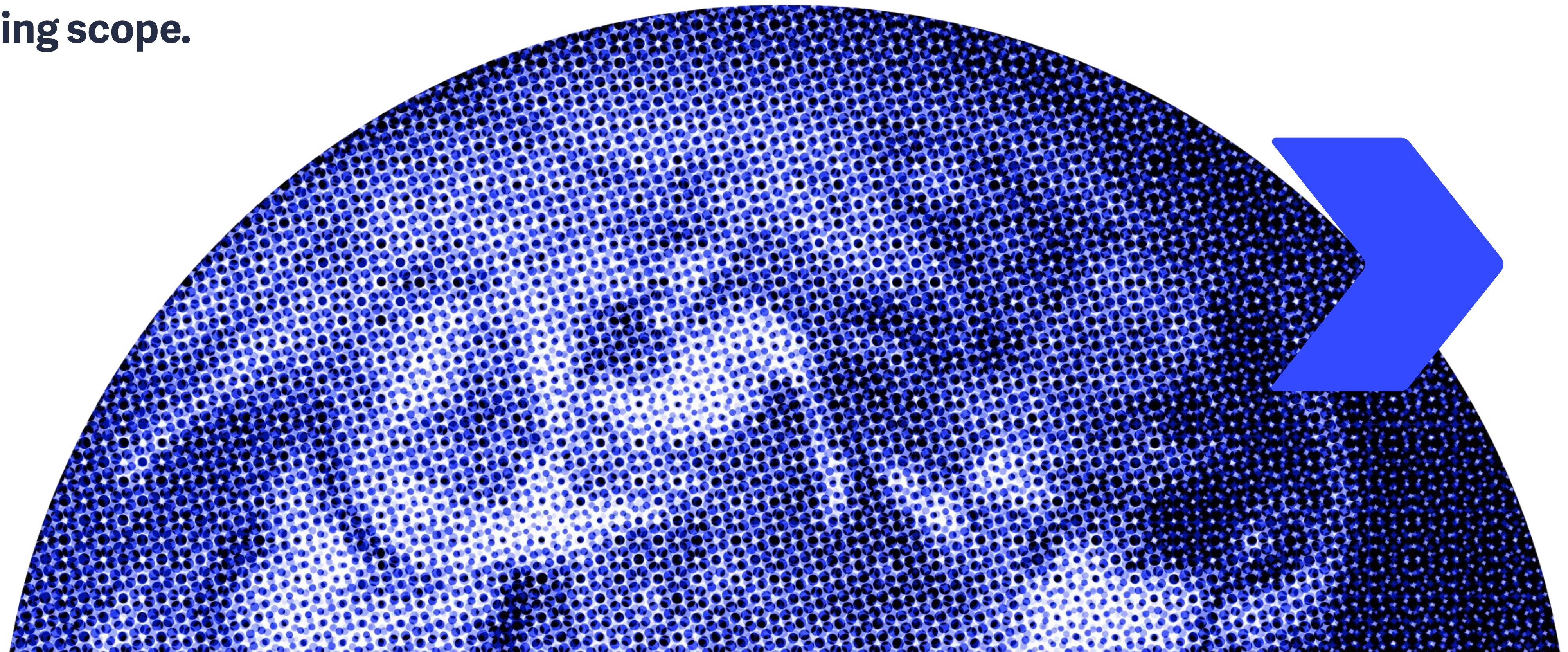
zix | appriver

01 A Tsunami of More

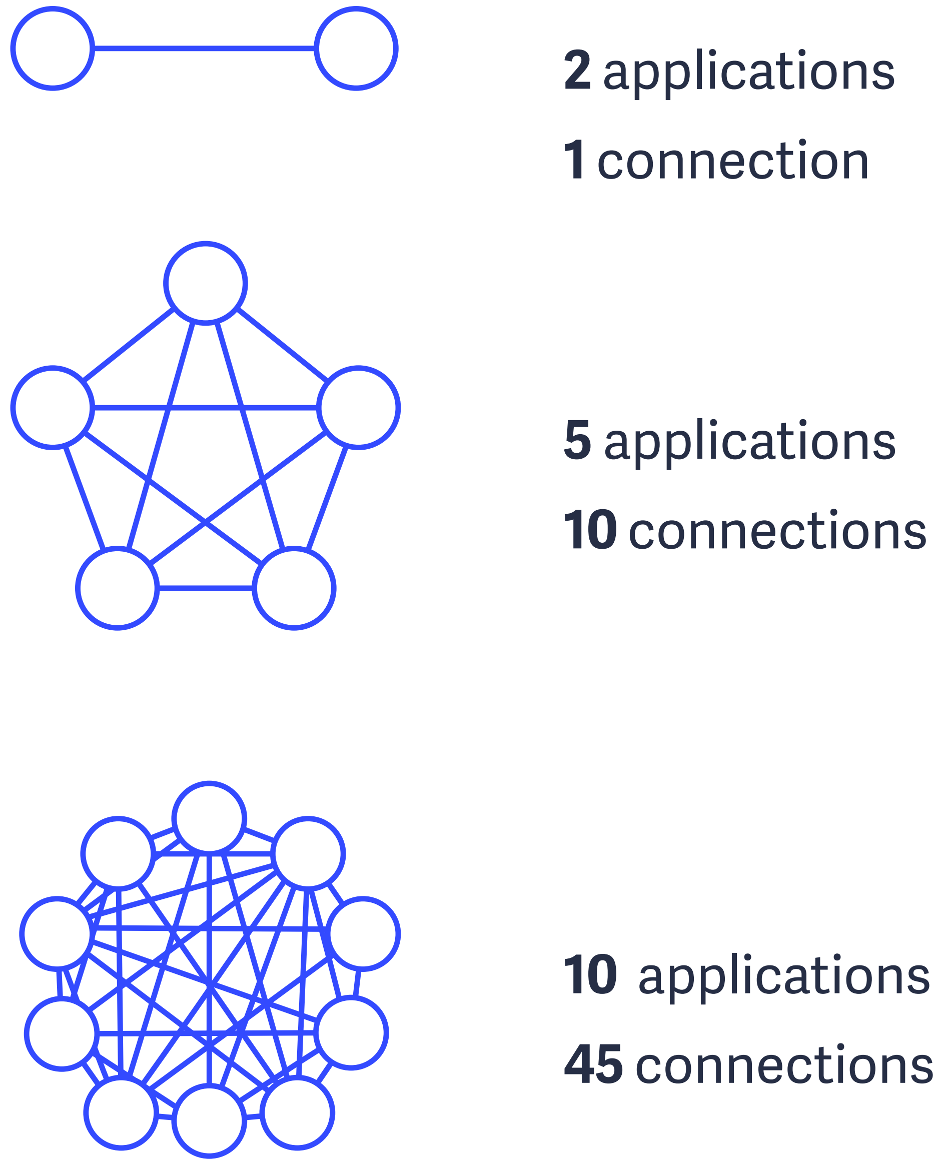
In the spring of 1976, the Control Data Corporation released the world's first supercomputer, the Cray-1. Shaped like a "C" to increase transmission speeds, it was six feet in diameter and featured freon cooling coils and 50 miles of wiring. It could process data with a then mind-boggling 64 bits. But, it only had one port. While extremely complicated, this 5.5-ton machine's network diagram was simple—just two dots and a line. To hack it, you had to physically saw through a padlock. Any bugs it encountered were actual insects.

To the modern IT and information security (InfoSec) professional, securing this sort of environment seems like an absurd, idyllic, far-off memory. Today, network diagrams are an incoherent cobweb of connectors, endpoints, and vulnerabilities. They aren't just complicated—they're complex. The difference being, a complex environment is one where there are not just many systems, but they're all networked together and influencing one another. Companies have an average of 123 software tools across the enterprise—most of them, connected through APIs. These systems each speak to other networks, store sensitive information, and transmit millions of messages through a growing number of new media across multiple devices per user.

To most, it's a problem of staggering scope.



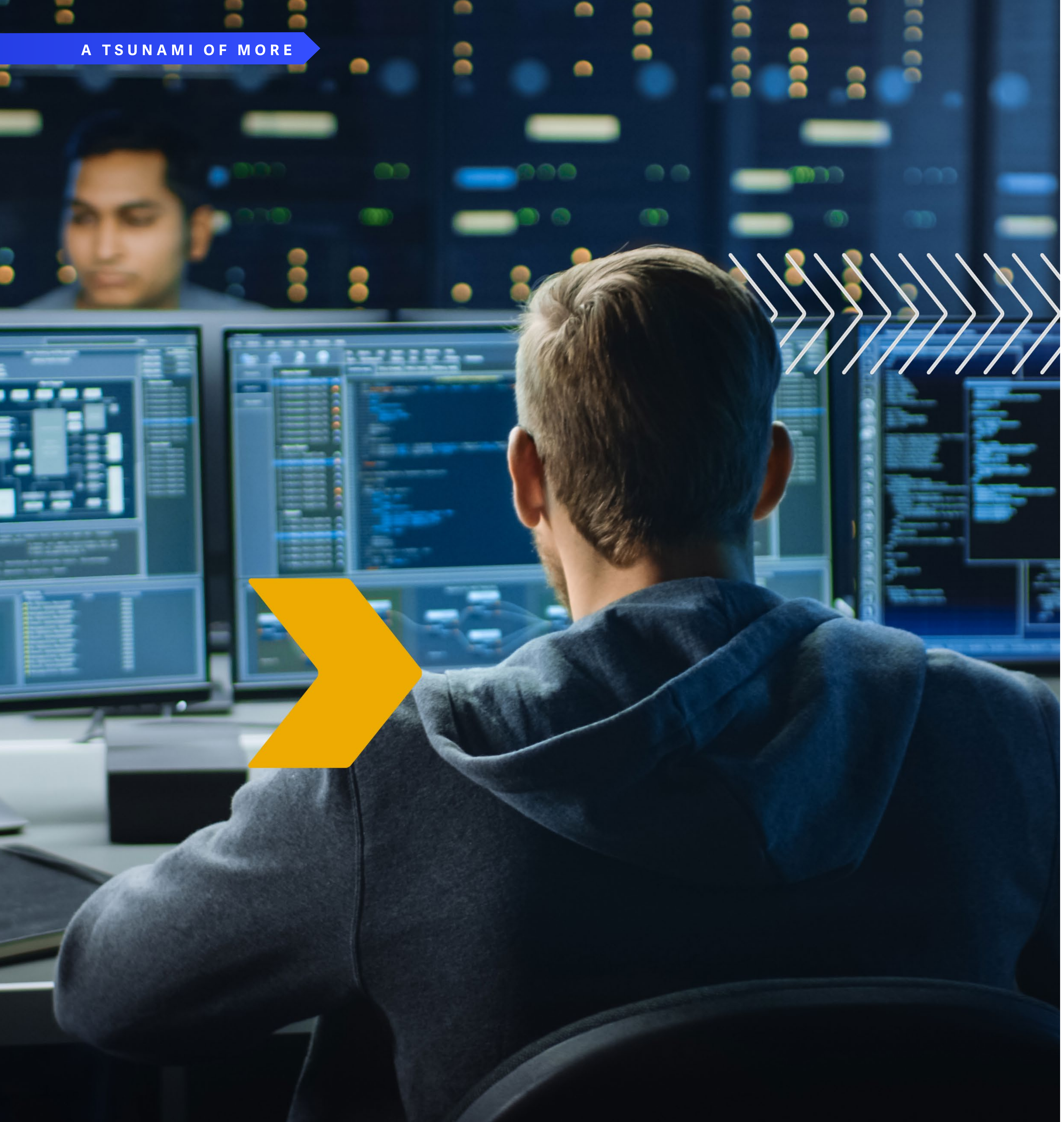
N2 problem diagram



2 applications
1 connection

5 applications
10 connections

10 applications
45 connections



Complexity is a battle and the enemy is winning

If IT and InfoSec teams are battling anything today, it's complexity. And when it gets the best of them, it erodes their ability to support the business. They find themselves hindered by time-intensive workarounds, breaches, audits, help-desk demands, and sprawling regulation. In an increasingly digital world, it holds back those companies and public sector organizations from growing, competing, or achieving their mandate.

> *79% of leaders say new business models introduce tech vulnerabilities.*

At healthcare organizations, breaches distract doctors, nurses, and administrators from life-saving duties. And if they can't easily share information protected under HIPAA, it can detract from patient outcomes. Financial firms, which are 300x more likely to be attacked than other businesses, face lower returns and are reluctant to digitize services because of cyber risk. The public sector, which is the target of 16% of all breaches, faces a recurring, catastrophic loss of privacy—5.3 million records were exposed in 2018 alone. Businesses in every sector also hemorrhage one of their greatest assets, customer trust.

Everything these organizations stand to lose, however, they also stand to gain, and that's the perspective we here at Zix advocate: This challenge is also an opportunity. Organizations that get a grip on runaway workplace complexity outperform their peers—they provide better care, earn higher returns, offer more responsive services, and attract 40% more customers.

As we will explore in this report, teams that are determined to win this fight are doing several things. Chief among them: doing less.

> *Organizations that get a grip on runaway workplace complexity outperform their peers.*

02 Adapting Under Fire

What is the point of an IT or InfoSec team? To build the network and secure the environment and their users, yes. But their ultimate goal today is to enable an organization's greatest assets—its employees—because the horrors of runaway complexity spill over into the business. Disconnected devices, file transfer limits, lost passwords, phishing attacks, malware, and audits derail work, and digital disruptions are growing more frequent. Employees spend 11 hours each year just recovering lost passwords, and an incalculable amount of time on nonessential and sometimes malicious email. (Business email attacks rose 350% in 2019.) It's all part of why according to a study by Atlassian, only 60% of work time is actually spent being productive.

All of this might make some yearn for the simple days of the Cray-1 supercomputer, and inspire them to prune the proliferating connections and go dark. But as Thomas Aquinas put it nearly a century ago, "If the highest aim of a captain were to preserve his ship, he would keep it in port forever." Progress and risk go hand in hand. More devices are coming. More channels are coming. Employees need them to work and remain competitive. IT and InfoSec teams instead need a strategy that reduces complexity without stifling the business. According to our research, there are three battlefronts they can fight on: Productivity, security, and compliance.

Productivity

Are workers connected? Do their tools save time or cost time? Can they work from anywhere? Can the team safely manage access for contractors and frontline employees?

Security

Is your security posture evolving as fast as threats? When is the last time you audited your email environment for security? Are workers safe from interruption? Can they communicate freely? Do their everyday actions endanger the business? How reliant is your security posture upon employees taking action?

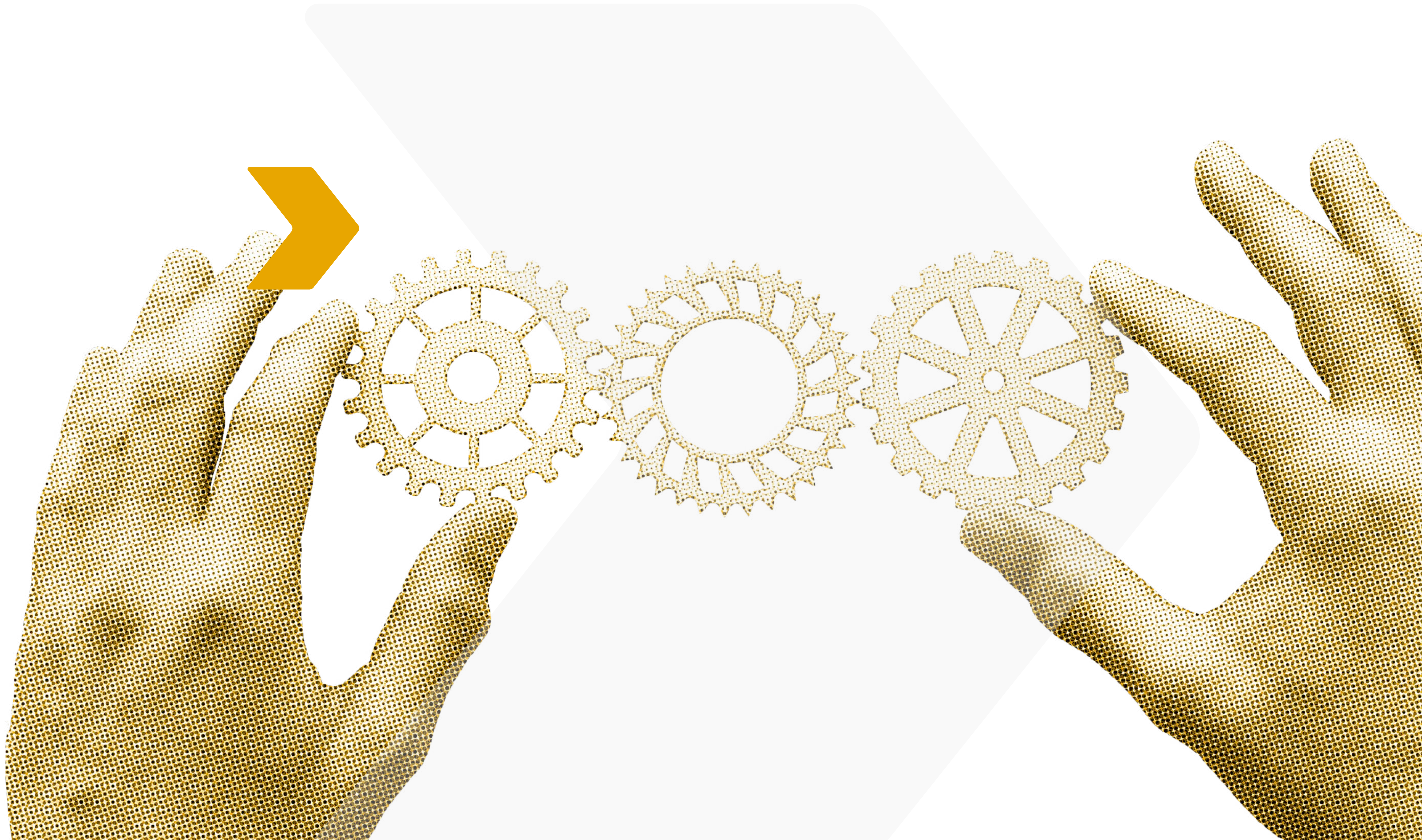
Compliance

Are you aware of all your sensitive data? Can you easily share it to meet regulation or comply with an audit? Can you track conversations on new media like messaging apps and social media?

It pays handsomely to think of these three factors—productivity, security, and compliance—as interrelated. One of the greatest causes of burgeoning workplace complexity is the long-held belief that buying many disparate "best-of-breed" apps and patching them together provided the best of all worlds. But the number of systems IT and InfoSec teams must manage has hurtled beyond the human span of control. Even modest-sized companies of 200-500 employees have an average of 123 software systems from nearly as many vendors and it creates worrying gaps in coverage:

- If two vendors each own half of an issue, they'll point fingers in an endless cycle.
- If your email security vendor doesn't also host your inbox, they can't monitor malicious escalations of privileges.
- If your security vendor doesn't play nicely with your compliance vendor, records could be hacked and you could not know it.
- If your compliance system is on-premise and only tracks email, you miss potentially sensitive information on other channels.
- If your file sharing system doesn't integrate with your email system, it creates exposure and limits productivity.

> ***The "best-of-breed" myth:***
> *Today, the number of systems IT and InfoSec teams must manage has hurtled beyond the human span of control.*



Like a mile-long white picket fence with gaps between every slat, too many "best-of-breed" systems by different vendors who compete rather than cooperate allows threats to pass through without resistance. It also creates a burden on IT and InfoSec teams which draws them away from more important work, like planning for the future of the business. What was once a novel approach is now woefully misguided advice.

> *If the highest aim of a captain were to preserve his ship, he would keep it in port forever.*

Today, the definition of "best" has changed. It's no longer a question of how a software works apart from other systems, but how it works within your existing environment. This context is crucial. You should be measuring vendor effectiveness by how it interoperates and improves your overall efficacy. An email filtering technology that achieves a high effectiveness rate in laboratory conditions but doesn't integrate with your existing email encryption system isn't very useful—it could allow encrypted threats to pass through. For every app or device in your technology stack, ask: Is its net effect to reduce the burden on IT and InfoSec and empower employees to be productive, secure, and compliant?

Far too often, many point solutions fall short. And when they don't work together, they start to work against each other.

03 Understanding the Complexity Challenge

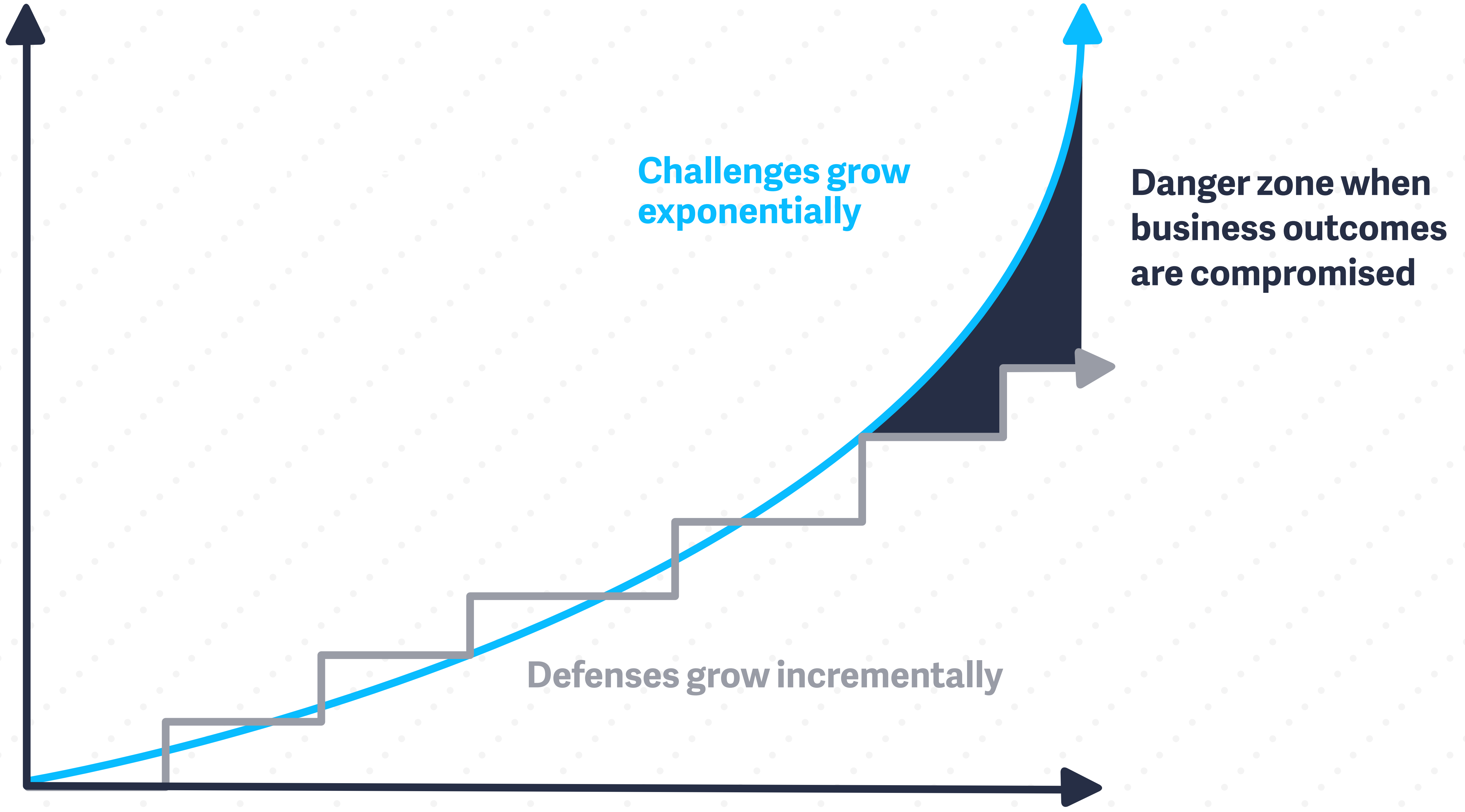
The complexity challenge goes a lot deeper than just there being too many devices on the network.

It's composed of four factors, each of which degrade an organization's productivity, security, and compliance:

- **A.** More software, devices, and dependencies
- **B.** Larger and more frequent threats
- **C.** IT skills shortage
- **D.** "Do more with less" mindset

Worse still, these issues compound. In a world of more devices and more threats, the challenge increase isn't linear but rather exponential.

The old way no longer works.


Challenges grow exponentially
Danger zone when business outcomes are compromised
Defenses grow incrementally

A. More software, devices, and dependencies

Creates more endpoints that need to be secured, more dark data, and more uncertainty

Affects: Productivity, security, compliance

Today, organizations are adding software and devices faster than IT can provision them, and people are increasingly doing it without IT's knowledge—a process known as shadow IT. Individuals are hooking personal devices to the corporate network and deploying software services paid by credit card without explicit permission, or without following data governance guidelines.

Shadow IT is also a leading cause of dark data—business data that the company is organizationally unaware of. It could be sensitive patient data stored in a note-taking app or insider information lodged in a team collaboration app. Dark data creates risk.

It's easy to see shadow IT as malicious, but it isn't. It's an outpouring of employees trying to make themselves more efficient. Workers are more productive when they select tools they're already familiar with, and working from mobile devices may save them an average of 58 minutes per day. But the productivity gains begin to backslide when the IT and InfoSec teams can't secure these endpoints, and they invite attacks, malware, and incompatibility snarls. A workplace of mixed-use operating systems like iOS, Windows, Linux, and Android is rife with errors, failed file transfers, time-consuming workarounds, and countless hours waiting for an overstrained help desk team to slog through its backlog of tickets.

> *Productivity gains begin to backslide when IT and InfoSec teams can't secure new endpoints.*

> *38% of technology purchases occur outside of IT. -Gartner*

B. Larger and more frequent threats

Rising cost of defense against breaches, ransoms, audits, and fines

Affects: Productivity, security, compliance

Cybercrime is growing more profitable while the barrier to entry has dropped through the floor. Tools designed to attack Bank of America were available until recently on the dark web for $11, according to Bloomberg. By 2021, the cybercrime industry is projected to be bigger than the drug trade. This makes for more attacks against more businesses. There was a 130% increase in data breaches from 2006 to 2019. And while the odds of a Fortune 1,000 business being hit by multiple attacks was 5% in 2005, by 2015, it was 20%.

IT teams today are still largely reliant on headcount to scale, but scale they are not. With the same sized teams spreading their attention across more areas, they're increasingly vulnerable, especially in some of the most obvious arenas, such as business email.

Work email is the number one attack vector for malicious actors for several reasons. Email is ubiquitous, email addresses are used as employees' login credentials to most systems, and untrained end-users present a soft target. At the same time, phishing, business email compromise (BEC), malware, and link attacks are far more sophisticated and precisely targeted than ever before, and especially effective on mobile where users are often multi-tasking and distracted. Without the ability to secure one of the biggest portals of communication with other organizations, teams doing the same as always have grown proportionally less secure.

> *Teams have grown proportionally less secure.*

C. IT skills shortage

Slows progress, reduces security, lowers the utility of software systems

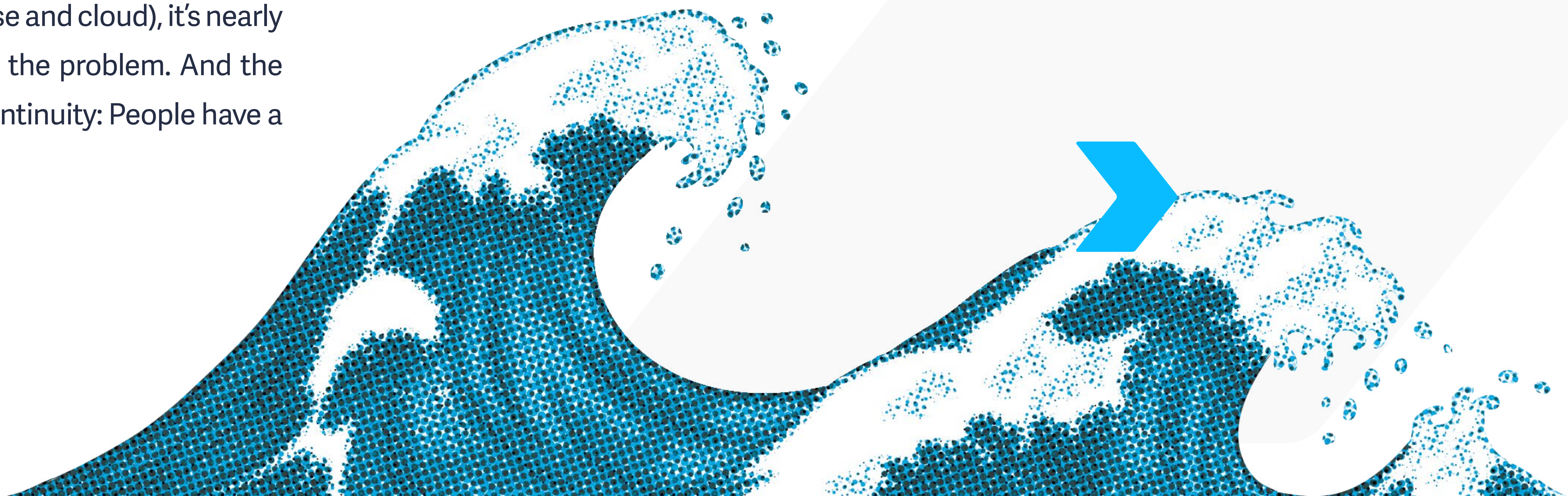
Affects: Productivity, security

Today's skills shortage hits every business unit, but it hits IT teams especially hard. A reported 83% of organizations struggle to recruit candidates today, reports the Society for Human Resource Management. Seventy-five percent of hiring managers say there's a skills shortage among candidates. By 2021, there are projected to be 3.5 million cybersecurity-related job postings unfilled globally, and a study by 451 Research found that the #1 desired role was server or systems administrators—people to manage the complexity.

Without the ability to hire niche experts in emerging areas like DLP filters, lexicography, productivity tools, encryption, risk mitigation, and security operations (SecOps), organizations will continue to experience coverage gaps. And with turnover, the issues compound.

With the sheer number of legacy IT products (much of it, mixed between on-premise and cloud), it's nearly impossible for incoming hires to ramp quickly. You can't simply throw bodies at the problem. And the older the products and the younger the hires, the more issues arise in network continuity: People have a harder time managing infrastructure they weren't there to install.

> *You can't simply throw bodies at the problem.*



D. “Do more with less” mindset

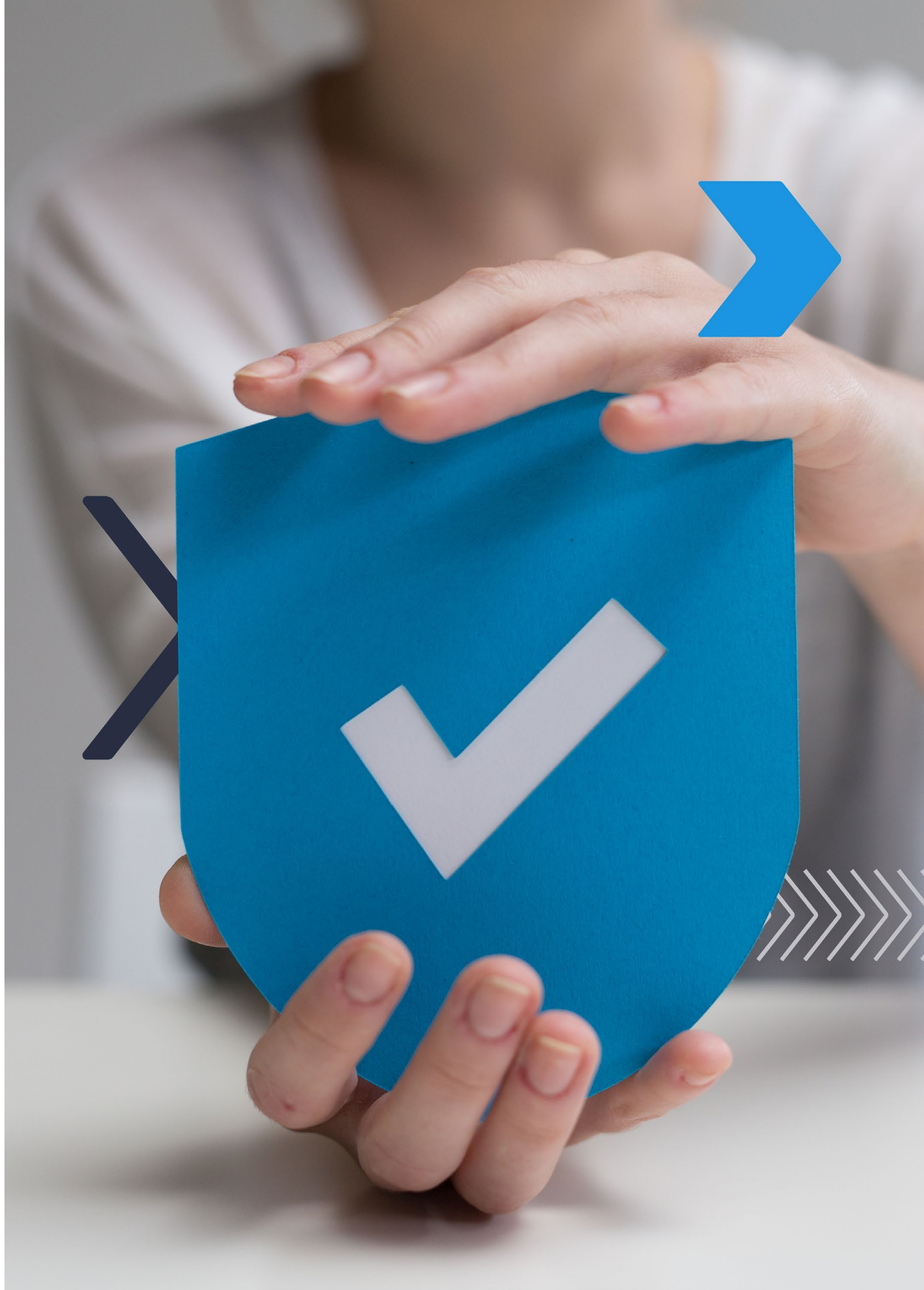
Creates technical debt, creates risk exposure

Affects: Productivity, security, compliance

All of the aforementioned issues—more devices, more vulnerabilities, and bigger skill gaps—exist, and budgets have not gone up. In 2019, IT budgets increased only 3.7% year over year, barely outpacing inflation, according to Gartner. It is clear that IT and InfoSec organizations are being asked to fight on more fronts but not armed with the tools to do so. Organizations cannot simply buy their way out of these problems, and in many cases, companies lack board-level awareness of the complexity challenge. Top-down orders issued without an understanding of the underlying issues only promise to spread teams even thinner. It causes burnout, delayed projects, and makes the organization a softer target for attack. As just one common example, many email compromises begin with inbox settings changes, but it’s a rare team that has the manpower to police them.

> *IT budgets increased only 3.7% in 2019.* -Gartner

Yet amidst all of this—devices, threats, and skills—some organizations are solving these issues. Our team’s research found that the biggest thing successful organizations are doing is they’re dogmatic about doing less.

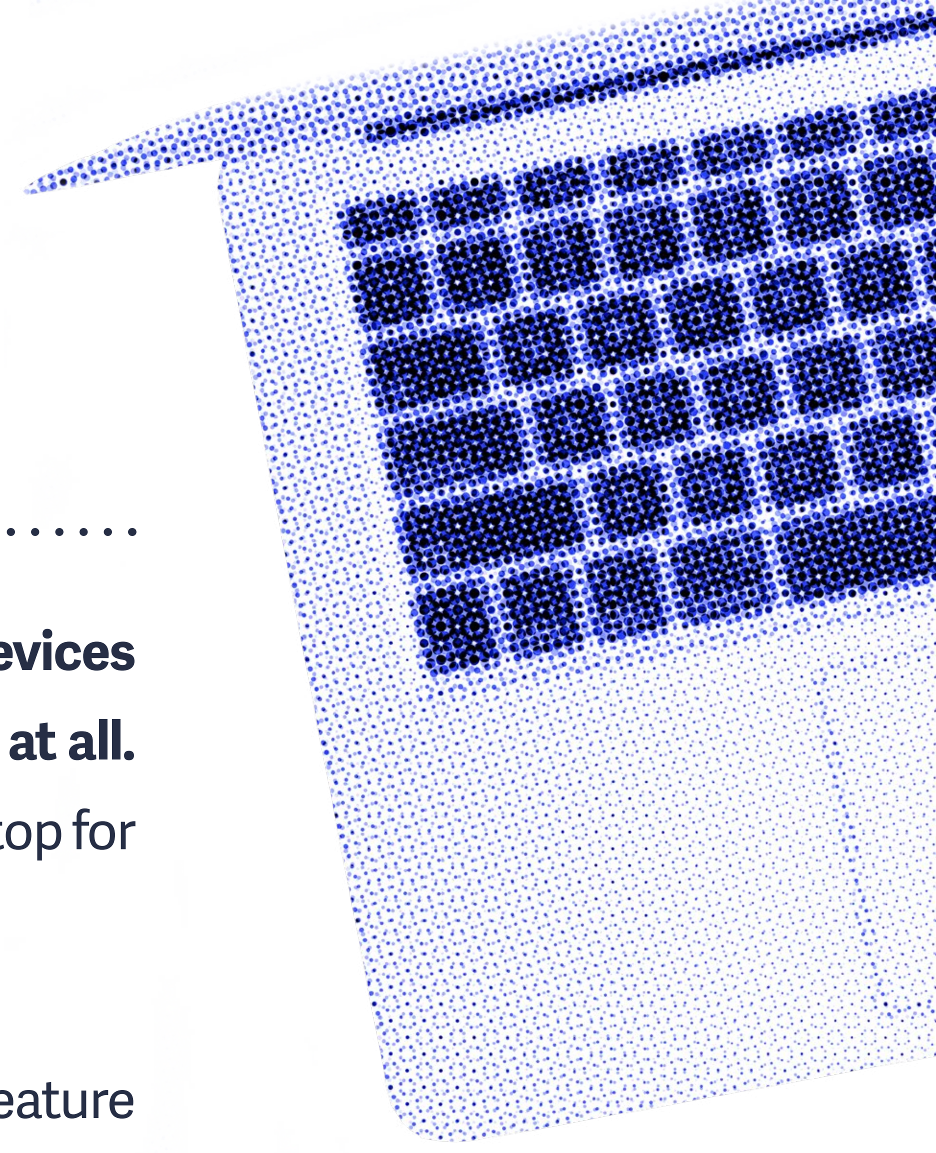


04 Why Consolidation is the Answer

The antidote to complexity is artful consolidation. Rather than more software and devices, teams need less, or need aggregator systems that can take control of multiple apps to reduce the administrative burden. In response to larger and more frequent threats, teams need more powerful encryption and threat protection tools and in this case, powerful means simple. A reported 90% of breaches due to phishing or BEC are caused by user error. We contend that no amount of training can make every employee a paragon of vigilance.

In terms of the IT skills shortage, teams are faced with a non-choice: Invent new ways to find or train qualified individuals faster, or look elsewhere—such as to partners—to rent or borrow the niche tools and expertise needed.

Here are four principles to guide your consolidation mandate:



~~A. More software, devices, and dependencies.~~

A. Less software is (often) more

Organizations buying the most complex productivity, security, and compliance software or devices without the requisite expertise or man-hours to use them may just as well not be buying them at all. Some 37% of software goes unused, reports CIO, which comes out to an average of $259 per desktop for the average business.

It's a similar story for user interfaces and features. The more complex a software, the less likely any feature is to be used, and as UX designers say, defaults are powerful. To a user unaccustomed to having to click a button to encrypt their emails, change comes hard. Far better to remove the unnecessary optionality and make encryption automatic. For users who are accustomed to outlets like social messaging in their home life, it can be far better to offer ways to safely permit their behavior, such as with internal social networks, than suffer what economists call deadweight loss—people circumventing the rules to use personal messaging apps like WhatsApp.

The Answer

- ✓ Consolidate platforms.
- ✓ Give greater weight to interoperability and automation.
- ✓ Seek out interlocking software suites.

> *As UX designers say, defaults are powerful.*

~~B. Larger and more frequent threats~~

B. Foolproof Security

As photographers say, the best camera is the one that's with you when something happens. So too with security and productivity. The best workplace tools are the ones that actually get used. Companies should give user experience greater priority when selecting cybersecurity tools, both for end-users and for IT and InfoSec teams, who carry the weight of poor experiences in terms of bulging help desk ticket backlogs.

The other big factor is any security system's ability to update itself. On-premise hardware is going the way of the dinosaur partly out of convenience, but also security: Cloud-native security software partners can patch the moment a new threat or vulnerability is detected.

A foolproof security system is one that can:

- Truncate complex defense capabilities into simple user experiences
- Reduce the administrative burden on end-users and IT
- Be continuously maintained, updated, and improved

The Answer

✓ Seek the security system that will be used, not the one with the most bells and whistles.

✓ Prioritize vendors that continuously improve and will provide unbiased guidance on the right solutions to purchase, not just the most expensive ones.

> *Give user experience greater priority when selecting cybersecurity tools.*

~~C. IT skills shortage~~

C. Greater reliance on vendors

At the time of writing, there are precisely 38 job postings on the job site Indeed for "lexicographer," which is someone who reviews compliance programs and adds lexicon to detect sensitive information. Yet any organization with an email filtering system has a need for at least a part-time lexicographer to determine what terms to filter for, detect, or track, to keep up with internal compliance policies and global privacy regulation.

In the same way, few organizations today can afford to staff an in-house follow-the-sun threat analyst team, but all need one. And when it comes to Microsoft and its suite of productivity tools like Microsoft 365, it's an unusual organization that can afford a full-time team to understand Microsoft's licensing, provision users, monitor inbox settings, and stay ahead of product end-of-life events like that of Windows 7, for which 31% of U.S. federal agencies were caught off guard.

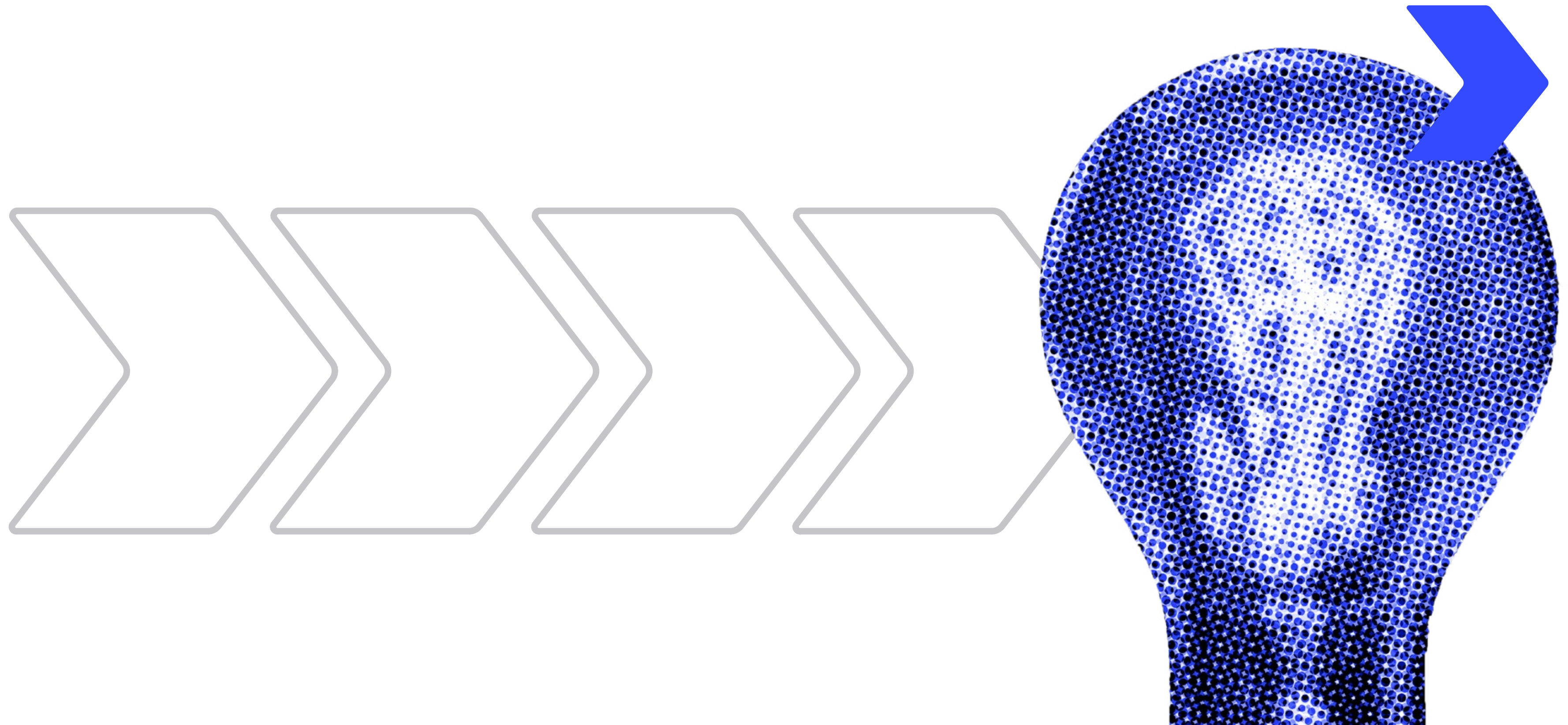
The only realistic way for today's IT and InfoSec teams to scale their capabilities is through partners. For instance, an email security software firm that employs a 24/7 threat analyst team offers a triple benefit: Companies get access to the insights as part of their software subscription, the software is updated automatically to reflect new threats, and each customer benefits from a sort of herd immunity. When one customer faces an attack and the software firm issues an update, all customers become instantly immune. (Or at least resistant.)

When it comes to regulation, a compliance software provider can afford to employ a regulation analysis team that saves their customers the time of having to understand how new regulations apply to them. And when it comes to Microsoft, a certified reseller, managed service partner (MSP), or value-added reseller (VAR) can staff in-house Microsoft experts who offer unbiased advice and tools that Microsoft can't. For instance, some vendors provide security audits to evaluate and remediate common vulnerabilities in a Microsoft 365 environment, as well as real-time monitoring and escalation if a product malfunctions. Some partners can offer honest insights, like the fact that Microsoft's native email spam filtering automatically whitelists all Microsoft customers, leading to a massive influx of spam when companies deploy it.

> ***Three benefits to a cloud email security partner:***
> *1. Ongoing access to threat insights*
> *2. Automatic updates*
> *3. Herd immunity between customers*

The Answer

✓ Consider using partners rather than headcount to fill some skill gaps.



~~D. A "do more with less" mindset~~

D. Security by design

With the pace at which things are moving, IT and InfoSec teams have to escape the gravitational pull of reactively solving issues. Burdened by complexity, many teams only reevaluate vendors when something breaks or they encounter a breach, but they have to be thinking five or 10 years out to be effective. We call this approach security by design. Whenever internal agents such as leadership or the board push IT and InfoSec teams to remediate a pressing threat, those teams must educate the board on how these are only the symptoms of an insufficiently defined productivity, security, and compliance policy, and if they want to address the root cause, they need more budget and the freedom to engage in longitudinal planning.

The Answer

- ✓ Seek support from top leadership for long-term planning.
- ✓ Seek tools that reduce the IT and InfoSec administrative burden and free them up for planning.

> *Teams have to be thinking five or 10 years out to be effective.*

So. Where do all of these fixes lead us? To a new mandate for IT and InfoSec: Get a hold of complexity so you can offer what the business truly needs—a work environment that allows all employees to do their work more efficiently and power the business. **As the next chapter explains, we call this vision a secure, modern workplace.**

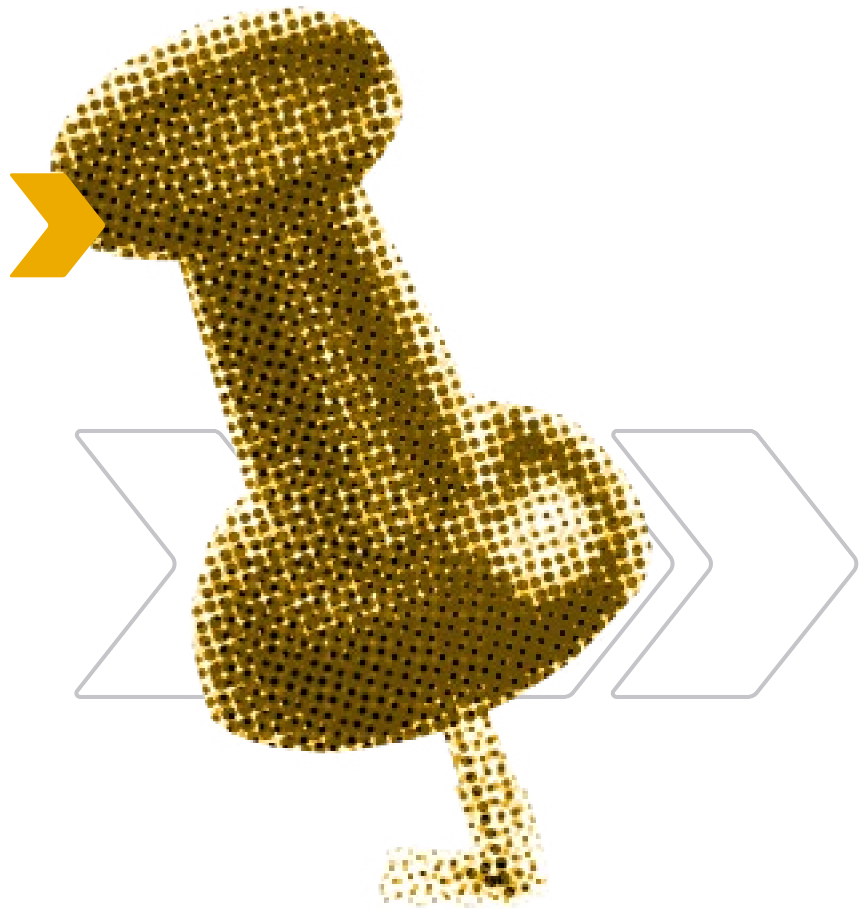
05 The Secure, Modern Workplace

When businesses get a hold of the complexity problem, they can provide employees with a secure, modern workplace: **A continuously improving work environment where employees are productive, secure, and compliant.**

This term is an acknowledgement that IT and InfoSec teams' purpose has shifted from maintaining equipment and hardware to enabling the entire company to be productive. Almost every employee today, including the 80% of America's workers known as first-line workers—retail associates, store clerks, nurses, and repair people—need office apps to function. And to be competitive, they have to function well, and that's a matter of having the right combination of productivity, security, and compliance tools.

When companies have a secure, modern workplace, they reduce the friction of lost passwords, failed file transfers, disruptions due to cyberattacks, and interruptions due to audits or fines. The systems work so that people can work, and can get on with their day.

> *"Today presents a perfect opportunity for companies to become the digital businesses they have wanted to be."*
>
> *-Wayne Kurtzman, Analyst, IDC*



Benefits of a secure, modern workplace:

- Improve productivity and responsiveness
- Foster a safe and well-governed workplace
- Attract higher quality candidates
- Secure the business against interruption
- Free your team up for the important things

Without a secure, modern workplace, healthcare companies are more likely to be rocked by breaches, financial firms to be hamstrung by audits, public institutions unable to modernize their services, and businesses of all types unable to retain that vital ingredient to competitiveness—customer trust.

With a secure, modern workplace, you eliminate much of that friction. The company has productivity apps like Microsoft 365 that allow them to collaborate virtually, so employees can work remotely. It also includes interlocked security software, so those remote workers and their data are just as safe as onsite ones. A secure, modern workplace means people can easily share and work on files, eliminating the duplicated effort of two people working on a document at once, separately. And it includes compliance tools like a unified archive so any business communications are stored securely, and so easily accessible that even HR can peek in and see. When everyone knows that communication is stored, you create a safer work environment, reduce harassment, and make your company more attractive to new hires.

Modern Workplace Challenges

A. Restrictive Access
"I can't get into my email"

B. Limited collaboration
"You're working on the old version?"

C. High-pressure environment
“Legal needs this information for a lawsuit.”

D. Increased vulnerability
"Let's find a workaround; we need this done."

E. Business disruption
"The email looked like it was from the CEO."

As an added benefit, such a workplace begins to achieve ancillary company goals, like employee engagement. People today expect to work securely from anywhere and “put a high premium on work that enriches and fulfills them,” according to research by Microsoft. When you free them to do that, you make them happier and become a more attractive place to work.

The secure, modern workplace is an ideal state that all companies want to reach, but for various reasons, struggle to get there. It takes much more than the push of a button. As we’ll explore in the next chapter, Zix has constructed the Zix Secure Cloud to neatly answer all of these issues and usher businesses into the future.

Foster a safe and well-governed workplace
Information archiving — Email, Twitter, Slack, Teams |
Data Loss Prevention policies | Encryption

Improve productivity and responsivenesss
OneDrive | SharePoint | Teams | Yammer |
Hosted or Desktop apps

Secure the business
Always up-to-date operating system and applications |
Encryption | Advanced Email Security | Security Audit

Seamless experience
White glove migration | Phenomenal Care

Free your IT team up for the important things
Turkney solutions | White glove migration |
Phenomenal Care

06 Introducing the Secure Cloud

If you buy into the idea that less software is more, simple interfaces offer greater security and productivity, and that a reliance on partners is necessary, you buy into the idea of a secure cloud. Here at Zix, we've built what our customers have asked for, and what we believe is necessary to create a secure, modern workplace.

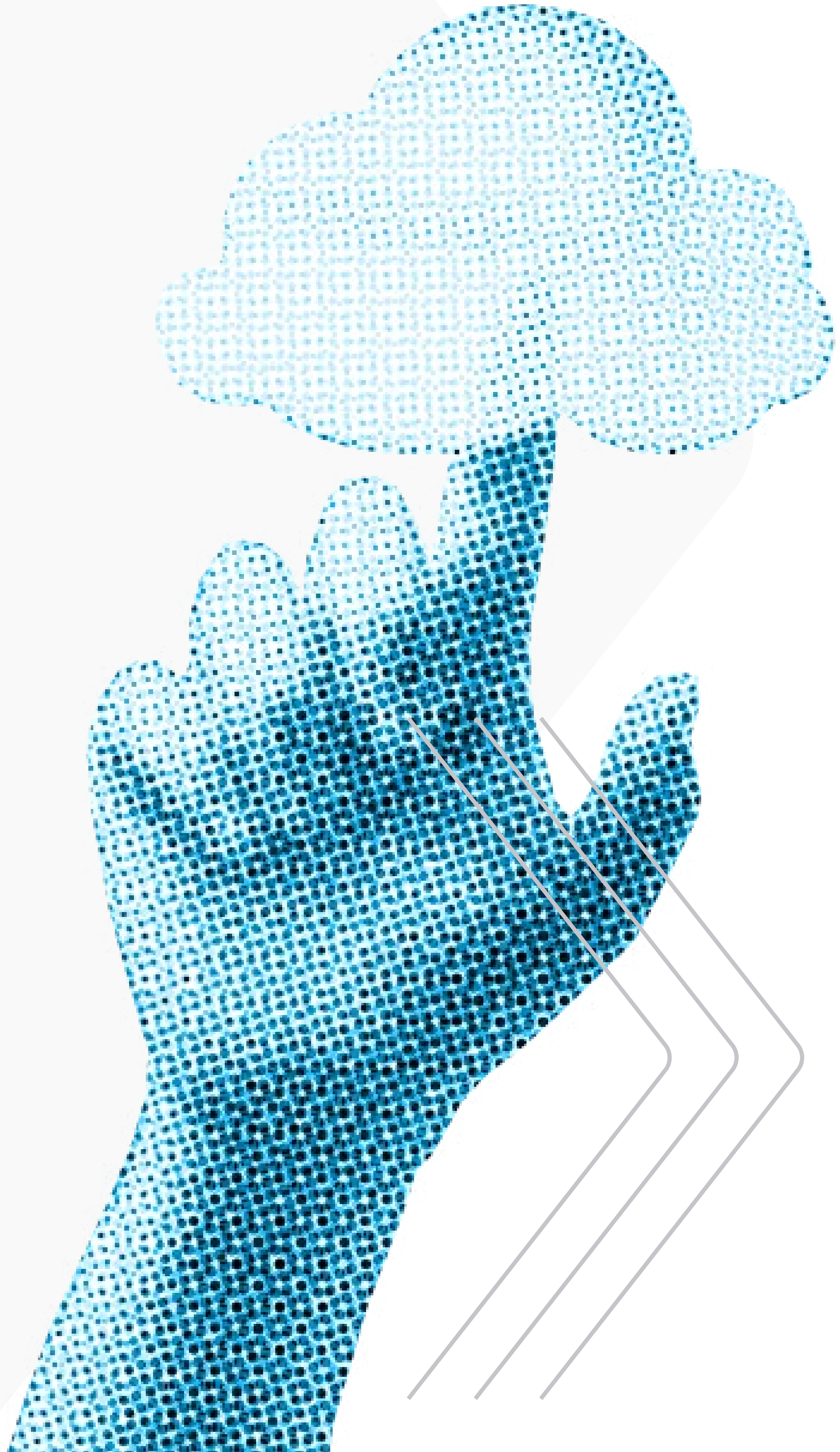
From the surface, users see the Zix Secure Cloud by its most visible element—the applications it offers, which fall into three buckets:

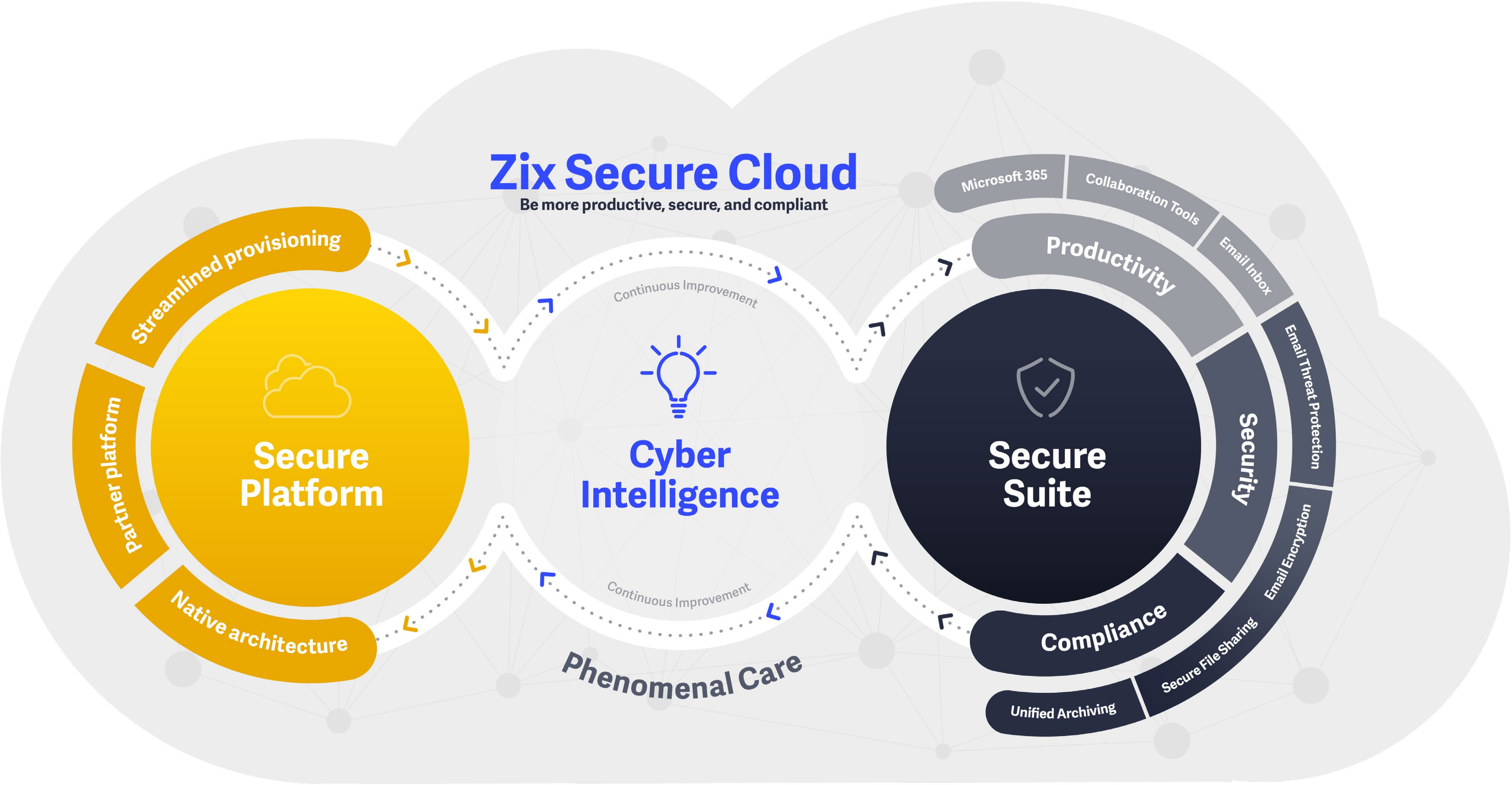
Productivity
Microsoft 365
Communication apps
Collaboration apps

Security
Email Encryption
Advanced Threat Protection

Compliance
DLP and Encryption
Unified Archiving
Secure File Sharing

What is absolutely key and unique to this offering is the degree of interlock between the solutions. They're all best-of-breed applications in their own right, but when deployed as a suite, they seal the most common gaps faced by teams at war with complexity from one pane of glass.




Zix Secure Cloud
Be more productive, secure, and compliant
Streamlined provisioning
Partner platform
Native architecture
Secure Platform
Continuous Improvement
Cyber Intelligence
Continuous Improvement
Phenomenal Care
Secure Suite
Microsoft 365
Collaboration Tools
Email Inbox
Productivity
Email Threat Protection
Security
Email Encryption
Secure File Sharing
Compliance
Unified Archiving

- ○ **Because Zix** hosts your Microsoft mailbox, we have unique insight into potentially malicious settings changes.
- ○ **Because Zix p**rovides threat protection and the world's largest email encryption network, your employees are able to communicate freely and get more done.
- ○ **Because Zix** offers unified archiving and eDiscovery, your security, legal, and HR teams comply with some regulations automatically.
- ○ **Because Zix** is the #1 provider of Microsoft Business Email in the U.S., we have a special relationship that allows us to provide the exact right licensing and act as your proxy with support.

And that's only half of it.

The Secure Suite is built upon a **Secure Platform** that provides one single interface from which IT and InfoSec teams (in-house or outsourced) can manage their productivity, security, and compliance applications. Rather than many disparate systems with different logins, interfaces, and quirks, Zix offers one, complete, best-of-breed solution. And we're always improving it.

Between the Secure Suite and Secure Platform is what we call Zix **Cyber Intelligence**, which is a combination of people and automation that continuously improve Zix's offerings. There's machine learning to adapt each customer's email filters and settings, and teams like Zix's 24/7 threat analyst team and compliance analyst team that are constantly conducting investigations so your team doesn't have to.

Undergirding it all is what we call our Phenomenal Care—a level of service that goes far beyond support and creates a culture of doing whatever it takes to help your business move forward. At Zix, we understand that your team is wrestling enough complexity. Our user interfaces are simple and intuitive. Our solutions consultants are uniquely effective at solutions mapping and looping in advice from experts, and our support team is so effective it resolves 97% of issues on the first call.

The net impact of having Secure Cloud is it strips away a considerable amount of complexity from your network environment. It frees IT and InfoSec teams to plan for the future, it makes your employees more productive and secure, and it sets you up to scale your team's capabilities without having to scale your budget. In sum, it helps you create a secure, modern workplace.

Secure Cloud benefits:

- *Increase productivity*
- *Empower employees to communicate freely*
- *Attract better candidates*
- *Guard against threats*
- *Get ahead of regulations*
- *Enter new markets*
- *Launch new business lines*

Conclusion

The Cray-1 supercomputer grew outdated just as quickly as it was introduced. As has been the fate of all technologies since the industrial revolution, it was copied, shrunk, and supercharged. A time-lapse video of its evolution to the present might show it being folded into a smartphone. What was essentially a 5.5-ton calculator is now one app among dozens on a pocket-sized platform with a single, user-friendly interface.

We think it's been a similar story for the Secure Cloud. What once required dozens of best-of-breed apps from just as many vendors is now a single pane of glass for your business' productivity, security, and compliance needs. For businesses seeking to expand, grow, and offer better services but locked in an unending battle with complexity, we think there could be no better tool. Our customers agree.

Learn more about Zix Secure Cloud at [Zix.com](https://zix.com).