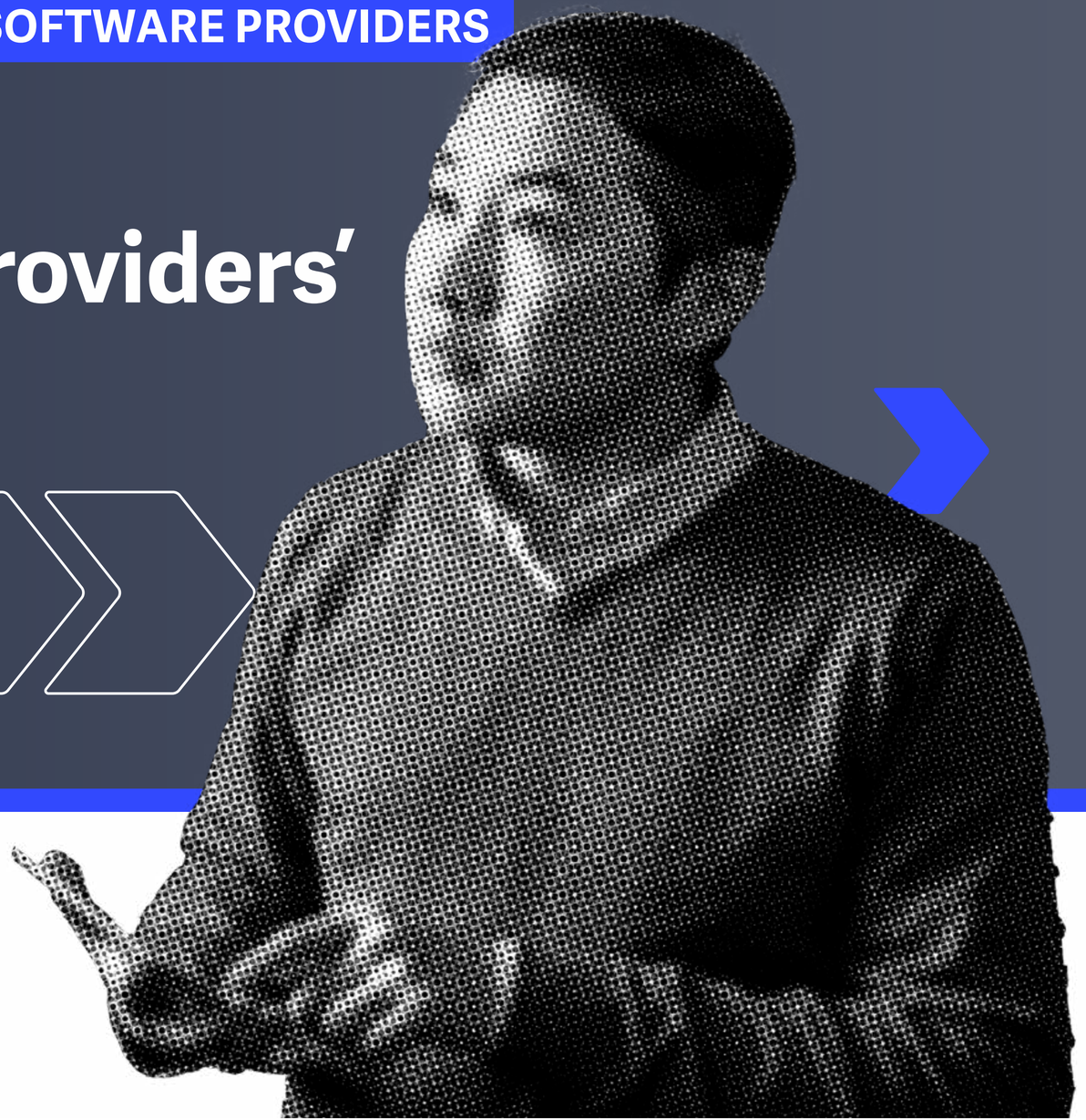
THE SECURITY SCAN GUIDE FOR IT SERVICE AND SOFTWARE PROVIDERS

The Flaw in the Fortress: IT Service and Software Providers' Big Email Security Risk

On Dealing with the Pandemic-Exacerbated Threat that's Hiding in Plain Sight



appriver®

The Danger Lurking in your Inbox

When the COVID-19 pandemic struck, technology came to the rescue. IT service and software providers found themselves in the thick of it—supporting their customers' sudden digital transformations while adjusting to their own new reality. They performed the transition admirably. But little do they know the precarious position they're in now.

IT service and software providers are the poster children of agility: They've embraced the sudden shift to remote work and adopted security solutions like CASBs, cloud-native endpoint protection solutions, and high-end VPNs. And they've done it while navigating the unfamiliar terrain of a strange new market landscape: A sudden uptick in demand for infrastructure as a service (IaaS), a sharp decline in demand for outsourced services, and a softer dip in demand for software as a service (SaaS).

Things are slowly starting to settle, even for outsourced IT services, the hardest hit of the bunch. Experts predict demand for outsourced IT will eventually increase, as many companies have laid off large parts of their workforce and will not be in a position to rehire IT staff full time. But IT service and software providers aren't out of the woods yet. In fact, one of the most insidious threats might be lurking right under their nose. That's because even though IT service and software providers are bullish on new security technologies, they're more likely to forget about the one channel that matters most: email security.

> *Phishing attacks are up 350% since the pandemic.* -UNICRI

Email is where most threats begin—and it's a particular challenge to secure. That's because it often places the burden of security on employees. For instance, they may need to remember to enable encryption settings. More worryingly, they have to remain vigilant against scams. And the pandemic is a perfect storm: Employees are more stressed and cybercriminals are producing a wave of clever scam lures designed to target peoples' pandemic anxieties, from vaccine results to government compensation. To remain safe, IT service and software providers need to adapt to the increasingly sophisticated targeted attack campaigns that threat actors are launching.

In this guide, we'll explain why email security, IT service and software providers' greatest threat, is also their greatest opportunity. The winners in the coming months and years will be those who secure their inboxes.

Part 1. Locked Doors. Open Windows.

While IT service and software providers tend to be ahead of the curve on implementing advanced protections like CASBs and VPNs, that's not where today's attacks are primarily coming from. Cybercriminals still mainly strike through email. And the pandemic has been their playground: Phishing attacks are up 350%, and email continues to be the place that 96% of attacks originate. This is to say, while IT service and software providers have extremely high walls and deep moats, they have lots of open windows scattered about the business in terms of people's mailboxes. And **remote work has exacerbated things**.

Even before the pandemic, email security was an issue because it relies heavily on employees and the honor system. But now, the stakes are higher: Some 64% of Americans now work from home, up from 7% in 2019. That means more potentially sensitive information is traveling over the open internet via email and file transfers (often, non-InfoSec validated ones like Dropbox and WeTransfer, because of 25MB email file send limits). There's always been the possibility of human error—an employee forgets to hit "encrypt" before sending a sensitive email or sends a confidential document over WeTransfer—but this risk has gone up substantially in the last few months.

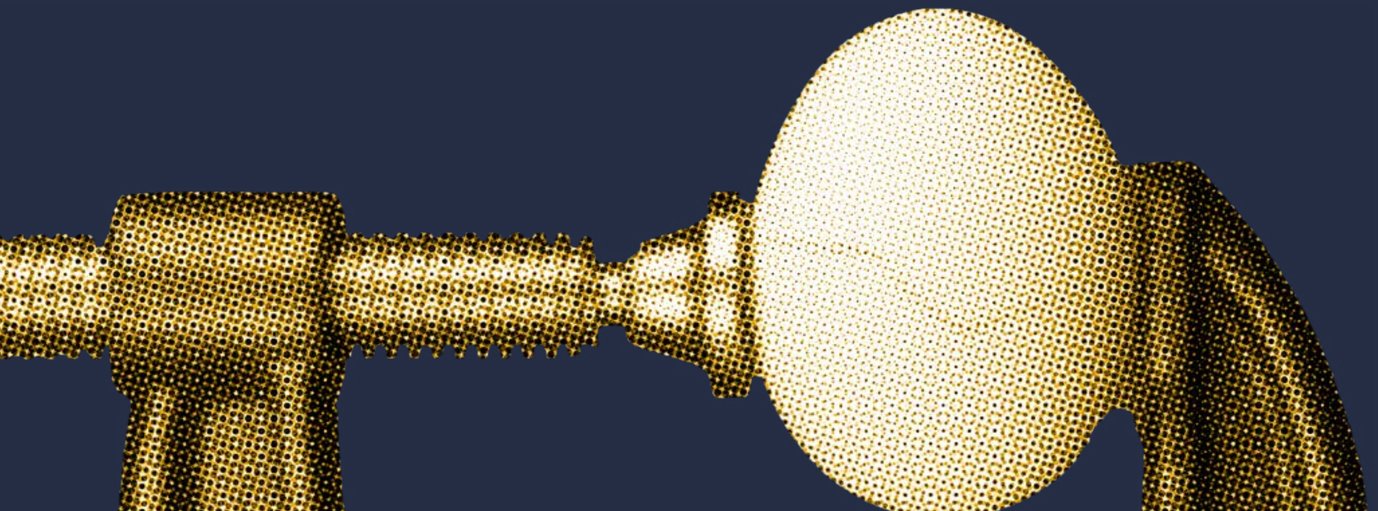
> *Email security is an issue because it relies heavily on employees and the honor system.*

The pandemic has led to an immediate and immense shift in the remote workforce.

Is Stress making you Sloppy?

Not only are there more attacks, more endpoints, and more sensitive information circulating unprotected, but employees themselves are also less vigilant. IT service and software professionals are dealing with a lot. These organizations have been hit at both extremes: Some are busier than ever as they try to keep up with the surging demand for cloud infrastructure and remote collaboration tools. Others are trying to ride out this sudden drop, budgeting their months of runway and making the gut-wrenching decision to furlough or even lay off employees. On top of the upheaval in their work lives, they're coping with working from home, managing child or elder care, and the myriad pandemic-related anxieties that shift on a day-to-day basis.

Studies in psychology show that **stressed people are more prone to making mistakes**—even if they've consistently performed a task well in the past. "In stressful situations, the ability of working memory to direct attention to what's relevant is compromised," notes psychologist Sian Beilock. "A computer is a good analogy. If you're running lots of programs at once, everything slows down. If you add worry to the mix, the attention needed to focus on the task can go awry." Stressed and overworked teams are less careful in their security preparations, and less likely to catch malicious activity, like an unexplained escalation of privileges on a vacant mailbox.



Blame Systems, Not People

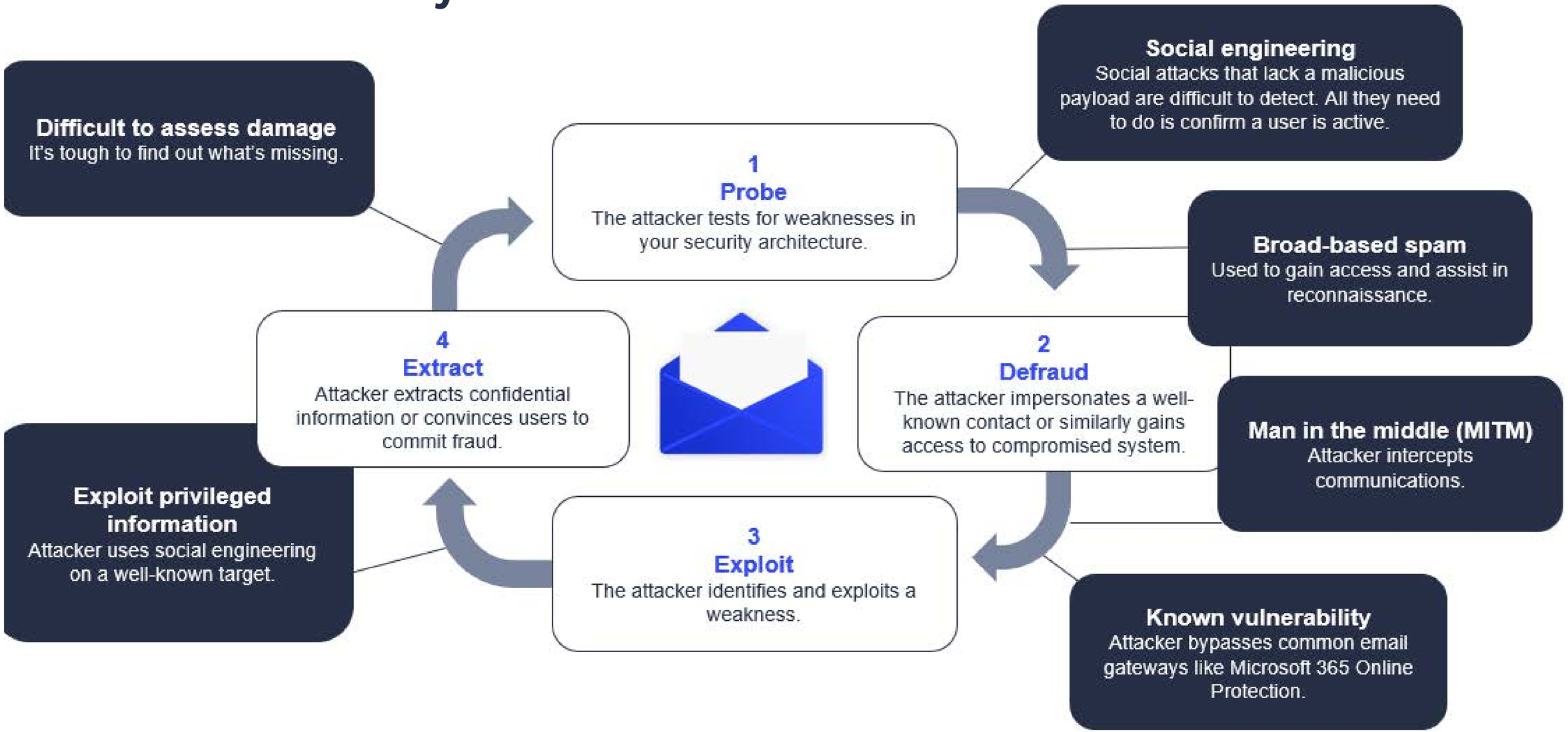
It's human nature to blame mistakes on the people who make them. When a doctor administers the wrong drug, an engineer builds a bridge that collapses, or a pilot crashes a plane, it's easy to attribute these catastrophes to their negligence.

90% of quality lapses "blameless."

But critical safety and security failures are more often the result of flawed systems. A study of mistakes in aviation maintenance deemed 90% of quality lapses "blameless." While you can try to double down on security with scare tactics—naming, blaming, and shaming employees who slip up—fearmongering won't get you far. In fact, it makes people less likely to report security concerns.

"We cannot change the human condition, we can change the conditions under which humans work," reports an NIH study on human error. The solution is to re-examine your systems. Instead of punishing people for not getting it right, the most secure teams put safeguards in place so they can't get it wrong. If your email requires someone to press a button to secure, there's a flaw in your system. Email security shouldn't have to be something that team members add to their cognitive load—it should run smoothly in the background and just work, without employees having to think about it.

The Email Threat Lifecycle



The Stakes for Securing Email

Increased attacks have left IT service and software providers more vulnerable—aided and abetted by the sudden shift to remote work, disruptions in peoples' working lives, and employees' heightened level of anxiety. Research shows that small and medium businesses (SMBs) typically lose a quarter of their revenue following a breach. Breaches are more likely than ever and their high cost, debilitating even in "normal" times, is more than most SMBs can stomach right now. Shoring up email security is more critical than ever.

> *Small and medium businesses typically lose a quarter of their revenue following a breach*
>
> *-Cyentia Institute*

Part 2.
The Critical Gaps—and How to Close Them

In this chapter, we'll summarize the aforementioned concerns into the three major challenges that IT service and software providers face. Together, they show the factors leading to a heightened risk of an email breach and the dire effect such a breach could have on a brand's reputation at this especially vulnerable moment. However, as we will explain near the end of this chapter, these challenges also present tremendous revenue growth opportunities.

The Challenges Summarized:

1 Remote work brings increased security concerns

COVID-19 and the shift to work from home has prompted a wave of new cybercrime. According to the UN's security arm, phishing attacks are up 350%. "From our Cyber Intelligence Centre, we have observed a spike in phishing attacks, Malspams and ransomware attacks as attackers are using COVID-19 as bait to impersonate brands thereby misleading employees and customers," writes Deloitte.

Remote work also means companies' intranets have expanded well beyond their walls, and more communications are happening over the open internet. Employees are sending more email containing potentially sensitive information, and more files. More attacks, coupled with more entry points, means more risk. **To adapt, IT service and software providers need to weave cybersecurity into their remote work policies and provide secure email and file transfer tools.**

96% of threats start with **public email**. -Verizon

4 in 10 threats involve employees; 75% lack skilled resources. -Deloitte

Only 52% of surveyed executives are confident or extremely confident in their organization's security. -Deloitte

2 Teams are stretched thin with more endpoints and responsibility, but less budget

IT service and software providers are facing more responsibilities—and stress—than ever, so they're less able to respond. With stagnant headcount (and sometimes even layoffs) and unchanged budgets, they're being asked to do more with less. There could be no better situation for hackers to exploit them, and IT teams know it.

Stressed and overworked teams make mistakes. But it's often not their fault: Many email security vendors have broad but shallow capabilities that don't take into account some of the dependencies that remote work introduces, like more email communications and more cloud-based inboxes. As an example, many vendors can't detect subtle changes to a hosted mailbox until it's too late. The only way for IT teams to catch it is to be monitoring every inbox frequently, which is impossible for them to do. **To adapt, IT service and software providers must centralize security under one title, and standardize systems across the business, so security features function on autopilot.**

One-third of Americans have experienced high levels of psychological distress during the pandemic; for those facing financial difficulties, that number jumps to 55%. -Pew Research

79% of business leaders say new business models introduce technology vulnerabilities faster than they can be secured. -Accenture

3 The impending great separation

In times of uncertainty, the people buying from IT service and software providers will increasingly default to working with big, reputable providers. Plus, the assumption is that the better known a provider is, the tighter their security, and the easier it is to request budget to hire them.

Over time, this will lead to what's known as 'the great separation' where the top IT services providers will pull so far ahead that others may never catch up. For mid-market IT services companies, the U.S.'s 50 largest companies which receive 40% of all IT services revenue pose a great threat. The better mid-market providers can secure their email, the better they'll be able to ride the separation—rather than be buried by it. **To adapt, IT service and software providers must secure their most vital channels of communication—email and file transfer—to retain a high degree of trust.**

A lack of trust cost U.S. businesses $756B . -Accenture

Small businesses are especially at risk:

- 43% of breaches in 2019 involved SMB . -Verizon
- SMBs typically lose 25% of revenues after a breach. -Cyentia

The opportunity in all this

There is good news after all. If IT service and software providers solve the aforementioned issues easily and affordably, they're at a competitive advantage. While competitors face risk and exposure, those who have addressed cybersecurity are more agile, more profitable, and more able to swiftly enter new markets without incurring unacceptable risk.

Specifically, dealing with these issues allows IT service and software providers to:

Reduce risk of hacks and breaches:

Hacks and breaches are increasingly expensive. If IT service and software providers can shore up their email defenses, they reduce costs.

Free teams for higher-order challenges:

Businesses everywhere are blocking and tackling trying to figure out what comes next. If IT service and software providers are no longer mired in the minutiae of managing email encryption and threat protection issues, they're freer to help the business expand into new markets, select new partners, and grow.

Invent better processes:

With more elastic software services, manufacturers are freer to scale up or down business units quickly, or reallocate head count.

Save budget:

Teams that are able to consolidate vendors, and select cloud providers, often get better unit economics. There are lots of things they can do with that repurposed budget.

Become essential, ride the great separation:

IT service and software providers that are seen as reliable, reputable, and leaders in their field will win the lion's share of business and enter a virtuous cycle of growth.

How to seize the opportunity?

In the next resource in this series, **The Security Scan Playbook for IT Service and Software Providers**, we provide a step-by-step checklist for manufacturers to address these issues, and seize the opportunity.

The Security Scan Playbook for IT Service and Software Providers

Access my copy of the playbook