Your Guide to Cybersecurity: Why Traditional Defenses are no Longer Enough

Modern businesses are outgrowing traditional cyber defenses. Discover how to stay ahead of evolving threats and the implications of a cyber-attack.

MENTIS GROUP

Empowering IT Solutions

This eBook covers;

1. Where Your Business Stands on the Cyber Battleground
2. The Anatomy of Modern Cyber Attacks
3. The True Impact of Cybercrime on Businesses
4. The Power of Real-Time Protection for Modern Businesses

Where Your Business Stands on the Cyber Battleground

With AI and advancing tech, launching a cyberattack has never been easier. A simple Google search or ChatGPT prompt can turn a total novice into a serious threat. So what does that mean for your business? More hackers, more attacks, and more ways for them to break into what matters most—your company.

One might think, “Why would a hacker go after little ol’ me?” If there are much larger organizations with deeper pockets, wouldn’t they be the more appealing target? Surprisingly, the opposite is true. Small and medium-sized businesses are the perfect targets—fewer layers of protection and less cybersecurity know-how make them easy prey, putting a cyber bullseye right on their backs.

51% of SMBs do not have cybersecurity measures in place, with 59% of those believing their business is too small to be a target — Verizon

Small and medium-sized businesses (SMBs) are increasingly vulnerable to cyberattacks

Higher Target Rate

SMBs are three times more likely to be targeted by cybercriminals than larger companies. — CISA

Prevalence of Attacks

Approximately 31% of SMBs have experienced cyberattacks such as ransomware, phishing, or data breaches — Microsoft

Financial Impact

Cyberattacks cost SMBs more than $250,000 on average, with potential losses reaching up to $7 million — Microsoft

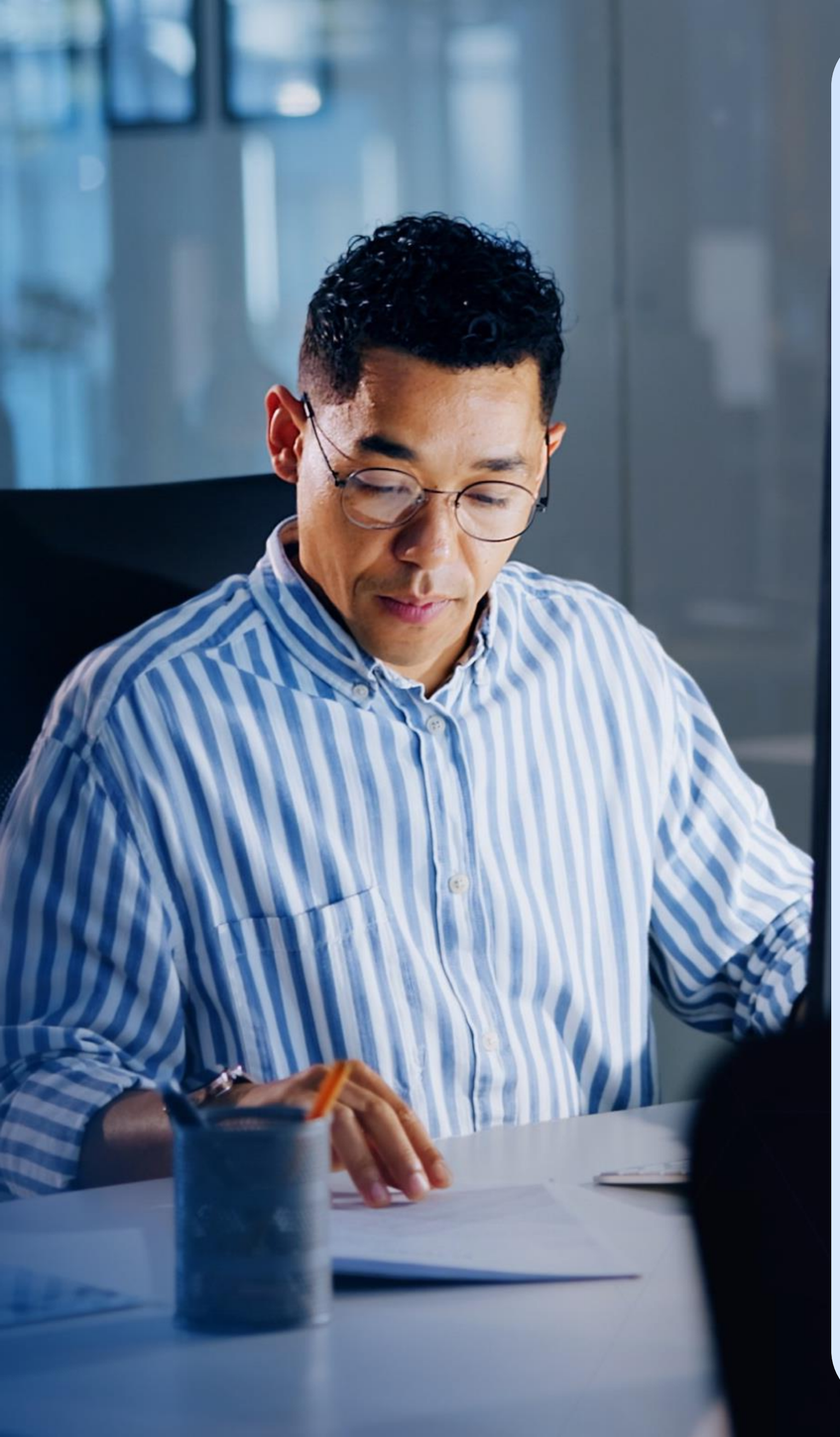
Business Continuity Risk

60% of small businesses that suffer a cyberattack go out of business within six months — Verizon

Cyber-attacks are evolving – *and escalating* – is your business one step ahead?

Cyber-attacks have come a long way since the early days of the internet. What started as simple and opportunistic threats, like viruses and worms, has evolved into highly sophisticated attacks targeting businesses' most critical systems. With each major shift in technology, cybercriminals have adapted their tactics, making it increasingly difficult for businesses to stay ahead of the curve.

1990s	Early 200s	2010s	Mid-2010s	Today
Early internet. Simple, opportunistic attacks like viruses and worms	Rise of e-commerce. Targeted threats like phishing and SQL injection	Cloud adoption. Attackers shift focus to cloud environments	AI-driven tools. Cybercriminals leverage machine learning and automation	New risks from unauthorized access and fraud.
Designed to cause disruption or steal data	Exploiting human error and poor security practices	Weak cloud security configuration and unpatch systems become key targets	Attacks like ransomeware and APTs become faster, larger, and more complex.	Often carried out through compromised account.



As our world becomes more digital, businesses must adapt, but it's equally important to recognize that cyber-attack tactics are evolving alongside this digital transformation. Each step towards modernization comes with its own set of risks a business owner must consider.

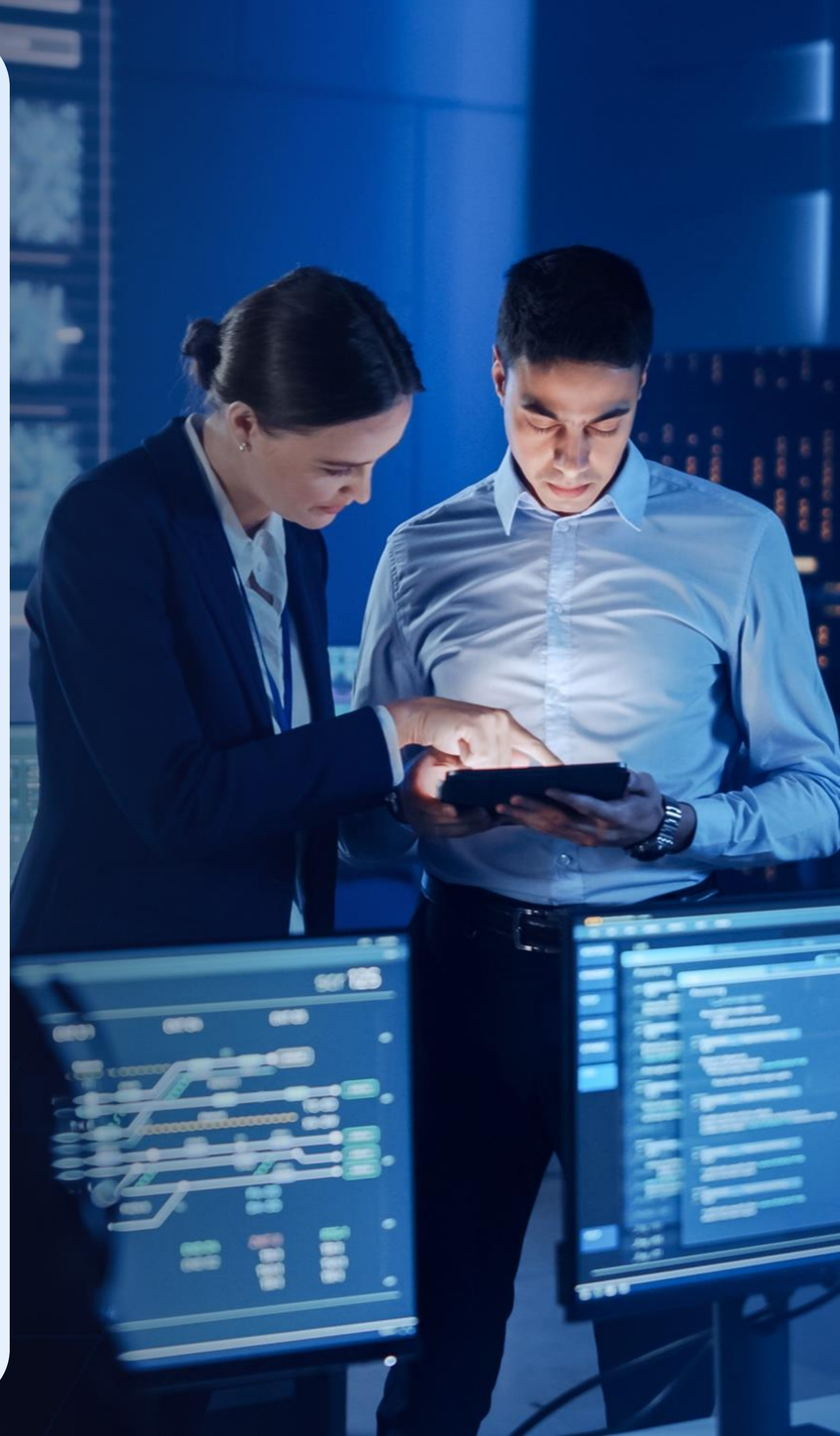
For example, most modern businesses are moving to a cloud infrastructure. Cyber companies, like Blackpoint Cyber, are seeing a **30 to 1 ratio of cloud attacks.** This is because the cloud is a more recent channel for business management, making it less secure and more appealing to threat actors.

Business advancement introduced risk

e-Commerce platforms	Payment fraud, client data leaks
Cloud based infrastructure	Data breach, expanded window for attack, commonly less secure
AI-driven tools	Data breach, AI Manipulation
Subscription based model	Fraud, unauthorized access

First comes cyber risk, next comes regulation

As technology becomes more integral to business operations and cyber threats grow increasingly sophisticated, compliance has become more complex. Cybersecurity regulations have expanded, with industries adopting stricter standards to safeguard sensitive data. As digital transformation accelerates, organizations must not only secure their infrastructure but also stay ahead of evolving regulatory requirements. Failing to do so can result in costly fines and significant reputational damage—potentially having a greater impact on the business than the cyber threat itself.



The Anatomy of a Cyber Attack

So attacks are escalating, small to medium sized businesses are the target, if we know this – why can’t we stop them? Put simply, traditional defenses have not kept up with advancing threats. Traditional security tools typically detect threats too late—when attackers have already gained control of critical systems. On average, it takes organizations 212 days to detect a data breach, according to the 2024 IBM Cost of a Data Breach Report

Cyberattacks are no longer an IT issue, they are a business risk. Without rapid detection and response, a single breach can cripple operations, damage customer trust, and lead to significant financial loss. Understanding this lifecycle is crucial for detecting and stopping threats before they can cause significant damage.

What we were once told was enough, firewalls and antivirus, are no longer sufficient to protect businesses against the sophisticated tactics used in modern cyberattacks. Attackers employ stealthy techniques such as fileless malware, credential theft, and lateral movement to bypass these legacy tools, often slipping through unnoticed. Without real-time detection, threats can linger in networks for months, causing significant damage before being detected.

The Cyberattack Lifecycle & Where SMBs Are Vulnerable:

1. **Initial Access** – Attackers gain entry through phishing, credential stuffing, or exploiting system vulnerabilities.
2. **Execution** – Malicious scripts or legitimate tools are deployed to carry out the attack.
3. **Persistence** – Cybercriminals don't just break in, they find hidden ways to stay in your network, even if initial vulnerabilities are patched.
4. **Privilege Escalation** – Attackers gain admin-level access to elevate their control over systems.
5. **Defense Evasion** – Security tools are disabled, and tracks are covered to avoid detection.
6. **Credential Access** – Passwords or authentication tokens are stolen for further exploitation.
7. **Lateral Movement** – Attackers navigate deeper into the network to locate valuable data.
8. **Data Exfiltration or Impact** – Critical information is stolen, encrypted, or destroyed.

The Real Cost of a Cyber Attack

The cost of a breach extends far beyond just financial loss. Many businesses believe it could never happen to them, but when it does, the toll it takes can leave your company in a state of disarray. From operational disruption to lasting reputational damage, the impact can be overwhelming, affecting not only your bottom line but your ability to recover and regain trust.

Financial Damage

Cybercrime can have devastating financial consequences for businesses. A report from IBM found that the cost of a data breach in 2023 was $4.45 million on average for all organizations. The expenses can quickly escalate when sensitive customer data is compromised, and recovery often takes months.

Operational Disruption

The operational impact of a cyberattack is often felt immediately. Downtime caused by a breach can cripple business operations, impacting everything from production to customer support. According to a study by Tenable, 82% of organizations report that breaches have significant operational disruptions, ranging from a few hours to several weeks.

Reputational Harm

Reputational damage from a breach can be long-lasting, leading to customer churn and a tarnished brand image. In fact, 60% of businesses that suffer a breach see a decrease in customer confidence, according to Verizon's 2023 Data Breach Investigations Report. Once customers lose trust in a company's ability to protect their data, it becomes incredibly difficult to regain that trust, which can result in lost sales and long-term brand harm.

Legal & Compliance Exposure

Legal and regulatory exposure is another major cost of cybercrime. Following a breach, businesses face the risk of regulatory fines and lawsuits, especially if they failed to meet data protection regulations. For example, the European Union's GDPR mandates penalties of up to €20 million or 4% of global revenue, whichever is greater, for non-compliance.

The Human Cost

The human cost of a cyberattack extends beyond financial losses and operational disruption. Employees may experience job insecurity, stress, and burnout due to the crisis, as well as increased workloads during the recovery phase.

True partnership delivers holistic security: protecting your brand, ensuring regulatory compliance, and securing your data

Essential Protection for Modern Threats

As a modern business owner, you are thinking about how to grow and sustain growth within your business like many others. With that modern growth, comes an expanded attack surface traditional tech cannot protect. We understand the risk versus reward and think you can have both – expansion and modernization. Thats why we offer solutions that delivers enterprise-grade protection without the complexity.

The Updated Approach You Need to Protect

To beat today's cyber criminals, you need a proactive security approach that combines the power of real-time threat detection, human analysis and rapid containment to stop attacks before they cause damage. The solution and service that delivers that unified approach is called Managed Detection and Response (MDR). MDR is your essential solution to persistent hackers

Here is how MDR keeps your business safe:

- **Endpoint Protection** — Enhances your Microsoft Defender Antivirus & Defender for Endpoint with continuous threat detection and real human response to threats.
- **Cloud Protection** — Secures Microsoft 365, Google Workspace, and Cisco Duo, preventing cloud-based breaches and responding to signs of identity threats.
- **24/7 Security Operations Center (SOC)** — Our expert analysts monitor and respond to threats in real time. There is no bot on the line, but rather real humans solving real problems.

How Hackers Move Through Your Business and where MDR comes in

Cybercriminals don't just break in and steal data right away. They use a sneaky method called lateral movement—where they quietly move from one system to another, looking for valuable information or ways to take control. This is how ransomware spreads and how hackers gain deeper access to your business.

Our MDR solution stops these threats before they cause damage by:

- **Spotting Intruders Instantly** — If a hacker gets into one system, our team sees it and shuts them down immediately.
- **Locking Down Compromised Devices** — Infected computers are isolated to stop the attack from spreading.
- **Blocking Stolen Admin Access** — If hackers steal a password, our tech disables it right away, cutting them off.

Let us protect your top and bottom line

According to a study by Kroll, nearly half (46%) of organizations are unable to contain a threat within an hour after initial compromise, and for 23% of organizations that reported more than three data compromises in the past 12 months, containment takes at least 12 hours.

KrollReports highlight that Managed Detection and Response (MDR) services can reduce breach dwell time from months to minutes, significantly enhancing an organization's ability to detect and respond to threats promptly.

Cyberattacks on SMBs are increasing—traditional security alone isn’t enough. Our offering delivers real-time protection across endpoints and cloud, eliminating complexity and providing confidence in your day to day operations.

You focus on business growth, and we’ll focus on business protection.

Contact Mentis Group Today to Get Started!

MENTIS GROUP

Empowering IT Solutions

214.691.7800 | sales@mentis-group.com | https://www.mentis-group.com