COST COMPARISON GUIDE

Weighing the Price of Security

Compare the Price of SMB Cybersecurity Solutions to the Real Cost of Being Unprepared
The evolution of technology has made it more dangerous than ever to be a small business competing in an increasingly digital arena. Hackers take advantage of patches (or lack thereof), databases, and infrastructures that haven’t evolved with security standards. As the number of small businesses targeted by malicious attacks continues to rise, you can’t just keep hoping the next attack won’t target your business.

While it seems like sophisticated next-generation protection won’t fit into your budget, the reality is that the upfront costs of a security solution are much more affordable than the recovery costs of a cyber-attack or data breach. Standard protection, ranging from network security to employee training, are available in a variety of prices that make security a reality for small businesses.

In this guide, we’ll help you better understand the risks and show you how the price of solutions weighs up against the havoc an attack can wreak on your business. Solutions are easier and cheaper than you would expect compared to the damage that can be brought on by a hacker.

**Increased Risk for SMB**

It is comforting to think that hackers only focus on enterprises, but that is a myth. Because smaller businesses often have fewer resources and minimally staffed IT teams, they are a prime target for digital destruction. In addition, small businesses are at risk for not recovering from an attack. While large enterprises can usually recover from a breach, the financial burden of just one disastrous attack can have a deep and lasting impact on a smaller organization.

The number of cybercrimes aimed at small businesses continues to increase year over year. From 2017 to 2018, attacks on SMBs have increased from 61% to 67%.¹ It should be noted that many of these attacks can be prevented with widely available security solutions.

The increased amount of attacks is just one of the reasons SMBs need to have an up-to-date security strategy. Unfortunately, many small businesses report that they don’t have any active strategy. In fact, 62% of SMBs don’t have an up-to-date strategy or any strategy at all for a security breach.²
Cost of an Attack

The true impact of any successful attack or data breach is multi-dimensional. There’s the cost of recovery efforts like replacing damaged technology or consulting with forensic experts, as well as the expense of operational disruption from the attack. A site being shut down by a DDoS attack can have a great impact on profits—and reputation—of any organization, even if the attack only lasts a few hours.

The damage of cyber-attacks has resulted in small businesses having to spend an average of $1.43 million to recover lost or stolen technology per attack. This doesn’t include the additional $1.56 million that businesses suffer in operational costs. A hack of that magnitude could be enough to put any SMB out of business.

Today’s Most Prevalent Threats

The most common attacks toward small businesses include compromised passwords, advanced malware, and ransomware. The average amount paid for ransomed data is $1,466. The cost of an attack due to a negligent employee with a weak password averages $383,365. With less damaged technology to upgrade, the losses are lower, but it can still be avoided with a balance of solid security solutions and proper employee training.

Another area of primary concern is the value of data lost in a breach. With fewer cloud backups and more vulnerabilities than enterprises, a small business can be even more susceptible to losing and exposing user and customer information. The average cost of lost or stolen data is $148 per record. The total costs can climb to millions of dollars, depending on the size of the breach.
Cost of Solutions
While the cost of a breach sounds like a lot, it is much easier to pay considerably less for proven security solutions that can keep your business safe. Despite the importance of cybersecurity, it doesn’t have to take a large portion of your budget. Standard practices typically involve spending less than 13% of your hardware and software budget on security solutions depending on your business size. There are a number of proactive solutions for SMBs that won’t break the bank, but can effectively neutralize and mitigate a range of threats from malware to phishing and compromised customer records.

1. Endpoint Security
There are effective solutions available for protecting users and endpoints. Antivirus is one of the standard defenses that should be installed on all users’ devices. It usually costs between $20-$60 per device per year, with some free options for small businesses. Unlike the standalone antivirus, endpoint protection software can cover a wider range of threats toward devices for a price of approximately $32-$340 per year for 5 devices.

2. Network Security
Network security is another important aspect to keep top of mind. While network security covers some of the same threats as endpoint security, it can also help monitor for potentially harmful traffic—meaning you can potentially stop a breach before it occurs. Network security software can cost anywhere from $50-$6,000 depending on the size of your network and the level of security you are looking for. Solutions specifically designed to monitor performance can cover a small network for the price of about $0-$2,656.

3. Fighting Specific Threats
Adjacent to network security are DDoS mitigation and VPN solutions to avert “man-in-the-middle” attacks. Preventing your servers from shutting down due to high traffic can cost just a portion of the price of a shutdown at $2,400-$36,000. One of the ways to fight digital eavesdropping is by using a VPN, which generally costs between $40-$100 a year for up to 5 connections.

4. Employee Education
No business can afford to neglect cybersecurity training for every employee. This can be accomplished with a variety of free training tools and a few hours of everyone’s time. There are also security courses that cost around $30 per employee per year. This training can be a great asset against threats like phishing, spoofing, and compromised passwords. The cost of $383,365 for an attack involving compromised passwords puts into perspective the value of cybersecurity training.
<table>
<thead>
<tr>
<th>Solution</th>
<th>Solution Price per Year</th>
<th>Highest Price for 100 Employee Business*</th>
<th>Percent of Average Attack Cost**</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus Software</td>
<td>$20-$60 per device</td>
<td>$6,000</td>
<td>0.42%</td>
</tr>
<tr>
<td>Endpoint Protection</td>
<td>$32-$340 for 5 devices</td>
<td>$6,800</td>
<td>0.48%</td>
</tr>
<tr>
<td>Network Security Software</td>
<td>$50-$6,000</td>
<td>$6,000</td>
<td>0.42%</td>
</tr>
<tr>
<td>Network Monitoring Tools</td>
<td>$0-$2,656</td>
<td>$2,656</td>
<td>0.19%</td>
</tr>
<tr>
<td>DDoS Mitigation</td>
<td>$2,400-$36,000</td>
<td>$36,000</td>
<td>2.5%</td>
</tr>
<tr>
<td>VPN</td>
<td>$40-$100 for 5 connections</td>
<td>$2,000</td>
<td>0.14%</td>
</tr>
<tr>
<td>Employee Cybersecurity Training</td>
<td>$0-$30 per employee</td>
<td>$3,000</td>
<td>0.21%</td>
</tr>
</tbody>
</table>

* Calculation based on the top price of a solution in the previous column, assuming 100 devices, connections, and employees. This is an estimate, not a guaranteed quote. Price could vary based on company needs.

** Percentage calculated by comparing the solution price for 100 employees with the average recovery cost of $1.43 million following an attack.

Different companies require different combinations of solutions, but the bottom line is it pays to be prepared. Most solutions cost less than 1% of the $1.43 million price of a cyber-attack. Even at an SMB with a low budget, there is room to pay for solutions that could save the company in the long run.
Conclusion

When the average cyber-attack on SMBs can cost hundreds of thousands of dollars in disruption of operations and recovery, it pays to invest in security. Every basic security solution costs less than 3% of the total amount your business could lose without said protection. By deploying solutions, you could save not only your budget, but also your business.

Our security solutions are on track to prevent over $1 billion in cybercrime damages this year with over 400k cyber-attacks halted each month.

As you take a closer look at how security solutions fit into your budget, make sure your solutions not only compliment your budget, but also your infrastructure and your IT team. With experts and threat labs on hand, there are solutions that can provide holistic support designed for the leanest IT teams.

CenturyLink offers solutions that keep your business secure from costly threats. Our security solutions are on track to prevent over $1 billion in cybercrime damages this year with over 400k cyber-attacks halted each month. That means saving your business from costly attacks.

CenturyLink solutions include adaptive network security services, DDoS mitigation services, adaptive threat intelligence, security log monitoring, managed security for Cisco Meraki, WorkWise™ cybersecurity awareness training, and security consulting. These multi-layered security options proactively defend against and dynamically respond to constantly evolving threats.

These solutions have the backing of CenturyLink Threat Research Labs, which are continuously identifying new threats. They discover more effective techniques to keep your business safe, and the labs can deploy a security solution before you even know a threat is coming.

CenturyLink securely connects, proactively monitors and effectively defends against constantly evolving security threats. Talk to a CenturyLink expert to find a security solution that not only saves you money, but protects the reputation of your business and keeps your customers’ information safe.

Learn more

See how solutions from CenturyLink can help you avoid paying the price of being underprepared.

Sources:

Learn more

See how solutions from CenturyLink can help you avoid paying the price of being underprepared.