ZETTABYTES

Cybersecurity Solutions for you

SMBs Are Being Targeted for Cyberattacks
Don't let yours be next.

When you're running a small to medium-sized business, you may think that you're not going to become a victim of a cyberattack. Maybe you think that your data and files aren't valuable enough to be stolen—or even worse, that your current cybersecurity strategy is strong enough to protect them. But nothing could be farther from the truth.

In fact, cybercriminals are becoming smarter every day, and since their methods are constantly changing, your security needs will also need to evolve. To stay safe, adopt a comprehensive cybersecurity solution that protects your entire organization.

Ready to Protect Your Business?
Find out how to minimize digital risk by working with the country's finest security experts. We can help you develop a plan designed to meet your unique needs. Take the first step today.

Why Are SMBs Top Targets?
- They often lack comprehensive protection
- They don't understand the magnitude of their risk
- They underestimate the value of their data
- They are unprepared to battle cybercriminals

Our sophisticated cybersecurity solutions protect all of your business environments, including your brick-and-mortar and your cloud. You'll also need to secure any home offices, mobile devices, hardware, software and cloud-based apps like Microsoft 365 or G-Suite.

Would Your Business Survive an Attack?
Hackers will stop at nothing to get to your valuable data, and it's up to you to protect your business. Ignoring cybersecurity may work in the short-term, but the time to be proactive is now.

Did You Know?
SMBs Account for Over 60% of all Attacks

Is Your Guard Down?
- 69% of SMBs have not identified and documented cybersecurity threats
- 43% do not have a recovery plan in the event of a cybersecurity incident
- 57% have not informed or trained all users on cybersecurity
- 48% have not analyzed cybersecurity attack targets and methods

ZETTABYTES

Your Cybersecurity To-Do List:

- **Understand the Risk**
  While you're busy trying to beat out the competition, cybercriminals are busy hatching schemes to infect your devices with malware, take you down with a business email compromise attack (BEC) and steal your valuable data. You can't let that happen. It's a cost you can't afford to bear.

- **Take Responsibility**
  After reading up on the latest cybersecurity threats and understanding how easy it is for a small to medium-sized business to fall victim to an attack, tackle the challenge head on. With so much at stake, you need to come up with a plan that gets your security on a strong foundation. Bring in the professionals.

- **Assess Weaknesses**
  You won't fully understand your risk until you meet with security experts who can conduct a thorough security assessment and diagnose structural weaknesses. To truly protect your business from cybercrime, you'll need to undergo a cybersecurity evaluation to identify vulnerabilities.

Close Gaps in Security
You can't secure your organization until you understand your risk.

Security for a Remote Workforce
Mobile workers are playing a more important role in operations than ever before. While empowering your remote workforce with the right technical tools will drive productivity and success, the work-from-home (WFH) era is also introducing new security risks for small to medium-sized businesses. In addition to providing IT support for remote workers, you'll want to defend your business from common cloud computing risks and cybersecurity threats.

Cybersecurity Risks

- **Mobile Devices:** Protecting and monitoring smartphones, tablets and laptops is harder in the bring-your-own-device era. Enter mobile device management.
- **Remote Access:** With employees working outside of the office, it's important that they have secure remote access to your network.
- **Identity Authentication:** It's easy for bad actors to impersonate your employees—keep the hackers out with identity authentication management.
- **The Company Cloud:** Storing and transmitting data in the cloud makes conducting business a breeze, but it opens up a lot of risk, too.
- **Cloud-Based Apps:** Collaborating in Microsoft 365 or G-Suite is simple, but that doesn't mean it's secure.

Are All of Your Business Environments Secure?

Given the rate at which risks evolve, you're going to need a dynamic strategy for cybersecurity that accounts for mobile workers. Protecting remote workers is easier once you understand

today's top cyberthreats and how they could take down your business. Secure your data and your future by partnering with a trusted MSP who will evaluate your risk and create a custom business continuity plan.

Why Partner with Zettabytes for Security Solutions?

Once you understand what's a stake, it's hard to put off cybersecurity any longer. When you're ready to prioritize security, it's time to bring in the professionals.

There's never been a better time to work with top-tier security consultants who are united around one common goal: Keeping your data secure. Let industry insiders protect your business with an all-encompassing approach to cybersecurity that will help you avoid falling victim to an attack.

Benefits of Professional Cybersecurity Services Include:
- **Comprehensive Cybersecurity:** Benefit from layered security solutions that protect your business from every angle and anticipate future challenges.
- **Nonstop Monitoring and Support:** Let security experts stand guard 24/7/365, identifying suspicious behavior and providing around-the-clock monitoring.
- **Future-Oriented Business Plans:** We'll assess your current cybersecurity risks and make sure your new strategy evolves alongside emerging threats.
- **Protection for Cloud-Based Suites:** Our team of security professionals can protect your Microsoft 365 apps, including SharePoint, Teams and OneDrive.

Security is Everything
Stop putting IT off and talk to an expert today.

How We Can Help
- **High-Level Security Assessment:** Let us provide you with a detailed picture of your cybersecurity health and security exposure, including scanning your information on the dark web.
- **Custom Cybersecurity Report:** Following the security assessment, we'll create a detailed report on your vulnerability, allowing us to assess how we'll proceed to keep you safe.
- **Industry-Specific Action Plan:** We'll work together to create an action plan that will start securing your organization and its technology. This includes monitoring threats on all managed devices, servers and firewalls.
- **Compliance IT Solutions:** After closing gaps in security, we can support compliance guidelines and make sure your data stays out of harm's way. Maintaining compliance is easier with security analysts on your team.