Whitepaper

jumpcloud™ CROWDSTRIKE

Combining Business Priorities and Security: Choose Your Own Adventure

How Small and Medium-sized Enterprises Can Defeat the Security vs. Business Dichotomy

Introduction

Small to medium-sized enterprises (SMEs) are highly nimble, adaptable, and innovative — it's what allows them to keep pace with (and often outstrip) larger competitors. These compact, agile environments are what inspire the collaboration, innovation, and passion that make SMEs a consumer favorite: In a consumer preference survey, 91% of consumers said they would prefer to buy from a small business if convenient.[1]

However, SMEs typically have fewer resources than their larger competitors, requiring high efficiency and strategic decision-making when it comes to resource allocation. Thus, initiatives that drive clear and immediate business value often receive higher priority than non-revenue generating initiatives like security. Over time, this prioritization can create increasingly large security gaps and heightens an SME's risk of attack. It also creates the illusion of a dichotomy between business and security, where SMEs can only invest in one or the other — not both at once.

This perceived dichotomy is exacerbated by a common misconception that cybersecurity is a problem for enterprises, but not for SMEs. This belief, built largely upon news cycles' tendency to focus on the largest and most impactful attacks, lulls many SMEs into a false sense of security.

42%

Over 42% of small business respondents had experienced a cyber attack between October 2020 and October 2021.

In reality, SMEs are targeted just as frequently (if not more so) than their larger counterparts. In fact, a 2021 survey found that over 42% of small business respondents had experienced a cyber attack within the last year.[2] Security threats are a problem for all businesses, and effective security is a critical component to stopping breaches and ensuring SME success.

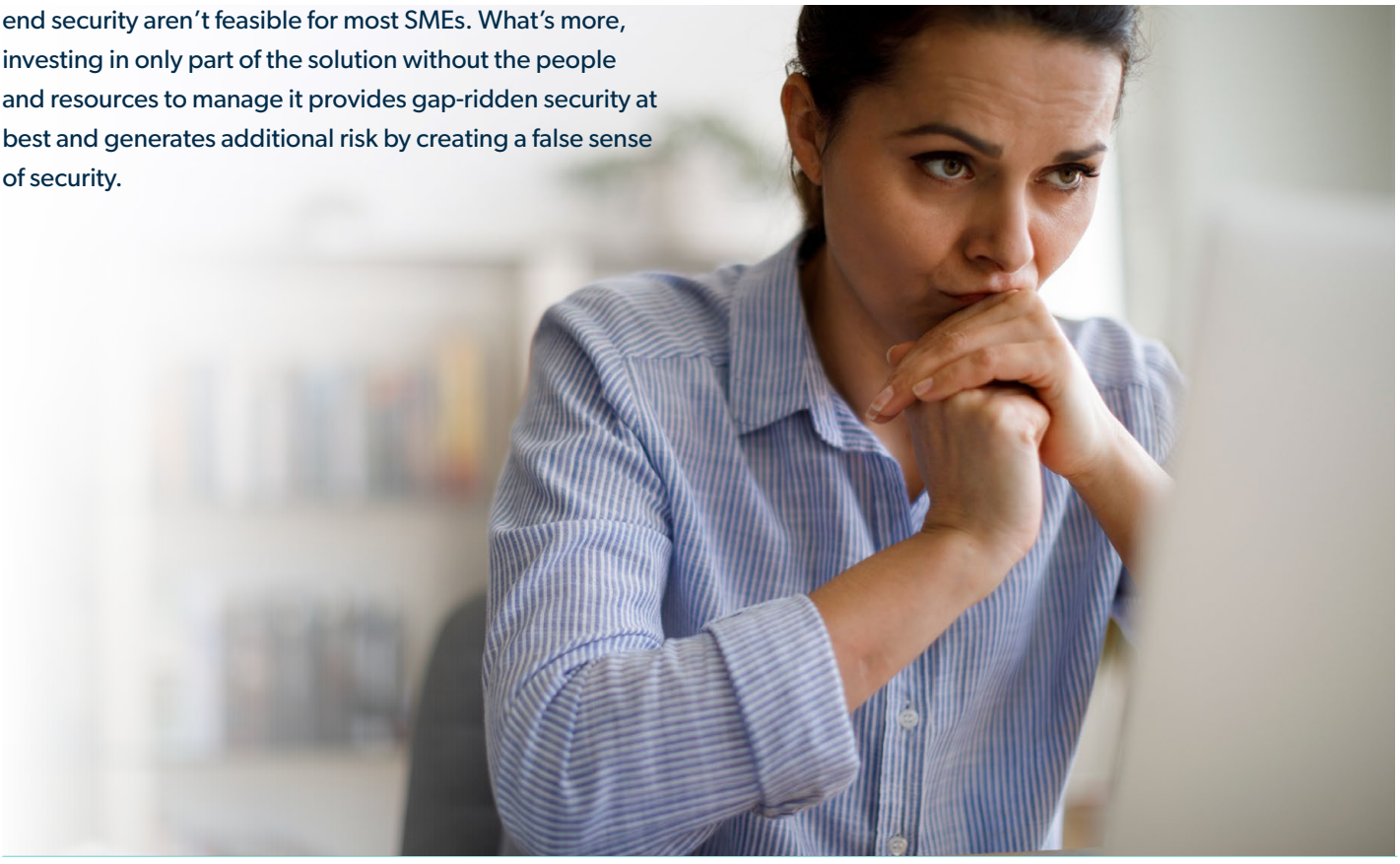
20%

20% of companies' solvency was materially threatened by a cyber attack.[3]

However, even if they feel both business priorities and security are important, SMEs decision-makers are often limited by tight resources, especially when the majority of security products seem to be designed for enterprises. Solutions that require security-dedicated personnel and a combination of several expensive tools to achieve end-to-end security aren't feasible for most SMEs. What's more, investing in only part of the solution without the people and resources to manage it provides gap-ridden security at best and generates additional risk by creating a false sense of security.

These challenges can make investing in security feel like a losing battle. **Fortunately, this perceived dichotomy between security and business is false: it's possible to drive both security and business at once.** While investing in resource-intensive, enterprise-tailored solutions can be too expensive to balance with other initiatives, there are ways to drive both security and business cost-efficiently and effectively. Solutions designed to be manageable, affordable, and still highly secure for SMEs make security much more feasible than many believe. Choosing the right solutions and incorporating them strategically into the stack can make efficient, comprehensive security and business empowerment possible.

This whitepaper will explore the challenges and threats SMEs face today and offer solutions that make sense for fast-paced SMEs with finite resources and limited security expertise. These solutions will not only help SMEs shore up their security, but they'll also help unify their business, security, and IT strategies, allowing them to drive all three forward at the same time. We'll start with the current state of security for many SMEs.



Understanding the SME Security Landscape

While certain high-profile attacks are designed to target the largest, most attention-grabbing organizations, the vast majority have something to gain from businesses of all sizes. In a 2020 survey, over 60% of MSPs reported that their SME clients had been targets of a cybersecurity attack such as ransomware in that year alone.[4]

The reality is that SMEs face significant threats in today's landscape; however, not all SMEs have the internal expertise to understand and defend against current threats. To start, IT and leadership should understand the basics of the threat landscape and how it affects SMEs. This context can help you and your team make decisions about security initiatives, better defend against and respond to threats, and make a compelling case for your organization's need for security.

What Motivates Cybercrime?

To better understand how adversaries might attack SMEs, it helps to understand the motivations behind cyber attacks.

- **Direct payments.**
  Naturally, receiving direct payments from victims is the most efficient way to profit from an attack. In attacks like ransomware, for example, adversaries earn money directly by locking down a company's assets and demanding a ransom in exchange for unlocking them. In others, adversaries may profit by selling breached data, assets, or information.
- **Credentials and network access.**
  Credentials aren't direct revenue in a cybercriminal's eyes, but they're close to it. Hackers often steal credentials and use them to further penetrate the target's network (or other networks), or sell them to other criminals who may leverage them to hack personal accounts, for example.
- **Intellectual property.**
  Adversaries know intellectual property (IP) is valuable and unique, which makes it a highly motivating asset to steal: Adversaries know SMEs will work hard (and likely pay big) to get it back. For similar reasons, leaked IP can be highly detrimental to an SME and highly valuable on the black market, which can motivate cybercriminals to spread or sell it.

The Recent Evolution of Security Threats

The year 2020 presented significant changes to businesses around the world — and security followed suit. Before 2020, when most business was conducted in the office, security threats were more focused on on-premises systems. When businesses moved quickly to remote work after the onset of the COVID-19 pandemic, adversaries shifted their tactics to target remote environments, capitalizing on swifty established (and often vulnerable) distributed environments. Now, businesses are shifting back to in-office work.[5] Security is likely to follow suit and increase its focus on exploiting in-office and hybrid environments.

- **Company information.**
  Like in any good movie heist, the majority of time spent in many attacks is reconnaissance-based: Adversaries often spend a considerable amount of time seeking out information about their target to plan their attack. Information about your network or defense system, for example, could either help the cybercriminal group strike later or be sold to another group looking to mount an attack.
- **Third-party access.**
  In supply-chain attacks, you may not be the attack's first or last stop. Some cyber attacks follow the supply chain to their intended target or leverage company connections by infecting one company or product and allowing it to spread throughout the supply chain.

  Aside from the damage caused by being breached in a supply chain attack, companies may also face compliance and reputational ramifications if they incurred a breach that spread to other parties.
- **Company damage.**
  Some attacks aim to cause damage — wipe data, cause downtime, or even drive a total business shutdown. They are often politically, competitively, or ideologically motivated.
- **Access to resources.**
  Some attacks leverage a company's resources or relationships. For example, a cybercriminal group may target an SME as part of a larger DDoS attack, to hijack compute resources for crypto-mining, or to steal personally identifiable information (PII) for financial scams or fraud.
- **Testing out tactics.**
  When cybercrime groups develop new tactics or mount high-profile attacks, they often test out their tactics first — sometimes, on real businesses. Some unlucky organizations end up acting as the test subject for a new attack vector.

Why Are SMEs Targets?

SMEs are sometimes targets by choice, but they are often targets by chance — even if an SME does everything right, it could still become an opportunistic casualty in an attack on another business. Thus, not drawing attention to oneself is not enough to avoid falling victim to an attack; SMEs must invest in their defenses to protect them against attack, should one occur.

The following are some of the common ways SMEs become cyberattack victims.

- **Playing the unwilling test subject.**
  Cyber criminals function just like legitimate businesses: They strategize and test before rolling out new tactics to optimize their efforts. When cybercriminals develop new tactics, they aren't likely to try them out for the first time in a high-profile attack. Instead, they usually do their testing on small, nondescript businesses whose defenses they expect they can overtake.
- **Becoming a casualty in a supply chain attack.**
  Some attacks hit several organizations by infecting the supply chain. In these attacks, cybercriminals usually target a large vendor's product, software, website, or other asset, and the infection spreads when partners, customers, and other third-parties access the compromised asset. While these attacks often target larger vendors, they trickle down the supply chain to impact many other organizations in the supply chain, and SMEs often end up becoming casualties.
- **Acting as a stepping stone.**
  Cybercriminals may also infiltrate an SME as a stepping stone on their way to a more high-impact target. Attacks may aim to conduct reconnaissance on the target or infect the target through the SME in another form of supply chain attack. SMEs that partner with larger enterprises are more likely to fall victims to this type of attack.

Supply chain attacks can spread rampantly. The famous SolarWinds breach, originally believed to have affected a few dozen organizations, actually impacted over 250.[6]

– **Showing signs of being an easy target.**
There are certain characteristics that may indicate to adversaries that an SME may be an easy or high-impact target. These traits are often results of the limited resources, lack of security awareness/concern, and IT sprawl in many SMEs. Fortunately, these are not inherent traits: SMEs can work to address their weaknesses and secure their areas of vulnerability to avoid being an easy cybercrime target.

- **Underinvestment in security.**
Because security and business seem to be at odds with one another and SMEs often don't see themselves as targets, they tend to allocate resources to other areas before investing in security. This often leaves their defense and response measures (including tooling, processes, and experience) underdeveloped, making attacks easier to mount and carry out without detection or counteraction.
- **Limited IT and security personnel.**
Adversaries are aware that SMEs often don't have the trained security staff to implement and manage enterprise-level security. For example, adversaries know that most SMEs operate during typical business hours (9 a.m. to 5 p.m.) and don't have the resources for 24/7 monitoring outside business hours. Thus, cybercriminals will often mount attacks after hours to maximize their chances of success. They also know IT admins at SMEs tend to have significant workloads and inefficient communication and documentation, which create oversights that make an attack less likely to be caught or stopped.
- **IT sprawl.**
IT sprawl is a common side effect of SMEs' fast pace, which can pressure IT to make quick rather than strategic tooling decisions. While this problem-solving approach might work at the moment, it can result in a plethora of poorly integrated and overlapping point products over time. This makes for a messy and sprawled environment where elements don't integrate or communicate well, creating communication and visibility gaps.

  This complexity makes adversaries' jobs easier by both introducing visibility gaps and lowering the chance of detection after infiltration. Adversaries know many SMEs have sprawling IT environments, and they look for these gaps in visibility and control to aid in their attack and prevent alerts to their activity.
- **Distributed cloud environments.**
Most SMEs have made their way (at least partially) to the cloud. However, this move to the cloud isn't always accompanied by sufficient security adaptations. For example, SMEs commonly implement "bring your own device" (BYOD) policies to save on the cost of issuing devices to every employee, but securing personal devices can be difficult, and SMEs don't always invest in the necessary mobile device management (MDM) tools to secure personal devices. In another example, some SMEs continue to use a perimeter-based security approach rather than adapting to secure devices and identities, or focus on endpoint security while neglecting cloud infrastructure security.

  Adversaries have become adept at exploiting these inefficiencies by stealing remote employees' credentials and using these credentials to access cloud resources.

  In addition, businesses often assume that the standard security that cloud service providers (CSPs) include is enough on its own. However, these standards aren't tailored to individual companies, and they are not robust enough to provide reliable security on their own. Organizations should supplement CSP-provided security with their own; failing to do so can create blind spots.

Investing in Patch Management

Patch management is a fairly straightforward baseline security measure that can significantly improve security; however, patch management isn't as strong as it could be in many SMEs.

About 40% of SMEs take more than one week to implement patches after a known software vulnerability is released. Nearly 40% rely on users to implement patches when prompted.[7]

- **More likely to cooperate.**
  When large enterprises are attacked, they often (though not always) have the resources to recover, even if they can't reclaim all of their lost data, assets, and relationships. However, this isn't quite so frequently the case with SMEs. With tighter budgets and finite resources, an SME being shut down after an attack is a real possibility. Adversaries know and exploit this: With more to lose in an attack, SMEs are more likely to cooperate (i.e., pay ransoms).
- **Positive news and press coverage.**
  Unfortunately, an SME's cause for celebration can be an adversary's cause for drawing up an attack plan. Because cybercriminals look for exploitable data and capital, news about an SME securing funding, experiencing growth, undergoing an M&A, or other similar events could put an SME on a cybercriminal's radar.

  Stopping all progress isn't a realistic way to fend off these attacks, nor is quieting all press about any company wins. Instead, being aware of these triggers is the best defense. This way, when your organization makes waves in the industry, you and your team know to keep defenses tight. (It might also be a great time to jog everyone's memory of security best practices with a quick refresher course.)

In general, shoring up weaknesses in these areas can be beneficial, but it's by no means foolproof. In fact, no method of attack prevention should ever be considered foolproof — organizations of all sizes are now advised to prepare for when attacks occur, not if. Even if an SME were to do everything in its power to shore up its security in the above areas, it could still become a random casualty in a supply chain attack or a target by chance. As such, avoiding common pitfalls and strengthening vulnerabilities isn't enough; SMEs must invest in comprehensive security that can defend against attacks they may fall victim to.

What Types of Attacks Should SMEs Prepare for?

Because adversaries have something to gain from just about any business, SMEs face many of the same threats that enterprises do. The following are some of the most common attack vectors and how they can impact SMEs. Adversaries often tailor these methods to target specific industries, vulnerabilities, applications, or other criminal goals that can pose significant risks and ramifications to SMEs. Note that attack methods are often used in tandem with one another — an adversary might take over an account to mount a ransomware attack, for example.

- **Ransomware.**
  While headlines tend to focus on the biggest attacks on well-known entities, ransomware is still a problem for smaller organizations. In fact, 50-70% of ransomware attacks are aimed at small businesses.[8]

  Ransomware attacks of all sizes generally follow the same basic principles: Adversaries seize and lock a company's data or assets and promise to return it upon payment of a ransom. For large enterprises, these ransoms can reach into the millions. For SMEs, they are often smaller — ransoms as low as $10,000 are common.[9] And while lower ransoms sound like a silver lining, there's a darker motive behind them: Adversaries know SMEs will pay them.

  For established enterprises with decades of built-up resources, six-figure ransoms and the downtime associated with an attack are painful, but not often a death sentence. For SMEs with tighter resources, this isn't always the case — the downtime and loss of data access alone can be crippling for a tightly-run SME. To adversaries, this means SMEs will fight to get their data back — so they demand a "reasonable" ransom and can expect with near-certainty that the SME will pay it. In a recent Capterra survey, 59% of SME respondents whose companies were hit with ransomware said they paid the ransom.[10]

However, ransom payments come with an additional price: The adversaries now know 1) that you are willing to pay ransoms to reclaim your data, and 2) how your defenses work and how your architecture is laid out. This makes repeat attacks highly likely — either from the same criminal organization or from another organization that the attackers sold your information to.

What's more, paying the ransom doesn't guarantee that your data hasn't been compromised or shared when under the adversary's control. The ramifications of a data breach to your employees, customers, partners, and/or reputation remain grave. A Ponemon study found that 65% of consumers whose data was breached lost trust in the company that experienced the breach.[11] In fact, paying the ransom doesn't even guarantee you'll get your data back. Of the 59% of SMEs who had paid the ransom in Capterra's survey, only 23% got all of their data back.[12]

– **Collateral damage from supply-chain attacks.** News sources don't always report on the trickle-down effect of large attacks; however, SMEs are often casualties in large supply-chain attacks, where an infection starts with a large corporation and spreads through the supply chain. Thus, large supply-chain attacks have ramifications on many of the target organization's partners, customers, or vendors. In REvil's attack on Kaseya's VSA software[13], for example, many of those impacted were SMEs that used the product; however, most headlines focused on the ramifications on Kaseya.

  In these cases, SMEs aren't direct targets but rather casualties resulting from a larger breach. Strong threat prevention and detection, in combination with ensuring your partners follow security best practices, are some of the best defense tactics.

– **Phishing and its variants.** Some of the most basic and low-effort tactics remain common — and effective — infiltration methods. Phishing remains one of the top three threats SMEs face[14], even despite increasing organizational awareness around it. The reason phishing is one of the most common threats is two-fold:

The Dangers of IT Sprawl

One of the key downfalls of a sprawling IT environment is its hampered ability to fully carry telemetry data from one element — and one security solution — to another. In environments with high tool sprawl and low visibility, lateral movement is hard to detect; weak integrations and incomplete telemetry shield adversaries' movement and often fail to alert teams of the breach. Adversaries know that SMEs often have sprawling infrastructures with visibility gaps, which makes them ideal targets. This stealthy lateral movement often lays the groundwork for an advanced persistent threat (APT).

- It is effective for adversaries. From the cybercriminal's point of view, phishing is relatively easy to deploy, and it often yields lucrative results. It takes few resources and minimal skill to launch phishing attacks, and yet it continues to dupe employees into sharing credentials, network access, and other sensitive (and, for cybercriminals, profitable) information and assets.
- It preys on human error. Unlike many other attack vectors that leverage vulnerabilities in systems, phishing uses social engineering to take advantage of human nature (and human error) to gain initial entry. While phishing training and awareness are increasing, it only takes one mistake to allow an attack to take hold. And in 2020, KnowBe4 found that the average organization had a 37.9% phishing test fail rate.[15]

Secure the C-Level

In cybercriminals' eyes, executives are a fast track to the sensitive data and assets they're looking for. Don't neglect executive security training, and make no exceptions — every executive should participate in security awareness training.

Cybercriminals have refined tactics to mount more targeted and precise phishing attacks. Spear-phishing, for example, involves background research to convincingly target individuals rather than bulk-sending an email to a group of recipients. This personalization and specific targeting makes spear-phishing attempts harder to spot.

A step further, whaling uses spear-phishing tactics to target company executives. Because executives have extensive access to systems and data, whaling is particularly popular — especially with SMEs, where scarce resources could hamper their ability to adequately train leaders on security and phishing awareness and best practices.

- **Software vulnerability exploits.**
  Leveraging software vulnerabilities is a common way to gain access into an organization's systems. Often, exploited vulnerabilities are known and even have patches available. In fact, many of the top exploited vulnerabilities were found years ago — for example, a Microsoft Office vulnerability found in 2017 continues to plague businesses that haven't kept up with their patches.[16] In a Ponemon survey, 60% of respondents who had experienced a breach said it could have occurred through a known vulnerability that had a patch available, but the organization hadn't applied it.[17]

  Routine patching is a critical basic cyber hygiene activity, and it is highly effective at blocking this type of attack. Native patching tools aren't enough to ensure devices are up to date; patch management software is the best way to reliably track and push out patches while easing IT's burden of tracking and implementing patches.
- **Account takeover.**
  As businesses move to the cloud and dispersed infrastructure becomes the norm, identity has increasingly come to define the new perimeter. Because identity permeates every element of the infrastructure, it has become a common infiltration point. In fact, the number of password-stealing attacks on SMEs around the world increased by almost 25% from 2021 to 2022[18], and nearly 80% of attacks leveraged identity to compromise credentials.[19]

  In account takeover (ATO) attacks, adversaries gain access to the network by taking over a user's account. Account access can be gained through various means, including password-stealing software, social engineering, and using (often by purchasing) the credentials of already-breached accounts. Once the adversary has taken over the account, they can access resources and move around the network under the guise of a legitimate user. This makes account takeovers difficult to detect.

Despite the prevalence and potency of cyber incidents today, the misconception that they don't affect SMEs is unfortunately fairly sweeping: In a 2022 CNBC survey, only 5% of small businesses named cybersecurity their top concern, and the 61% said they were not concerned about falling victim to a cybersecurity attack.[20]

Mounting a Strong ATO Defense

- Implement policies that strengthen passwords, like password rotation and complexity requirements.
- Challenge and limit users' sessions with multi-factor authentication (MFA), conditional access policies, and session timeouts.
- Conduct security awareness and best practices training to help prevent the credential theft that fuels ATOs.
- Use comprehensive detection tools to make sure teams are alerted to breaches right away.
- Start with strong identity security. Because ATOs target identities, the most effective defense is a strong identity strategy, ideally rooted in Zero Trust methodology. Zero Trust applies security at the identity layer, mandating that users should never be granted access before verifying their identity. Instead of allowing one login to grant access to all resources, Zero Trust continuously requires verification to help stop potential lateral movement.

This belief is built largely on the way cybersecurity incidents are reported. While just about everyone is aware of cybersecurity threats at some level, news stories tend to focus on the most dramatic and high-impact attacks, like enterprise-scale ransomware attacks and politically motivated breaches, which gives the impression that cybersecurity is a problem for only the largest, most prominent organizations. However, these large-scale incidents represent a fraction of attack vectors.

The misconception that SMEs are not affected by cyber crime contributes to SMEs' tendency to choose business over security: If the organization isn't threatened, why allocate resources toward protecting it? But the reality is that cyberattacks target and hit businesses of all sizes — including SMEs.

Advanced Persistent Threats

SMEs that work with large enterprises may be more likely to be susceptible to APTs, which are sophisticated attacks carried out stealthily over an extended period of time. APTs typically consist of infiltration, lateral movement toward targeted data or assets, and exfiltration. APTs can start from any ingress point and can enter through methods as simple as a phishing attack or stolen password.

For example, an adversary could gain the credentials of an employee with base-level permissions through a phishing scam, then take over the account to analyze the network and gather permissions, access and store the target data, and finally exfiltrate it to sell for profit.

Interoperable security tools are critical for detecting APTs and lateral movement by providing context and thorough detection across tools and platforms. In addition, some lightweight means of shoring up defenses against APTs and lateral movement include multi-factor authentication (MFA) and segmenting guest and employee networks.

SME Security Challenges

Defending against today's varied, frequent, and sophisticated attacks can be difficult for any organization. However, SMEs often face more frequent and complex challenges in mounting effective security defenses than their enterprise counterparts.

Typically, an SME's structure is vastly different from a large enterprise's, which usually has several thousand employees, generates at least nine-figure revenues, and works within an established bureaucracy and structured processes. SMEs, by contrast, typically have more limited resources and more fluid structures and processes. While these qualities make for flexibility and efficiency, they can also become barriers to implementing strong security.

One of the most challenging hurdles is also one of the most foundational: understanding how today's threat landscape affects SMEs. Unfortunately, SMEs often have less internal security expertise than enterprises, which can cause some to underestimate their risk. Thus, when faced with tough decisions, security doesn't always receive the investment it warrants. And because SMEs tend to work with lower headcounts, smaller margins, and more limited resources than enterprises, they are more frequently faced with the difficult task of prioritization. This only perpetuates the perceived dichotomy between security and business initiatives.

Without awareness of their high risk and the gravity of the security threats they face, SME leaders often underinvest in security. Even in cases where they do see the need for security, common internal challenges pose additional barriers. The following section focuses on the barriers SMEs face when it comes to implementing effective security. Fortunately, they are surmountable; the subsequent section will outline SME-friendly solutions for overcoming these challenges.

Lack of Familiarity with the Security Landscape

Because SMEs are generally lean, and IT and leadership aren't exempt from wearing many hats, it's rare for an SME to have multiple roles dedicated to security management and operations. In a 2021 study, 64% of respondents working at companies with fewer than 100 employees said they did not have a CISO, and 52% of companies with 100-5,000 employees noted that they also did not have a CISO.[21]

Moreover, SMEs may not have personnel on staff with an expert background in security (or the time to dedicate to mastering it sufficiently). A lack of comprehensive security experience may affect the team's ability to set up and manage tools effectively, which can create security and technology gaps that adversaries can exploit. Further, without this expertise to guide security decisions, teams often underestimate the risk and severity of today's threats while overestimating the efficacy of their current defenses. A Datto study found that while only 30% of respondents in a MSP poll said their SME clients were "very concerned" about cybersecurity, 84% of the respondents said they should be.[22]

Security Implications

- **SMEs underestimate their security needs.** Because many SME leaders aren't aware of the threats they face and their severity, they sometimes overestimate the effectiveness of their current security measures. Many assume that baseline security measures, like antivirus software and firewalls, are enough to block attacks. While they do block some, they are not effective on their own: Nearly three-quarters of hackers say traditional firewalls and antivirus software are obsolete.[23]

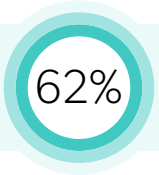
However, minimal security measures continue to instill a disproportionate amount of confidence in SME leaders. CNBC's survey found that 62% of small business owners feel confident they could quickly respond to a cybersecurity attack, while only about a third (34%) said they had any kind of incident response plan in place.[24]

– **Security is defined by compliance.**
When SMEs take steps toward security, they often use compliance regulations to determine what security they need. While meeting compliance standards is an important baseline, it should be treated as such: a baseline.

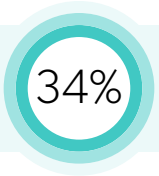
Compliance regulations may only define minimum acceptable requirements and are not tailored to specific businesses or threats. While compliance may help businesses form basic defenses, it isn't as effective in helping companies defend against or respond to new and emerging threats that target them. Generally, meeting compliance standards isn't enough to achieve reliable security.

Security programs developed solely based on compliance regulations tend to be fairly surface-level and lack strategy. All too often, compliance requirements become a checklist, and organizations try to meet each requirement as simply and cost-effectively as possible. However, this can result in a piecemeal approach where elements don't work well together, and poor interoperability creates its own set of security gaps and blind spots.

Anecdotally, many cyber insurance plans now seem to require more advanced and comprehensive security measures, like MFA and endpoint detection and response (EDR), in addition to more basic protections, like antivirus software, which has been a common baseline requirement in past years. SMEs that want cyber insurance often look to meet the MFA, EDR, and more advanced requirements quickly and cost-efficiently. However, purchasing solutions without considering how they will fit strategically within the existing IT environment can contribute to **IT sprawl** — a source of vulnerability and risk — without significantly improving security.



62% of small business owners feel confident they could quickly respond to a cybersecurity attack.



34% said they have an incident response plan in place.

Keep an Eye on Compliance Changes

As threats become more sophisticated and security concerns grow, organizations are likely to strengthen their compliance requirements for working with other vendors. You may start to see companies requiring more stringent compliance from their vendors and partners to help secure the supply chain.

Resource Limitations

As outlined in the previous section, SMEs' resource limitations can make them attractive and impactful targets to cybercriminals. Unfortunately, the same resource limitations also make it harder for SMEs to implement the proactive security required to protect against these attacks.

Limited resources require SMEs to make tough choices, further contributing to the perception that security and business are at odds with one another. When SMEs can't afford to invest heavily in every important initiative, they are forced to choose one over the other. The misconception that SMEs are not targets, combined with the lack of specialized security expertise in many SMEs, drives many to invest their limited resources in business initiatives rather than security ones. Over time, this tends to introduce blind spots in their security controls and weaken their defenses, which makes them an even more attractive target.

In addition, this decision-making approach sometimes extends to hiring and equipping IT teams: Allocating resources to business-driving initiatives can leave IT departments spread thin. This further compounds upon security risks and makes threat response even more difficult.

Security Implications

- **Security becomes "pick and choose."**
  When limited resources make it difficult to get funding allocated to security, SMEs must be highly selective about which security solutions they invest in. Often, this can make leaders feel they must pick and choose from among necessary security items, investing in some while passing up others. Many SMEs, therefore, end up with certain baseline measures in place, like antivirus software, but without more robust and comprehensive protections, like threat intelligence and identity-based security.

  Additionally, sporadically purchased tools often don't work well together. However, interoperability and comprehensiveness are critical to reliable security; baseline security measures that work in isolation from one another will do little to protect an organization.
- **IT teams are overloaded.**
  SME IT teams usually have fairly heavy workloads, and most IT professionals are responsible for a range of functions. And just as SMEs move and change quickly, their employees must also be willing to work in a fast-paced environment and be ready to adapt to change.

  While this creates efficiency, it can also lead to oversights. For example, overloaded IT teams may not have the time to communicate effectively with one another or document their processes, leading to confusion, lack of transparency, and tasks falling through the cracks. When working with the dispersed infrastructures common in SMEs, overloaded teams tend to lose comprehensive visibility over their environment, which opens up security gaps. Oversights and inefficiencies like these increase risk to the organization that can lead to future security breaches.
- **Mac and Linux security are left behind.**
  Windows has been the primary workplace OS for decades, and many legacy vendors tend to cater to this trend by tailoring their products more heavily toward Windows. Security products are no exception — in fact, macOS's and Linux's reputation for superior security has only exacerbated this trend. The combination of Windows' longstanding popularity, vendors' increased attention given to Windows, and Mac and Linux devices' perceived ability to fend off attacks on their own may drive many SMEs to de-prioritize Mac and Linux security when it comes time to make tough budgeting choices.

  However, workplace devices are diversifying, and now Windows devices make up only 68% of the devices at the average SME, with Macs accounting for about 21%, according to a JumpCloud survey.[25] While Mac and Linux devices do have some viable security protections built in, they are not enough to stop the frequent and sophisticated attacks SMEs face today.

IT Sprawl

IT sprawl is common in SMEs; pressured to solve problems and make decisions quickly, teams often have to make tool decisions with immediate solutions in mind rather than big-picture strategy. While this ad hoc purchasing approach is natural in growing SMEs, it often leads to teams unknowingly duplicating features across tools and paying for both. It also removes architecture strategy from the purchasing process, which can create environments where tools don't work well together. As this effect grows, integrations become weaker and dependencies become more complex, which makes change difficult and complications frequent.

IT sprawl has implications for the entire organization, from resource allocation efficiency to negative employee experiences. And disjointed IT means disjointed security.

Security Implications

- **Visibility is restricted.**
  Tools that don't integrate well with one another can't effectively report on things as a whole; telemetry sourced from several different tools fails to provide comprehensive accounts of infrastructure activity. This hampers systems' abilities to detect intrusion. Even advanced attacks like ransomware can enter via just about any ingress point, from leveraging stolen credentials to entering through a phishing scam. When narrow-scope tools can only report on activity within certain portions of the infrastructure, they leave blind spots that may allow for undetected intrusion.

  Further, the more tools in an infrastructure, the more likely friction will develop. For IT, pulling data from several different tools rather than one pane of glass is time-consuming and error-prone. And when tools aren't designed to work together with native or pre-built integrations, they're prone to breakage, faulty intercommunication, and blind spots.

  In addition, visibility gaps impact an SME's ability to spot and address shadow IT as it arises. Unaddressed shadow resources are significant sources of vulnerability, as they often facilitate resource access or store company data without adhering to company best practices or regulations.

What Is Shadow IT?

Shadow IT is essentially any non-sanctioned IT activity initiated by non-IT personnel. It often arises from good intentions — e.g., an employee creating a free account with a non-vetted tool to increase their productivity — but if IT can't see or manage it, IT can't protect it. Shadow IT is common, especially in fast-moving teams, but it poses serious security risks.

Learn more about shadow IT risk and management ⇒

- **Gaps in communication arise.**
  Without comprehensive reporting and clear security resource allocation, it becomes difficult to track who has done what. This can lead to oversights — for example, people may assume that someone else addressed an alert, may mistakenly believe that someone else implemented certain policies, or may lack a documentation process to report on past incidents and responses. Aside from the danger these oversights pose from potentially missing security activity and threats, they also present challenges for managing and troubleshooting the infrastructure over time.
- **Endpoint security is fragmented.**
  Often, cloud security is treated as a separate function from endpoint security: For example, SMEs might invest in endpoint detection that applies to devices but doesn't extend to cloud servers and workloads. But servers and appliances can be managed like endpoints, and can be just as in need of protection as computers and mobile devices (see CrowdStrike's list of endpoint types). Securing endpoints with separate solutions creates visibility and control gaps among the security tools, which can lead to a failure to detect suspicious activity and alert to critical threats.
- **Alert fatigue is real.**
  Working with a multitude of IT and security tools can create substantial noise, and managing all their alerting and reporting capabilities can be a substantial challenge for IT and security teams. The lack of integration, correlation and relevant contextual information often results in an overwhelming number of false positive alerts for activity such as basic user log-ins or routine software updates. IT teams naturally learn to tune these out, which can cause true alerts to slip by unnoticed.

Trying to juggle business and security functions in a sprawling environment only perpetuates the dichotomy between the two: How can SMEs power both with so many tools to support and manage? Counteracting this clutter helps SMEs recenter around a more strategic, streamlined, and efficient environment that can power both security and business, simultaneously and cost-efficiency.

Power Business and Security with IT-Security Unification

Contrary to popular belief, SMEs face very real and dangerous security threats. The wide range of these evolving threats can make enterprise-level security seem like the only option. However, SMEs can rarely afford their direct costs, not to mention adding the burden of learning and managing them to IT's already-overwhelming daily workload. This leaves them faced with the decision to drive security progress or drive business progress, and SMEs are often pressured to choose business.

What's more, when SMEs do invest in security, adding layer upon layer of solutions only exacerbates the common point-solution problem SMEs face. Additional security solutions haphazardly tacked onto an existing architecture limit visibility with complex, sometimes brittle integrations and bog down the user experience with non-intuitive processes.

Rather than approaching security with a "more is more" mindset, SMEs need to refocus on the basics. Those basics start with IT and security unification.

99.9% of Account Compromise attacks can be blocked with MFA.

IT-security unification provides a strong foundation of highly effective tools like MFA.[26]

Unifying IT and security breaks down sprawl and establishes a clear, functional, and efficient base layer of the IT infrastructure that needs to be secured. This unified and transparent infrastructure forms a strong foundation for incorporating and integrating the right security tools for the environment. When unifying their IT and security, many SMEs only need to add a minimal number of tools and can eliminate others where capabilities overlap. They also tend to derive more value from their previously existing solutions.

Further, IT-security unification eliminates the vulnerabilities, high costs, and burdensome workloads generated by disjointed IT and security, ultimately creating an architecture where IT and security tools work together seamlessly. It empowers IT and security teams and helps SMEs achieve a more strategic, cost-efficient stack that:

- Reduces complexity, which makes the stack more flexible and manageable.
- Offers better controls for easier configuration and management.
- Improves visibility and context, allowing teams to detect and respond to alerts faster.
- Reduces alert fatigue, which improves productivity and threat response efforts.
- Allows teams to spend more time on business-driving tasks without sacrificing security.

Because it's affordable, manageable, and effective, IT-security unification is the best action SMEs can take to affordably shore up their defenses.

Achieving IT-Security Unification

Unification occurs in four main steps, detailed above. These steps help you determine what to include in your environment and how elements will communicate with one another. Ultimately, the process of unification helps SMEs achieve a streamlined, cost-effective, and secure environment that drives productivity without hindering performance.

Where to Begin

If you already have foundational security controls in place and generally understand what your organization needs in terms of security, it can be beneficial to unify both IT and security at once. With this approach, consider the core tools you need for both your IT and your security stacks, and then incorporate, integrate, and consolidate them as one unit. This helps keep IT and security fully unified throughout the process.

However, if you're newer to security and don't have many security tools or processes established yet, consider following this process with your IT infrastructure first, and then move on to follow the same steps with your security tools. This process will help you gain a clear understanding of your infrastructure as well as your security needs and gaps before making decisions about your security tools. This approach will help you form a strong foundation upon which to build your security strategy and infrastructure.

Regardless of which approach you take, be sure to prioritize tool functionality and interoperability as you identify, incorporate, and integrate your core tools. Choosing technology that can accomplish your needs and scale with your organization as it grows is critical. Aside from core functionality, thorough and streamlined intercommunication among tools is the most critical component of a reliable IT-security infrastructure.

How to Prioritize

Most SMEs don't tackle all of these steps at once. Prioritize by focusing on the most impactful capabilities that materially help you reduce risk first. These can be simple things like patching systems, encrypting disks, and implementing MFA to add a layer of security and resilience to attacks using tools you already have.

1. **Identify.**

   In this step, you identify the core of your infrastructure. The core is the solution or group of solutions that creates a foundation for the rest of your architecture. For example, because identity dictates access throughout your infrastructure, an identity management solution or directory is likely to be part of your core. Similarly, because end users must use some type of device to get their work done, your core will also likely include an endpoint protection solution.

   In this stage, focus on the following critical facets of tool suitability.

   - **Meets criteria.** First and foremost, the tools you choose should be able to collectively accomplish everything you need your stack to do.
   - **Compatibility.** Make sure the tools you choose can communicate smoothly with one another. The best way to ensure this is through native or pre-built integrations and open APIs. Try to choose tools that already offer pre-built integrations with the other tools in your stack; avoid those that won't easily integrate with one another.
   - **Ease of support.** Make sure your IT and security team will be able to support the core solutions you choose. This includes ongoing maintenance, operations, and management. If you plan to hire outside support for certain tools, factor this into your budget and operating model. CrowdStrike Falcon Complete™, for example, takes the burden of both detecting and responding to threats off your team's plate by offering managed detection and response from a team of security experts.

2. Incorporate.

Incorporate the core solutions you've identified into your stack. This includes acquiring new solutions, implementing them, and configuring them to meet your needs.

3. Integrate.

Integrate the core solutions with the rest of the tools in your infrastructure. Because pre-built and native integrations are critical to maintaining a secure and transparent environment, knowing which integrations you'll need in steps one and two can help you choose compatible elements for your core.

4. Consolidate.

Finally, consolidation involves taking stock of your stack and looking for places where you may be able to eliminate excess. Look for instances where your core products can take on the work of another tool, where features are duplicated or where certain capabilities are no longer necessary.

Unified Security

With a unified stack, you will be able to build a security program that is reliable, manageable, and comprehensive. Your security program should include:

- **Endpoint, workload, identity, and data security.** Your security should span your endpoints, workloads, identity, and data with both detection and remediation.
  - **Detection and remediation.** Threat detection is critically important — but it's only half the story. Often, SMEs invest in threat detection technology without also investing in the means to respond to detected threats. This setup is not much more useful than having no threat detection at all. SMEs need to be able to both detect threats and respond to them quickly and reliably.

    This should be accomplished through strong native or pre-built integrations; detection and response tools that are designed to work together will deliver the comprehensive security, visibility, and control IT teams need to manage their security holistically and reliably.
  - **One tool to address all endpoints.** Security cannot be unified if SMEs treat different endpoints with different security methods and tools. While a step up from no security at all, this approach still breaks security into discrete parts. Just like point solutions in a sprawling IT environment, this obfuscates visibility, generates friction for IT, and may fail to detect or alert to threats.

    The same goes for Mac security. All endpoints must be protected, regardless of their OS — and ideally, they should all be protected with the same security tools and measures. Otherwise, the same interoperability issues tend to arise. Look for security solutions that work for all of the operating systems in your environment.

> "In distributed, cloud-based, or hybrid environments, all endpoints and workloads should be protected, and that protection should be comprehensive and well-integrated throughout the infrastructure.

- **Security at the identity level.** As identity becomes the new perimeter in distributed environments, SMEs must address security at the identity level. Ideally, this security should be achieved with a Zero Trust strategy, where no access is granted without verification.

  Instead of allowing full, sustained access to all resources once someone is admitted into the network, Zero Trust prescribes continuous, secure authentication. This is critical to reducing the possibility of attack as well as reducing damage if one were to occur by limiting the possibility of lateral movement. MFA, single sign-on (SSO), and conditional access policies are key tools that support Zero Trust security.

- **A well-integrated stack.**
  Tool interoperability is critical to security: It keeps visibility clear, eases management, ensures activity is trackable as it moves through the network, and keeps security alerts reliable. Native and pre-built integrations are always the better choice when it comes to integrating tools — while custom ones can work, they are often difficult to change and cannot guarantee full visibility among tools.
- **Smooth operations.**
  Interoperability shouldn't stop at tooling. Your IT and security operations should be just as streamlined and clear: Communications among IT personnel must be transparent, and duties must be clearly defined. Every member of the IT team should understand what items fall under their responsibility and who is responsible for other duties, and should keep clear records of their activity.
- **Comprehensiveness.**
  While endpoint and identity security is critical, comprehensive security includes network security, 24/7 monitoring to complement automatic monitoring and alert systems, regulation and compliance monitoring, and more. Often, comprehensive security falls outside the scope of an SME's resources — hiring a dedicated security professional or outsourcing security to a managed service can yield significant ROI for SMEs working with limited resources.

Do You Need Managed Security?

"Analysis of the breakout time for hands-on eCrime intrusion activity over 2021 — where such a metric could be derived — revealed an average of just 1 hour 38 minutes."
– Crowdstrike 2022 Global Threat Report

If you can't begin response in minutes and remediate threats in less than one hour, partnering with a 24/7 managed security service is your best option for reliable protection.

- **Cost efficiency.**
  Security programs must account for budget; a plan that ignores resource constraints cannot be enforceable or effective over time. Look for tools and configurations that are efficient and optimize resources to ensure your security program will be effective over time.

To illustrate the power of IT-security unification, consider the pre-built integration between JumpCloud and CrowdStrike: JumpCloud, an open directory platform, partners with CrowdStrike, one of the cybersecurity leaders in protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. The combination of the two enhances visibility, response, controls, and end-to-end protection without increased resource burden. Here's how it works.

Integrating JumpCloud and CrowdStrike

JumpCloud is a cloud directory platform that offers many of the key elements required for a secure, comprehensive core, including:

- Identity and access management (IAM)
- Device management with patch management, disk encryption, and MDM capabilities
- Single sign-on (SSO)
- Privileged access management and conditional access policies

Because it offers several solutions typically sourced from different vendors, the JumpCloud platform is an ideal piece of the core infrastructure in a unified environment. It unifies device and identity management, tying security and access measures to holistic user and device telemetry.

This unification permeates throughout the infrastructure, offering SSO and access management to all of the resources users need to work as well as comprehensive MDM, with the ability to enable full disk encryption, remotely lock and wipe devices, and create device-contingent conditional access policies. Further, JumpCloud is compatible with Mac, Windows, and Linux management, which prevents the need for separate Mac management tools.

This holistic unification enables a significant amount of consolidation by replacing several point solutions and their many custom integrations with native ones.

JumpCloud has nearly 1,000 pre-built integrations with partner vendors that can help round out your core infrastructure. It integrates with the CrowdStrike Falcon® platform's endpoint detection and response solution to wrap robust EDR into the infrastructure core.
The CrowdStrike Falcon platform, powered by the CrowdStrike Security Cloud and world-class AI, leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft, and enriched telemetry from across the organization.

When integrated with JumpCloud, companies get the benefit of CrowdStrike Falcon Real Time Response (RTR) on their managed endpoints, and can leverage intelligence and capabilities from both platforms from a single console. Hyper-accurate reporting and alerts, combined with intricate policy creation and OS-agnostic MDM capabilities including patch management, allow IT to immediately and effectively respond to threats. The ability to create policies like enabling full disk encryption on devices helps with threat prevention, increasing the comprehensiveness of the integration.

For example, if the CrowdStrike Falcon platform detected a threat on an employee's smartphone, it could immediately alert the IT and security team, who could use JumpCloud to access device logs and diagnostics and respond to the threat by remotely quarantining, locking, or wiping the device in question. IT could administer the entire process through the Falcon interface without sacrificing the security of pre-built and native integrations.

The JumpCloud-CrowdStrike integration not only eases security, it also streamlines compliance. Clear visibility into your entire infrastructure at once in combination with thorough and reliable detection methods help SMEs more easily comply with compliance standards. Further, both JumpCloud and CrowdStrike support Zero Trust security, prioritizing security at the identity level and the tools required to enforce continuous verification before authorization (like MFA and conditional access policies). Ultimately, the two products deliver streamlined security that empowers teams and drives business forward.

To learn more about the JumpCloud-CrowdStrike integration, visit **our overview**.

1 Zendesk - Big Expectations, Small Businesses: What Customers Want

2 AdvisorSmith - Small Business Cybersecurity Statistics

3 Hiscox - Cyber Readiness Report 2022

4 Datto - Global State of the Channel Ransomware Report

5 https://jumpcloud.com/resources/sme-trends-security

6 New York Times - As Understanding of Russian Hacking Grows, So Does Alarm

7 JumpCloud - Creating a New Normal for SMEs in 2022

8 CrowdStrike - Ransomware Realities for SMBs

9 Backblaze - The True Cost of Ransomware

10 Capterra - How Prepared Are SMEs for Ransomware Attacks?

11 Centrify|Ponemon - The Impact of Data Breaches on Reputation & Share Value

12 Capterra - How Prepared Are SMEs for Ransomware Attacks?

13 CSO Online - The Kaseya Ransomware Attack Timeline

14 CrowdStrike - Ransomware Realities for SMBs

15 KnowBe4 - New KnowBe4 Benchmarking Report Finds 37.9% of Untrained End Users Will Fail a Phishing Test

16 CISA - Top Routinely Exploited Vulnerabilities

17 Ponemon - Costs and Consequences of Gaps in Vulnerability Response

18 Kaspersky - Small Businesses Are Still in Danger, Facing an Increasing Number of Attacks in 2022

19 CrowdStrike - 2022 Global Threat Report

20 CNBC|SurveyMonkey - Small Business Index Q2 2022

21 Navisite - The State of Cybersecurity Leadership and Readiness Report

22 Datto - Global State of the Channel Ransomware Report

23 https://thycotic.com/resources/black-hat%20%20-2017-survey/

24 ibid.

25 JumpCloud - Creating a New Normal for SME IT in 2022

26 Microsoft - One Simple Action You Can Take to Prevent 99.9% of Attacks on Your Accounts