illumio

The Cybersecurity Survival Guide

Why cyberattacks target small and midsized businesses — and how Zero Trust can help

Contents

Small IT teams. Big ransomware targets.

In April 2024, a small but powerful player in the Australian property valuation industry suffered a ransomware attack that would change its operations, reputation, and future forever.

The BlackSuit ransomware gang wasted no time, leaking nearly 300GB of stolen data — customer records, transaction databases, and more — on their darknet site. The ransom amount is still a mystery. But the fallout was immediate: Australia's big four banks hit pause on valuation work with the firm.

This is yet another incident in the growing wave of ransomware attacks targeting small and midsize businesses (SMBs) globally.

And it's only a matter of time before the next attack.

SMBs can't afford to ignore cybersecurity

BlackSuit's SMB target shows an important fact: Cybercriminals don't just go after big companies. In the last year, 75% of all cyber incidents hit SMBs, and 90% of those attacks stole data and credentials.[1] Ransomware was the biggest threat.

SMBs are becoming popular targets because they often don't have the same level of protection as larger companies. A ransomware attack can seriously damage — or even shut down — a business with fewer resources.

In 2024, the average data breach cost for SMBs reached $2.64 million.[2] This highlights the severe financial strain cyberattacks place on smaller enterprises.

How this guide can help

This guide is here to help SMBs with simple, effective strategies to protect against ransomware and other cyberattacks. By using basic security ideas such as Zero Trust and tools such as microsegmentation, even smaller enterprises can defend themselves against modern cyber threats.

75%

The percentage of cyber incidents that targeted SMBs in the last year

70%

The percentage of SMB cyber incidents that were from ransomware

$2.64M

The average cost of an SMB data breach

[1] Sophos 2024 Threat Report
[2] IBM Cost of a Data Breach Report 2024

Understanding today's SMB cyber risk

The threat landscape is no longer about *if* an attack will happen but *when*.

Understanding the realities of today's threat landscape is the first step to protecting your business.

The top threats facing SMBs

SMBs are no longer flying under the radar — they're prime targets for cybercriminals. Let's break down the top threats SMBs face and why it's crucial to stay ahead of them.

Ransomware

A particularly devastating form of attack, ransomware encrypts data and holds it hostage until a ransom is paid. For SMBs, ransomware is the most common threat. Paying ransoms can be a last resort — but a financially crippling one.

Disruption attacks

By targeting critical systems, networks, or data, attackers can paralyze operations. These attacks, including denial-of-service (DoS) attacks, aim to halt workflows, interrupt service delivery, and sow chaos. For SMBs, they strain limited resources and jeopardize survival.

Supply chain attacks

When a vendor or supplier is breached, attackers use that connection to infiltrate SMBs. This makes SMBs vulnerable even if their own defenses are sound.

Why SMBs are attackers' favorite targets

Cybercriminals see SMBs as low-hanging fruit: quick, profitable, and less likely to fight back. In today's cyber landscape, being small doesn't mean being safe. Here are the main reasons SMBs are attackers' favorite targets.

Lean IT budgets and teams

Cybercriminals know SMBs are less likely to have sophisticated defenses, making them easier targets. SMBs often don't have the budget for advanced cybersecurity tools. Small teams lack dedicated security roles and expertise. Many struggle to monitor and respond to the growing number of threats.

Outdated technology and strategies

At the same time, many SMBs are missing core security tools such as security information and event management (SIEM) frameworks, intrusion detection tools, and next-generation firewalls (NGFWs). And in some cases, SMBs haven't even taken the steps to deploy simple security measures such as two-factor authentication, which help frustrate common threats.

Beyond outdated security, SMBs also often rely on legacy systems. Many of them no longer get critical security updates and often have vulnerabilities cybercriminals can exploit.

Less cybersecurity awareness

Most larger businesses conduct some kind of company-wide security training. But SMBs often lack the resources to do the same, leaving them more vulnerable to attacks. Compounding the issue, many SMBs don't even see themselves as targets, leading to a dangerous complacency around cybersecurity.

High value-to-effort ratio

Cybercriminals view SMBs as easy targets because their networks are often easier to breach with minimal effort. Despite the lower effort needed, gaining access to critical data can yield rewards comparable to more complex and time-consuming attacks.

And even if the ransomware payout isn't much — tens of thousands compared to possible millions in the case of enterprises — the bar is so low that the effort is worth the earnings. Often, they can breach multiple SMBs in the time it takes to breach one large enterprise.

Less chance of getting caught

Many SMBs don't have strong security, giving attackers more time to move through their networks. This can lead to long delays between an attack starting and being detected. Attackers can use this long dwell times to move laterally through the environment without being noticed. They can watch user activity and pick the perfect moment to strike.

Regulatory and compliance pressures

Regulations such as GDPR, HIPAA, DORA, and other industry rules require businesses to protect data, ensure privacy, and stay resilient.

Breaking these rules can lead to major fines. But for SMBs, it's not just about avoiding penalties. Compliance is key to staying up to date and earning the trust of customers and partners.

For SMBs, investing in cybersecurity can yield tangible returns. They can improve their reputation, lower the risk of legal problems, and even land bigger contracts and partnerships. If a ransomware attack happens, having a track record of following these rules can help reduce the damage, rebuild trust, and avoid further penalties.

SMB cybersecurity: Myth vs. reality

MYTH	REALITY
Cybercriminals focus only on large enterprises that have a lot of money and data to steal.	SMBs are common targets because they often have weaker defenses than large companies. Smaller networks are usually less complex and require fewer resources to attack. For cybercriminals, hitting several smaller businesses for a big reward is easier than spending the same effort on a single, well-protected company.
The endpoint detection and response (EDR) tool and firewall we've been using for decades have protected us so far. They'll continue to work in the future.	While EDRs and firewalls are important, modern cyberattacks have outgrown these traditional tools. Today's security needs a layered approach. Breaches will happen, so it's critical to not only reduce the chances of an attack but also minimize its impact when it does occur.
Today's cybersecurity tools are too complex for a company our size to manage.	Many modern security tools are designed to be simple and user-friendly, even for SMBs with small IT teams. Managed security providers (MSPs) can also help SMBs stay protected without spending too much or needing advanced technical skills.
The security features that come with our systems and apps are enough for a business our size.	Many platforms offer basic security, but it usually only protects the infrastructure. Contractually, businesses are responsible for securing their own data and access settings. Attackers can exploit weak user settings to get around built-in protections.

From risk to resilience: Zero Trust security for SMBs

Flat networks are a malicious actor's dream. Once they breach your perimeter and compromise one device, they can spread like wildfire across your entire network.

It's a race against time before they reach your critical resources. And with GenAI-powered attacks, they're moving faster than your detection tools can keep up.

Prevention and detection tools are crucial, but they're not enough. Breaches are inevitable.

The key to staying resilient? A Zero Trust security strategy.

What is Zero Trust?

In the early 2010s, then-Forrester analyst John Kindervag introduced the Zero Trust security model to challenge the outdated concept of implicit trust in network design.

Traditional networks build strong perimeter defenses. But they trust anything inside the perimeter — a fatal flaw. Once attackers breach the perimeter, they can roam freely, accessing critical systems and causing widespread damage.

Zero Trust eliminates trust inside and outside the network altogether. It replaces implicit trust with granular security controls that stop breaches from being successful.

How Zero Trust transforms SMB security

Zero Trust offers a practical, scalable security framework to protect critical systems, reduce cyber risk, and build resilience against ransomware attacks.

With Zero Trust, SMBs can:

Reduce the attack surface

Zero Trust enforces strict, granular controls that significantly reduce the chance of unauthorized access and lateral movement. It offers a consistent, cohesive strategy for every part of your network, from cloud to on-premises data centers and endpoint devices.

Build cyber resilience

By getting rid of implicit trust, Zero Trust stops and contains breaches before they can spread through the network. This means a small security incident doesn't become a catastrophic attack. Cyber resilience is crucial for SMBs with limited IT resources because it strengthens their security posture without requiring extensive infrastructure.

Lower recovery costs

Since Zero Trust limits attackers' access to critical systems and sensitive data, any breach that does happen impacts fewer assets. This containment reduces both the scope and cost of recovery. It lowers downtime, data loss, and the overall financial impact of a breach. For SMBs, this translates to faster recovery times and reduced costs for incident response which can be crucial for keeping your business up and running during an attack.

Streamline compliance

Zero Trust aligns with the key requirements of many security regulations, including PCI-DSS, HIPAA, GDPR, and DORA. By adopting Zero Trust, SMBs can more easily meet these regulatory requirements while building a better security posture.

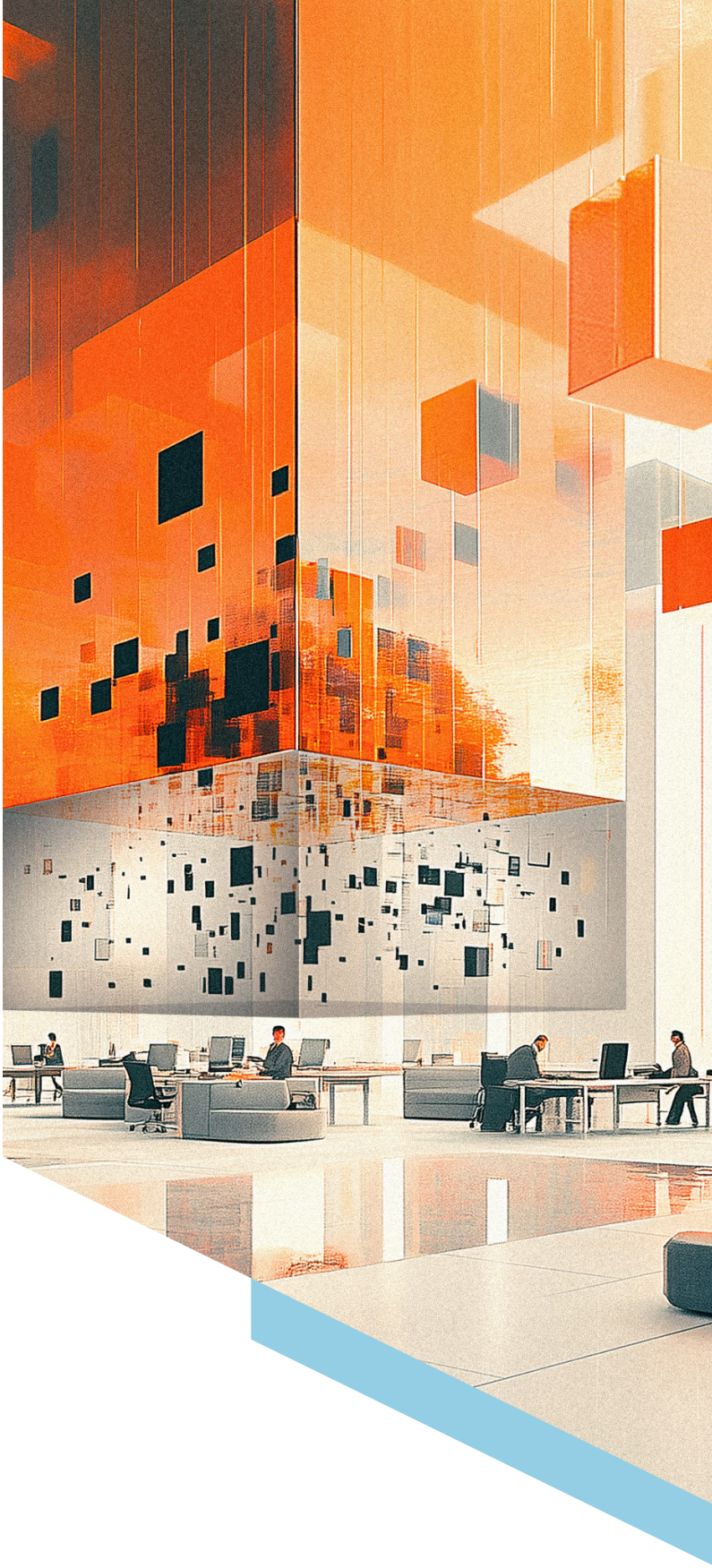
Zero Trust is a journey, not a destination

Implementing Zero Trust may sound daunting, especially if you have a small IT team. But experts recommend taking a phased approach to Zero Trust. This makes changes easier to manage and helps you get quick wins early in the process.

Remember, Zero Trust isn't a destination. It's a journey. It's an ongoing effort that your team will always been adding to and improving over time.

Kindervag encourages organizations to follow his five-step process for building Zero Trust:

1. **Define your protect surface:** You can't control the attack surface because it's always evolving. But you can shrink your organization's protect surface into small, easily known parts. The protect surface usually includes a single data element, service, or asset.
2. **Map communication and traffic flows:** You can't protect the system without understanding how it works. Getting visibility into your environment shows where you need controls.
3. **Architect the Zero Trust environment:** Once you get complete visibility into the network, you can start adding security controls that are tailor-made for each protect surface.
4. **Create Zero Trust security policies:** Build policies that provide a granular rule allowing traffic to access the resource in the protect surface.
5. **Monitor and maintain the network:** Inject telemetry back into the network, building a feedback loop that continuously improves security and builds a resilient, anti-fragile system.



Microsegmentation: The foundation of Zero Trust

Kindervag has advocated for segmentation to be part of every Zero Trust strategy for years.

In the second report on Zero Trust ever written, *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*, he recognizes segmentation and centralized management as key components of Zero Trust:

> New ways of segmenting networks must be created because all future networks need to be segmented by default.[3]

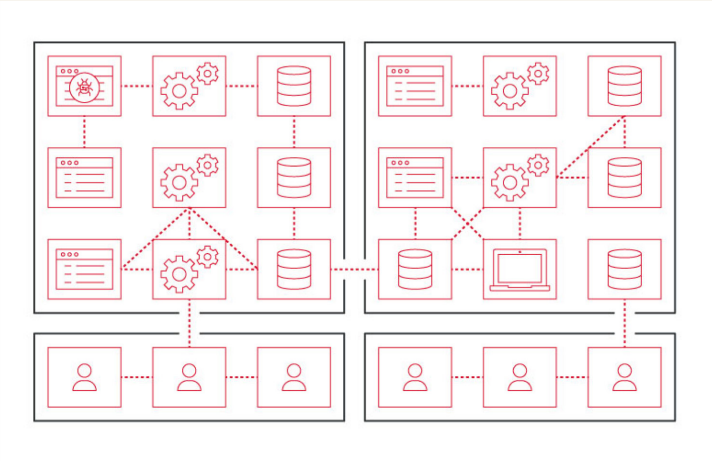
Microsegmentation is becoming the segmentation technology of choice.

What is microsegmentation?

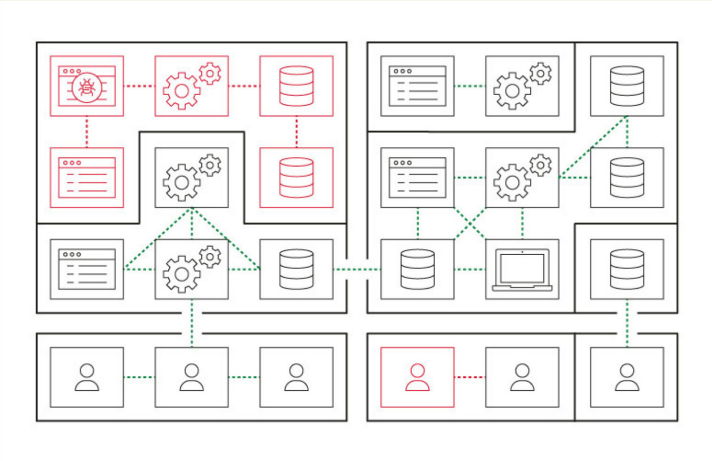
Microsegmentation is a highly granular form of segmentation. It secures individual resources by separating them into secure zones.

With microsegmentation, you can quickly and easily create segments based on things like function, location, or environment. For example, you can separate production from test environments or keep certain apps secure no matter where they are.

Microsegmentation also helps you respond faster to security incidents. This reduces the chances of disrupting business operations.



WITHOUT MICROSEGMENTATION



WITH MICROSEGMENTATION

[3] Build Security Into Your Network's DNA: The Zero Trust Network Architecture

Why SMBs need microsegmentation

SMBs can't afford to take chances with cybersecurity. One breach can bring your operations to a standstill and cost more than you can recover.

Microsegmentation is the ultimate safety net. It contains breaches so you can keep your business running. For SMBs, it's a practical way to build resilience in an unpredictable threat landscape.

Here's why microsegmentation should be a top priority for your business.

Reduce ransomware spread and impact

Microsegmentation stops ransomware from spreading across the network. This is called lateral movement. It keeps the ransomware contained at its entry point which helps prevent a total network shutdown.

For example, microsegmentation can block common attack methods like Remote Desktop Protocol (RDP). This makes it harder for attackers to move ransomware to other parts of the network.

Achieve compliance requirements and frameworks

Microsegmentation helps organizations isolate specific systems or data, like customer information or financial records, that need to follow regulations. Because fewer systems need to meet strict security standards, following compliance requirements is easier and less expensive.

Microsegmentation also aligns with security guidelines such as the NIST Cybersecurity Framework and CIS Critical Security Controls. Though these frameworks are different, they all include microsegmentation as a key security tool.

Simplify security for lean IT teams

Microsegmentation can help automate Zero Trust security, lightening the load for small IT teams. It can automatically adjust security controls and contain breaches. This helps busy IT teams feel confident that the business can keep running, even when a breach happens.

Speed up incident response and recovery

When an incident occurs, microsegmentation allows SMBs to isolate compromised systems quickly, containing the breach and minimizing downtime. This can save time and resources that would otherwise be spent restoring systems and recovering from a larger attack.

Lower security expenses

Robust microsegmentation platforms let you combine several tools into one. By reducing the number of security platforms you need, microsegmentation can make it simpler for security teams — and the whole organization — to work together and access the data and resources they need.

Checklist:
What to look for in a microsegmentation platform

- ☐ **Simple policy setup and management:** A good microsegmentation platform should be simple to use, with an easy-to-navigate design that makes setting up policies quick and straightforward. Ready-made templates or recommendations should be available to help you get started confidently.
- ☐ **Granular visibility and mapping:** The platform should provide clear insights into network traffic and application connections. Visual maps are important for creating the right security policies and understanding how traffic moves across your network.
- ☐ **Low impact on network performance:** Choose a platform designed to operate with minimal latency, allowing business operations to continue smoothly. It should also secure the network without compromising overall performance.
- ☐ **Flexibility for any environment:** A platform should function well in on-premises, hybrid, or multi-cloud setups. It should also work with major cloud providers to keep security consistent no matter where your systems are.
- ☐ **Policy testing to avoid interruptions:** The platform should include a "simulation mode" that lets you test policies before making them active. This helps catch problems early and keeps your network running without interruptions.
- ☐ **Quick time to value:** Pick a platform that delivers fast results. With built-in automation and insights, it should help you find weak spots and protect critical assets in just a few hours.
- ☐ **Scalable for growth:** Choose a platform that can grow with your business. It should handle more work and adapt to new environments without losing performance or security.

Thrive without fear of compromise

Breaches and ransomware attacks will happen. It's only a matter of time. But with the right strategies in place, you don't have to be an easy target.

Building a robust Zero Trust strategy grounded in microsegmentation isn't out of reach for SMBs. It's possible to meet cybersecurity best practices without overwhelming limited budgets or small IT teams.

You're not just defending against attacks. You're building resilience, showing clients and partners that your business is secure and reliable.

Don't wait until you're the next victim. Take control of your cybersecurity now and secure your business's future.

Cyber incidents are inevitable. But they don't have to be disasters.

Contain the breach with Illumio Zero Trust Segmentation.

Visit illumio.com/solutions/smb

About Illumio

Illumio, the most comprehensive Zero Trust solution for ransomware and breach containment, protects organizations from cyber disasters and enables operational resilience without complexity. By visualizing traffic flows and automatically setting segmentation policies, the Illumio Zero Trust Segmentation Platform reduces unnecessary lateral movement across the multi-cloud and hybrid infrastructure, protecting critical resources and preventing the spread of cyberattacks.

illumio