Whitepaper

jumpcloud

Zero Trust Demystified

Simplifying the Zero Trust Journey for Small and Medium Enterprises

Contents

Zero Trust is a security model that has gained traction since the shift to remote work, and has now become necessary for all small to medium-sized enterprises (SMEs). However, its novelty and pervasiveness in the market have earned it buzzword status, giving rise to confusion around what Zero Trust is (and, equally important, what it isn't), whether businesses need it, and how to achieve it.

Zero Trust arose for a reason, and despite its reputation for complexity, it's actually a straightforward (but important) concept: that employees should only have the necessary amount of access to accomplish their tasks.

Despite its straightforward core concept, however, Zero Trust implementation takes time and planning. In Forrester's *Practical Guide to a Zero Trust Implementation*, it estimates that a typical Zero Trust roadmap might extend about two to three years.[1] What's more, the initial steps (like the mapping process itself) can take significant time and resources.

Fortunately, there are many Zero Trust wins businesses can implement quickly and cost-effectively, and many more Zero Trust elements businesses already have in place, even if they weren't implemented for the purposes of Zero Trust (like multi-factor authentication (MFA), mobile device management (MDM), and identity management projects). Small tweaks to these structures or building off of them can speed up your overall Zero Trust progress alongside your planning and mapping processes.

This guide intends to demystify the complexity that's built up around Zero Trust and help you identify and implement quick wins in your organization as part of your longer Zero Trust journey. From clarifying its definition and place in the market, to outlining actionable Zero Trust steps that can kickstart your progress, this guide is designed to accompany you on your Zero Trust journey, offering practical guidance alongside your strategic, long-term planning.

What Is Zero Trust? What Isn't Zero Trust?

Trust nothing. Verify everything.

What Is Zero Trust?

The term "Zero Trust" has been overcomplicated by "latest-and-greatest" products and overzealous sales pitches. As Forrester puts it, "Zero Trust is the trend du jour in the security vendor community, giving it the stigma of a buzzword."[2] Because of this, it can feel more like confusing jargon than a meaningful practice.

However, Zero Trust is much simpler than the market positions it to be, and the sentiment behind it remains strong. When boiled down, Zero Trust is essentially the mantra, "trust nothing; verify everything," put in practice, and it's critical to protecting your organization against modern threats.

Recommended Reading

In August, 2021, Forrester released a **Practical Guide to a Zero Trust Implementation**, in which it guides IT professionals through the process of identifying their Zero Trust maturity, creating Zero Trust security goals, and drawing up a roadmap to get there. Consider reading it alongside this whitepaper for a more holistic view of Zero Trust security and how to plot your long-term journey to a pure Zero Trust architecture.

What Isn't Zero Trust?

While some vendors and sales teams may want you to believe otherwise, Zero Trust is not a product or service. Although Zero Trust has become productized in today's market, Zero Trust isn't something you can purchase or add to your stack; rather, it's a modern framework for securing IT infrastructure. While products and services can help you construct a Zero Trust architecture, getting on board with every latest and greatest solution can be more harmful than helpful in the long run. Instead, smart Zero Trust journeys look for strategic solutions that work holistically within the existing environment.

The Origins of Zero Trust

Zero Trust was developed in response to the shortcomings of the outdated "castle and moat," security method that was designed to protect on-premise environments. In this method, organizations would secure their networks and resources by building strong controls at the perimeter with tools like firewalls, intrusion prevention, and VPNs. The method inherently trusted anything that made it past the perimeter controls and onto the corporate network.

This perimeter approach to security made sense when businesses were constrained to physical spaces that had an actual perimeter. Servers were stored in the server closet, devices wired into them, and the office was protected under lock and key. Now, however, work can happen remotely, in the office, and on the go; resources must be secure, no matter what form they take, where they're located, or how they're accessed.

This perimeter security method fails in modern environments on two key accounts. First, cloud services and remote workplaces have rendered the idea of a physical perimeter — which used to be an office building with legacy wired equipment — irrelevant. In perimeterless environments, positioning security at the main entry points no longer suffices — in fact, it can be hard to even determine where those entry points lie when resources are cloud-hosted and accessible from anywhere. Instead, security today should focus on securing devices, identities, and access.

The second area where perimeter security falls short is that it places all of its safety guards at the initial access transaction (i.e., the perimeter), and trusts these safeguards so fully that it assumes that anyone inside the perimeter is trustworthy. While a desirable ideal, this has proved unrealistic; cybercriminals are now so fast and sophisticated that security experts say attacks are inevitable: plan for when, not if they occur. Security without backup and mitigation contingencies, like many perimeter security implementations, is little more effective than no security at all.

Zero Trust in Practice

To address these shortcomings, Zero Trust prescribes secure authentication at every access transaction — not just the outer perimeter. This addresses the increasing complexity of the now virtual perimeter.

While Zero Trust can take time to implement fully, its core framework is quite straightforward. In practice, Zero Trust requires the following three elements:

- **Principle of Least Privilege (PLP)**. PLP lies at the very heart of Zero Trust. Zero Trust's goal is to ensure that no one can access anything that they shouldn't be able to. This goes for employees, customers, and third-parties alike: end-users shouldn't be able to change network settings; customers shouldn't be able to see other customers' data; cybercriminals shouldn't be able to access any corporate resources or data. PLP ensures everyone only has access to what they need — no more.
- **Secure authentication**. Passwords have been around since the 1960s. Now, about six decades later, cybercriminals have mastered the art of infiltrating the password so completely that the password is no longer a reliable method of security. In fact, 61% of breaches[3] involved credentials in 2021, and cloud-sourced compute power has broken password cracking down to a science: password cracking tools can crack an 8-character NT-hash password in about 12 minutes.[4] Zero Trust prescribes secure authentication, and passwords no longer meet this mark.
  To fill this gap, companies are using more secure methods of authentication, like MFA and passwordless authentication.
- **Authentication at every access transaction**. It's not enough to just use secure authentication at the outset, or to gate certain resources; Zero Trust prescribes secure authentication everywhere — that's at every access transaction. This "everywhere" contingency directly responds to the dissipation of the perimeter. Instead of assuming that any successful authentication is a friendly one, it continues to challenge a user's identity as they move throughout the network, from application to application, and even within a system itself. This prevents lateral movement in case of a breach: if a cybercriminal does gain access to a resource, they aren't guaranteed access to the rest of the network.

Zero Trust: The Virtual Lock and Key

The Zero Trust concept stems from a highly familiar in-person form of security: the lock and key. In offices, employees often have badges that grant them access to the main building, and then the suite and rooms they're assigned to, while it might still deny them access to other office suites and high-security rooms. Some badges might also include a photo as a second form of identification. Zero Trust virtualizes this security process: it creates and stores identities and their permissions — often through a directory platform — and uses secondary forms of verification for reliable security at every access transaction.

Benefits of Zero Trust to Small and Medium Enterprises

Security

Cybercriminals don't just target large conglomerates and Fortune 500 companies; cybercrime trends tend to follow similar patterns in small and large businesses alike.[5] And they're on the rise. The shift to remote and hybrid remote work created a security gap: many organizations adopted remote models quickly and haphazardly, and security took a backseat to keeping the business afloat. Cybercriminals acted quickly while companies' defenses were down, and cybercrime skyrocketed in 2020.[6] Today, bad actors continue to exploit gaps in companies' remote and hybrid infrastructure, and cybercrime continues to rise.[7]

Remote and hybrid environments necessitate modern security; while the perimeter method may have gotten companies by before the pandemic, it's no longer adequate in the face of modern environments and threats. Now that the average SME has 30% of employees working remotely and 32.5% working hybrid-remotely, SMEs' security programs need to support remote and hybrid setups.[8] In fact, SME IT professionals ranked "adding layered security so work-from-anywhere is truly secure" as their top priority for both 2021 and 2022, and over 80% agreed that remote and hybrid-remote work increased their focus on security.[9]

IT Industry Pulse Check

JumpCloud conducted two surveys in 2021 to assess SME IT professionals' experiences with their technology in the rapidly changing workplace. The first survey, conducted in April, reflects organizations' changing priorities in the face of remote work. The second survey, conducted in October, shows IT professionals pivoting to embrace security and work-from-anywhere models.

As Zero Trust is designed to protect modern cloud environments, it provides the best defense against cybercrime and offers SMEs a sustainable security foundation for long-term remote and hybrid work.

Usability

Zero Trust frameworks are designed to accommodate cloud resources, which have evolved to be more user-friendly than their legacy counterparts. As such, Zero Trust implementations tend to be similarly cloud-based and user-friendly. From reducing the user's need to remember and input passwords to automating onboarding and offboarding, Zero Trust implementations tend to improve the employee experience. Pure Zero Trust environments use integration, automation, and a single source of truth, which in turn offer users consistent, intuitive, and seamless experiences.

Future-Proof

Because Zero Trust was designed to work within and support cloud environments, it is better-suited to securing cloud-based resources than older security models. As the shift from legacy to cloud continues to pick up steam, Zero Trust will likely continue growing in popularity and replacing perimeter security models over time.

Further, Zero Trust's departure from physical infrastructure makes it more malleable and adaptable than traditional perimeter-based security and, therefore, better-suited to adapt to future changes. Most Zero Trust tools and practices are software-driven and can be controlled virtually, allowing them to adapt and scale as organizations and technology do over time. This is particularly important to the SME, which needs to remain nimble and adaptable amidst frequent organizational and market changes.

Better Admin Experience

Zero Trust's software-driven architecture makes it easier for IT to manage. While its implementation is a large undertaking, its adaptability, automation, and remote accessibility make it user-friendly to the IT administrator in a hybrid-remote environment. Further, Zero Trust architectures provide better visibility into the infrastructure as a whole and its activity. This simplifies security administration, making it easier for IT admins to detect and address issues before they become breaches.

Streamlining the IT admin's experience heightens security while creating an environment that fosters smooth organizational changes, scaling, and IT maintenance. In SMEs where IT departments may be strained, this saved time can be reallocated to make a significant impact in other IT initiatives without compromising on security.

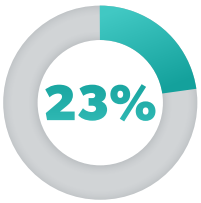
Why Haven't More SMEs Adopted Zero Trust?

According to a survey conducted in late 2021, a little over half (58.6%) of SMEs reported pursuing or planning to pursue a Zero Trust security program.[10] In another survey conducted in the same year, only 23% of respondents said they had fully adopted it already.[11] If Zero Trust is so beneficial to SMEs, why haven't more of them adopted it yet?

The Piecemeal Problem

The all-too-common products claiming to be the "Zero Trust magic bullet" have been more harmful than helpful to Zero Trust adoption. The SaaS market tends to encourage companies to keep up with the latest and greatest tech; companies, in turn, end up stacking their infrastructure with security tools that lack cohesion and strategy. This ad-hoc purchasing approach and high tool volume tend to move companies further away from Zero Trust rather than closer to it.

These cluttered infrastructures require many complex integrations to get tools to work with one another. They likely contain many dependencies (which are not all documented) that slow any agility that the tools might have promised. Anything from a tool update to a new addition to the stack can break one integration, sending a domino effect through the rest of the infrastructure.



Percent of SMEs that have fully adopted Zero Trust

SOURCE: IT Trends Report

Businesses working within such an environment, therefore, hesitate to make sweeping changes to adopt Zero Trust. Businesses that went this piecemeal route to achieve Zero Trust might have abandoned the cause after witnessing an ever-increasing complexity without any increased security to show for it.

Cost and Labor

The piecemeal approach to Zero Trust can cause costs to compound — not just in terms of solution purchases, but in terms of the labor and expertise it takes to manage them as well. Introducing new solutions in an environment requires ramping up time and training followed by ongoing management and maintenance. This ongoing labor can either be filled in-house or by hiring additional expertise. Because point solutions tend to accumulate, SMEs that manage them in-house often end up with strained IT teams. Those that hire new employees or external help usually find that cybersecurity expertise is hard to come by and expensive, which can quickly make this approach cost-prohibitive.

Overcomplication of Zero Trust

For many, Zero Trust seems like a monumental undertaking that intimidates them. For many more, Zero Trust remains somewhat of a mystery. IT professionals are tired of hearing about the latest and greatest "Zero Trust product" and feel that Zero Trust is just another buzzword.

In addition, seeing many different tools with "Zero Trust" labels can further confuse the Zero Trust concept, making the Zero Trust goal feel too broad and unattainable for SMEs. But in reality, it's a straightforward concept that can have a lasting impact, even when implemented in incremental phases.

Simplifying the Journey

There are many stages in the Zero Trust journey that precede the end goal of a pure Zero Trust architecture, which takes years to achieve. The best way to start and plot your journey is to embrace your perimeter/Zero Trust hybrid state and set your sights to smaller, achievable milestones.

In its Practical Guide to Zero Trust Implementation, Forrester recommends mapping those milestones in three key phases:

Milestone Mapping Phases

1. Assess your current Zero Trust maturity.
2. Understand current business initiatives, including where you can leverage existing technology.
3. Set future-state goals and a timeframe to achieve them. This becomes your roadmap.

The goals and roadmap developed in step 3 can be broken up into five categories, which Forrester recommends addressing in roughly the following order:

Roadmap Stages

1. Identity.
2. Workloads.
3. Devices.
4. Networks.
5. Data.

This order allows your security to compound and build off of existing initiatives to form a cohesive Zero Trust security framework. However, these phases are (purposefully) broad; when your entire infrastructure stands to be reformed, it can be hard to know where to begin.

In the next section, we'll cover some high-impact Zero Trust implementations in each of the five categories above and methods for deciding where to begin.

Actionable Steps to Kickstart Zero Trust

Forrester's Practical Guide to Zero Trust Implementation offers a holistic method for plotting your Zero Trust journey from A to Z. However, if you're under pressure to get started, working on achieving buy-in, overwhelmed by your roadmap, or feeling stuck in your journey, taking any step forward can be more productive than agonizing over which step to take first.

To help IT professionals find direction quickly, this section will outline some of the core elements of the Zero Trust roadmap. These implementations make significant, direct impacts on the three core elements of Zero Trust: the principle of least privilege (PLP), secure authentication, and authentication at every access transaction. This list should help you identify what you already have in place and what might be easy to implement in your environment.

Impactful Zero Trust Implementations

Identity

- **MFA everywhere.** Implementing MFA everywhere is a significant step toward Zero Trust. It graduates your organization from relying on the highly vulnerable password to an authentication process that not only significantly improves login security, but also prevents lateral movement in the event of a breach. MFA tools can be low-cost — some even come free with identity and access management (IAM) and directory software — and generally easy to implement. Newer MFA technology like push notifications and biometrics streamline the experience, making this a palatable step for users.
- **IAM.** A cohesive approach to IAM creates a single source of truth for the identities in your organization. This is critical to establishing secure authentication practices and maintaining PLP.
- **Streamline onboarding and offboarding.** In SMEs, growth and churn can run high, and manual onboarding and offboarding are both inefficient and insecure. Onboarding and offboarding should be as automated as possible. Automating onboarding helps companies bring employees on remotely; automated offboarding prevents IT teams from accidentally forgetting to revoke access from any resources. This step generally follows IAM implementation; tracking users' accounts with one source of truth helps automate account provisioning and deprovisioning.
- **Single sign-on (SSO).** SSO helps organizations reduce password usage by allowing users to log into all the resources they need with one set of credentials. To uphold Zero Trust's secure authentication requirement, SSO should be secured with MFA.
- **Conditional access.** Conditional access uses contextual information to judge the security of a login and act accordingly. For example, secure login attempts could bypass an MFA requirement while insecure login attempts — like an attempt from an unknown device using public WiFi — could be prompted with MFA or denied outright. Conditional access both rewards users with lower friction in secure, predictable environments and locks down security for suspicious behavior.

These implementations make significant, direct impacts on the three core elements of Zero Trust: PLP, secure authentication, and authentication at every access transaction.

Workloads

- **Resource visibility.** Your organization should be able to track and view all resources — systems, software, files, applications, and assets — on its network. This helps ensure they are all properly secured and enforce secure authentication at every access transaction.
- **Access control.** All your resources should be assigned access controls according to PLP. Role-based and attribute-based access control methods are ideal for assigning secure and appropriate permissions. Resource visibility and an IAM platform are typically prerequisites for this step. Even better, an IAM platform that can enforce access controls on your company resources implements both in conjunction with one another. This combines two critical functions while enabling intuitive, contextualized rules that report to a single source of truth.

Devices

- **Device visibility.** You should be able to see and manage all the devices accessing corporate resources. Now that environments are largely hybrid and remote, this should include smartphones and other mobile devices, both corporate-issued and employee-owned.
- **MDM.** A step beyond device visibility, MDM grants organizations the ability to manage the devices connecting to its resources. The need for MDM increases with remote and hybrid-remote companies, where security can quickly fall to the wayside without close management in place.
- **Patch management.** Vulnerability exploits are a popular attack vector; a recent study found that 60% of breaches could have been avoided with a patch that was available at the time of the breach.[12] Patch management processes and tools are significant to closing this gap, and especially important in modern SMEs where devices may be remote and dispersed. Patch management should allow you to, at any moment, confirm with confidence that all the devices and software accessing your company's data are up to date on their patches. Your patch management system should be able to do the following (but achieving one step at a time is still good progress):
  - Identify and alert to missing patches.
  - Schedule and enforce patches.
  - Offer visibility into patched and unpatched devices and software.

Networks

- **Segmentation.** NIST names micro-segmentation one of the key methods of pursuing Zero Trust.[13] Network segmentation with strategies like dynamic VLAN assignment helps build smaller, software-based perimeters within larger network structures. These perimeters prevent lateral movement, protect core assets, and help apply PLP: only those with the highest permissions should be granted access to the VLANs that host the most sensitive resources.
- Infrastructure visibility. Visibility is critical to maintaining security. Event logging, SIEM tools, threat detection tools, and directory telemetry all contribute to infrastructure visibility.

Data

- **Data encryption.** Data should be encrypted both in transit and at rest. Cloud providers tend to manage this for cloud-based services; start by auditing your current SaaS providers' practices. To rectify any tools that don't use encryption, you could change the tool settings or licensing (if encryption is offered), supplement with separate means of encryption, or switch providers. Data stored on devices needs to be protected by the devices themselves. Full disk encryption can automatically encrypt all locally stored data; some MDM and directory solutions like JumpCloud automatically and remotely enforce full disk encryption.
- **Central directory.** A central directory can unify virtually all of the Zero Trust components in your stack under a single source of truth. Modern cloud directories use secure protocols to connect many different types of resources, including users, devices, networks, applications, files, equipment, and more. Some, like JumpCloud, even come with many Zero Trust-driven features baked in, like MFA, MDM, patch management, and telemetry. Implementing a central cloud directory can be one step that spans several Zero Trust strides at once.

Where to Start?

There are a few angles you can take when deciding what to prioritize. However, the key to any of these angles is prioritizing the steps that make the most sense for your organization. Below are a few guiding metrics to choose from when identifying which steps will be most impactful.

Start Small

For some organizations, baby steps are the best route. This may be the case for strained IT teams, smaller organizations, organizations at the very beginning of their journey, and organizations without much leadership buy-in.

Small steps don't have to yield small impacts. Some small, low-cost initiatives can have substantial effects on your security and move you significantly closer to your Zero Trust goal.

The key to any of these angles is prioritizing the steps that make the most sense for your organization.

Example of a small but impactful initiative:

MFA everywhere. Many organizations already have MFA in place in some of their tech stack. Expanding this to cover more of their tech stack — to eventually be in place everywhere — has substantial security gains, and can be cost-effective and easy to implement. Most users are familiar with MFA processes, so buy-in effort is usually minimal. Some MFA solutions even come free with IAM and directory software, which can further amplify your Zero Trust progress. Investing in one tool that can do both (among other Zero Trust initiatives, like automating offboarding and patch management, for example) is a cost-effective way to spur significant progress.

Start With High-Traffic Tools

Another place to start can be at high-traffic junctures: what people use the most. For instance, while securing access to documents only HR leadership uses may be worthwhile, its low usage might allow it to wait while you focus on more frequent touchpoints, like collaboration platforms or project management tools. This method can be ideal for larger SMEs with many users working on certain platforms and remote or hybrid SMEs that worry about proper tool usage in unsupervised environments. Securing these high-traffic tools can be a great catch-all safeguard to start with.

Example of a high-traffic tool to start with:

Single sign-on. SSO can apply to all employees and all resources, making it a high-traffic tool with a high security yield. Implementing SSO is a low-cost and low-effort way to drive immediate security benefits across your organization.

Secure the Crown Jewels First

This methodology approaches security at the most critical level first. Of course, in an ideal world, you'd be able to secure all the elements in your infrastructure right away. But prioritizing one thing de-prioritizes another by nature; understanding your company's infrastructure, resources, environment, and threat vectors can help inform these tough choices.

Thus, this approach works well in organizations that already have a good understanding of their environment, resources, and stack, and can easily identify their most critical assets. If inventorying your infrastructure to identify your crown jewels becomes a large task that could hold up progress, consider starting with another, more digestible step instead as you inventory and assess your infrastructure.

Example of a step that secures the crown jewels:

Network segmentation. Segmenting the network to at least guest and corporate levels can work wonders in protecting your critical assets. Segment resources on each segmentation based on PLP, with the crown jewels only accessible on the admin/highest-privilege network.

Note: Don't Underestimate Usability and Buy-In

Even the best-laid Zero Trust plans won't take hold without buy-in from users, IT, and leadership.

Buy-in from users stems from usability. As cloud-based tools become more user-friendly and people integrate technology more heavily into their personal lives, users expect clear, intuitive, and seamless technology experiences in and out of the workplace. In fact, the employee experience is becoming a key differentiating factor when it comes to employee retention. Thus, implementing a security system that accumulates friction for the user will result in avoidance, shadow IT, human error, and even higher employee churn. This failure to seamlessly adopt the security practices can create more vulnerabilities than they prevent — shadow IT and human error in particular are substantial contributors to security breaches.

Similarly, the IT team should also experience usability gains when implementing new security measures. While the initial implementation can be expected to create work and friction, the long-term plan should produce a better management experience for your IT team. Otherwise, you'll face similar challenges like avoidance, workarounds, lack of maintenance, and failure to maintain one source of truth. These challenges create an environment with poor visibility and a lack of central management — a breeding ground for security threats.

Finally, buy-in from leadership and stakeholders should never be underestimated. Trusting in your security program requires trust in your users and administrators; you need to cultivate a strong security culture, and culture comes from the top. Leadership will either drive or stymie your security efforts based on how they treat security. If leadership doesn't believe in or emphasize the importance of your security program, you won't be able to achieve buy-in from your users or IT team.

On the other hand, if leadership believes in your initiatives, you'll not only have the funding and support to invest in the initiative, you'll also have reinforcements when it comes to enforcing security best practices across your organization.

Overall, when choosing which Zero Trust steps to take, consider buy-in from the user, IT team, and leadership perspective. Choosing steps that will deliver a positive user experience, align with existing buy-in, or easily cultivate buy-in can help ensure the steps take lasting hold.

Choosing Technology Solutions

While it's important not to overload your IT stack, you will likely need to invest in technology solutions somewhere along your Zero Trust journey. When evaluating solutions, keep the following in mind.

Choose a solution that makes sense for your organization. Look for tools that your organization can afford and manage successfully. The robust, feature-rich tools Fortune 500 companies choose might not always make sense for an organization of 50 that needs to accomplish a straightforward task. Similarly, purchasing several popular tools may not be ideal for your organization if one could do the job more cost-effectively. Often, integrated tools offer both cost effectiveness and easier management, making them the ideal investment for SMEs.

Consider compatibility with your current and future state. Organizations that aren't nearing their Zero Trust journey's completion should ensure tools work with both their current architecture (including Zero Trust and non-Zero Trust elements) and their future-state, pure Zero Trust environment. Organizations at the beginning or middle of their Zero Trust journeys should look for tool flexibility and adaptability.

Think ahead. The tools you purchase now will have lasting impacts on your environment. Tools that don't integrate well with another tool in your stack, for example, will plague your environment for years to come. Similarly, overly complicated tools may offer many features, but they can make upkeep tedious as your environment changes. Often, upkeep dwindles over time and creates new security problems. For instance, failing to update a role's privileges can result in users with too many permissions — the antithesis of Zero Trust. Look for tools that keep maintenance streamlined for the admin and the experience positive for the user.

Tool Tip

JumpCloud offers a pricing comparison tool that estimates the cost of different directory and infrastructure implementations based on your organization's size and environment.

Try the Pricing Tool →

Consider costs holistically. A solution's price tag is just one of many costs to consider. The operational costs of maintaining a complicated product, for example, can make it a worse investment than a product with a higher price tag but easier maintenance and lower overhead. Tools that combine several functions can also help keep TCO down by eliminating the need to purchase additional tools. These comprehensive tools also streamline upkeep by ensuring more elements in the infrastructure work well together and minimizing the need for integrations that create compounding tool dependencies down the road.

Take the Complexity Out of Security

Although it sounds counterintuitive, complexity is a detriment to security rather than a strength. Complexity around the "Zero Trust" term has prevented SMEs from embracing it, complexity in the user experience hurts security adoption, and complexity for the IT admin causes infrastructure degradation over time. Instead, straightforward, intuitive, and cohesive solutions form the strongest foundations for a reliable security program.

To help IT professionals eliminate unnecessary complexity from their security initiatives, JumpCloud® has drawn up a library of resources designed to simplify important security concepts and offer IT professionals practical security guidance in real-life environments. Visit the resource library, **Security Without the Complexity**, to continue honing your security strategy.

1. https://jumpcloud.com/resources/forrester-research-practical-guide-to-zero-trust-implementation
2. Ibid.
3. https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf
4. https://jumpcloud.com/blog/the-password-management-queens-gambit-how-to-manage-it-attack-it-and-counter-it
5. https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf
6. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics
7. https://www.idtheftcenter.org/post/identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/
8. https://jumpcloud.com/resources/creating-a-new-normal-for-sme-it-in-2022
9. https://jumpcloud.com/resources/it-trends-report-remote-work-security-cloud-services
10. https://jumpcloud.com/resources/creating-a-new-normal-for-sme-it-in-2022
11. https://jumpcloud.com/resources/it-trends-report-remote-work-security-cloud-services
12. https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf
13. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf