Identity Thieves, Hackers and Crooks, Oh My!

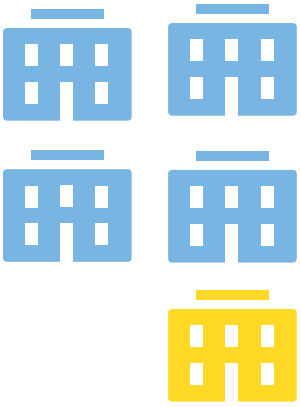
4 IT Security Features Every Business Needs

MYDIGITALSHIELD

Table of Contents

(Click to jump to section.)

Overview of the Online Security Landscape



1 in 5

small businesses falls victim to cybercrime each year, and of those, some 60% go out of business within 6 months

Small businesses are getting hit left and right by identity thieves gunning for customer credit card numbers, hackers attempting to sabotage networks and gain access to sensitive data, and employees looking to make a quick buck.

According to the National Cyber Security Alliance, 1 in 5 small businesses falls victim to cybercrime each year, and of those, some 60% go out of business within 6 months as a result of the accompanying financial damages.

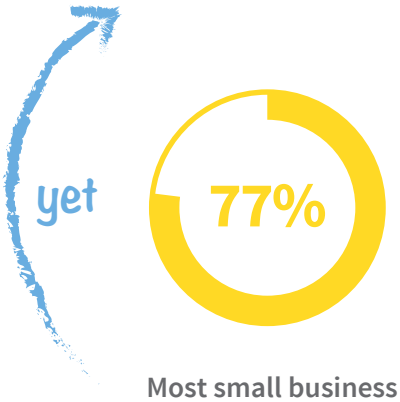
Antithetically, **most small business owners are unaware of these threats,** as 77% say their company is safe from cyber-attacks, yet **83% have no formal cyber security plan to speak of**.

Of course, not every small business is equally likely to fall prey to cybercrime. Hackers usually don't discriminate by company type, valuation, or any other characteristic of the business itself, rather they look for those businesses that are vulnerable because of lax digital security.

4 IT Security Features Every Small Business Needs

With the number of security attacks and threats out there today, even small businesses need enterprise-grade IT security features in place. But most small businesses can't afford the costs associated with incorporating an enterprise-level anything, let alone an IT solution.

> **Visa Inc. reports small businesses represent more than 90% of the payment data breaches reported to the company.**



Most small business owners are unaware of these threats, as 77% say their company is safe from cyber-attacks

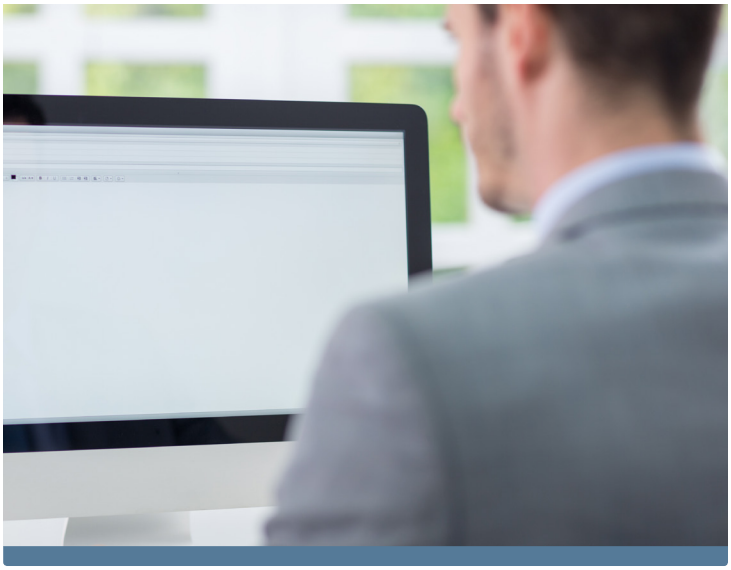
That's why it's important for small business owners to find a cloud-based solution that doesn't involve expensive hardware, installation, setup or engineer-related labor costs. **Cloud-based security solutions can be had for as little as $69 per month and work to protect small business owners from the financial and legal disasters that can result from security breaches.**

Additionally, unlike most traditional methods of protection, a cloud-based IT security solution does not operate on your network and take up precious bandwidth, allowing small businesses to remain competitive and function seamlessly in an age where everyone and everything is interconnected and fast-paced.

In this e-book we'll cover the top 4 security features every small business needs to stay safe:

Four Security Features Every Small Business Needs

1. Next Generation Firewall (NGFW)
2. Advanced Threat Protection (ATP)
3. Secure Wireless Connection
4. Data Leakage Prevention (DLP)



1. **Next Generation Firewall (NGFW)** – Installing a NGFW will control what applications are allowed on your network and protects against malicious activities, threats and attacks. It's the first line of defense against intruders and hackers.
2. **Advanced Threat Protection (ATP)** – Implement a large-scale enterprise IT security apparatus at a small business cost with Advanced Threat Protection that gives your network the most up-to-date protection against all new and developing threats.
3. **Secure Wireless Connection** – If you're running on an open, unsecured Wi-Fi network, you're asking for trouble, plain and simple. Even the most unsophisticated hackers are wise on how to crack into your network. From there, your company's tax records, financial documents, customer lists and transaction details are fair game.
4. **Data Leakage Prevention (DLP)** – Protect credit card numbers, transaction details, and other forms of sensitive data by implementing Data Leakage Prevention (DLP) policies and encrypting all devices and removable media with access to confidential information.

83% of small businesses have no formal cybersecurity plan to speak of.

Protecting your business and clients from cyber-crime and online threats is no longer a secondary priority for smaller businesses today. While in the past, only large companies were in the sights of **hackers and online criminals**, increases in their network security and cyber defenses **have redirected these threats towards smaller, easier targets**.

Obscurity is no longer a viable strategy for online protection and IT security, and with the prevalence of these cyber-attacks, coupled with the devastating financial consequences that accompany them, every business owner needs to take a serious look at how protected their business is against threats in the digital age.

Next Generation Firewall

The world is changing, and in the perpetual arms race between hackers and internet security protocols/systems, traditional network security strategies have become obsolete. **New sophisticated attacks and methods of mal-code delivery are able to easily bypass traditional firewalls, intrusion detection systems, and host-based antivirus programs**.

Firewalls were designed to serve as the boundary between the open internet and an organization's private network, and typically act as a gatekeeper by controlling specific protocols and ports, as well as restricting traffic to and from certain IP addresses.

A traditional firewall policy focuses on five factors, commonly referred to as the "5-tuple," to assess whether or not to allow certain types of traffic through to the web server:

- **Source of the IP address**
- **Destination of the IP address**
- **Source of the port**
- **Destination ports of 80 and 443**
- **Destination of the specific protocol**

Unfortunately, as more and more people are using the internet and firewalls encounter more and more traffic, the line between malicious and genuine traffic has become blurred. Since almost all internet traffic traverses through http (port 80), firewalls are forced to keep it open, allowing hackers to use it as their private highway to deliver mal-code and access your private network.

Next Generation Firewalls (NGFW) are the next step in effective internet and network security. In essence, NGFWs go beyond the common protections provided by traditional firewalls by widening the scope of the 5-tuple to include intended application, user identity, and source reputation of all incoming traffic.

However, not all NGFWs are the same – or rather, not all firewalls named NGFWs actually offer next generation protection. **In order to get the protection you need, your NGFW should include:**

- **All the standard features of traditional firewall**

  Includes packet filtering, network address translation, and VPN capabilities.

- **An integrated network intrusion prevention system (IPS) with deep packet scanning**

  While Intrusion Detection Systems (IDS) have been one of the most common security solutions on the market for some time, such systems continue to evolve and respond to the ever-changing threats of the modern cyber-world.

  One such evolution brought on by the NGFW is the change from a basic Intrusion Detection System to a Signature-based Intrusion Prevention System, which incorporates all the pre-emptive detection abilities of a traditional IDS with the ability to then tag and prevent potential threats from entering a network or organization.

  Similar to an IDS, a Signature-based IPS monitors and scans traffic flowing into the network for malware and suspicious activity. Where it differentiates, however, is in its ability to respond to known, and suspicious, malicious signatures.

  Additionally, with the adoption of cloud computing, the effectiveness of Signature-based IPSs has skyrocketed, as they grant signature-based IPSs access to an online database of thousands of new and unique signatures, as well as real-time updates and data on new, developing threats and reputation-based detection technology.

Traditional Firewall

"5-tuple"

- Source of the IP address
- Destination of the IP address
- Source of the port
- Destination ports of 80 and 443
- Destination of the specific protocol

Next Generation Firewall

Includes all the standard features of traditional firewall in addition to:

- An Integrated network intrusion prevention system (IPS) with deep packet scanning
- Web filtering to prevent access to 'high-risk' websites
- Gateway anti-virus to scan incoming data for malicious content
- Application Control Abilities

▶ Web filtering to prevent access to 'high-risk' websites

Unknowingly going to 'bad' websites, or downloading 'infected' content, is one of the most common ways a computer or network gets infected. With web filtering, a NGFW goes beyond traditional firewall protection by 'following' the user out onto the web, and preventing them from accessing questionable sources and thereby accidentally putting your network at risk.

With cloud-based web filtering, provided by Fortinet, users can select category-based filtering depending on the needs and concerns of their specific business model and industry. Additionally, as some threats only occur occasionally, cloud-based web filtering also allows for temporary blocks, or in some cases bypasses, on certain web content, giving more control and customization to the user.

▶ Gateway anti-virus to scan incoming data for malicious content

Gateway Anti-Virus allows applications across your devices to check files and other types of incoming data for potential threats to the system through a full proxy mode scan, which catches zipped files, polymorphic viruses, and other more advanced threats that the average anti-virus is unable to protect against.

▶ Application control abilities

Application control, also known as application awareness, is capable of identifying applications and applying controls at the application layer (such as allowing regular Skype calls but blocking users from being able to transfer files over the service.) This service is an addition brought on by the NGFW, which monitors and blocks the input, output, and system services calls when they do not meet the configured policy of the NGFW.

> **Gateway Anti-Virus catches zipped files, polymorphic viruses, and other more advanced threats that the average anti-virus is unable to protect against.**

These additional features are necessary to provide effective protection in the modern internet age, and relying on a simple, traditional firewall is paramount to relying on an unlocked door to protect your brick-and-mortar business.

However, while employing a NGFW is a major step toward securing your internet connection from malicious attacks, it is only the first step.

A NGFW will provide sufficient protection from internet-based attacks, but it is incapable from stopping people within range of your wireless signal from accessing your network and wreaking havoc from within – and with the latest technology, your Wi-Fi signal may be reached from all the way down the block.

Advanced Threat Protection (ATP)

On today's internet, threats to a company's network security can come from anywhere, with threat levels ranging from 'novice hacker' to 'hardened cyber-criminal.' Luckily, the former is rather easy to deal with, but while more advanced firewalls and strategies to secure your wireless signal may protect your business from 'run-of-the-mill' cyber-threats, **small businesses are increasingly becoming victims of more targeted, and hard hitting, cyber-attacks that are not so easily dissuaded**.

To put it simply, professional hackers are discovering the unmined potential of relatively unprotected small business networks, and the average cyber-threat these businesses

face is becoming more sophisticated, and more difficult to prevent, requiring business owners to implement enterprise levels of protection to face Fortune 500 levels of attack.

Unfortunately, the type and level of protection that large-scale enterprises use often come with a large-scale price tag, making them unaffordable, for small businesses to implement. In effect, many vendors have begun suggesting 'sandboxing' as an alternative strategy for small businesses to mitigate some of the increased risk inherent to being online today.

However, while strategies like these certainly have their benefits, they are only one part of an overall professional enterprise-like protection apparatus that small businesses really need in order to meet the modern demands for network security.

Fortunately, due to the adoption of cloud-computing, small businesses no longer need to sacrifice quality protection for affordability. With Advanced Threat Protection (ATP), **small businesses now have access to Fortune 500-levels of IT protection that focuses on the five most fundamental areas of advanced protection at a fraction of the cost that big companies pay.**

In addition to the basic protection provided by services like 'sandboxing,' **the five areas that make up the framework for large-scale enterprise IT protection are:**

1. **Access Control:** By limiting access to the network through certain, predetermined authorized ports available to authorized users only, this feature of an ATP system reduces the overall risk of a network breach or data leak by minimizing the vulnerability of the network to only a few access points.
2. **Threat Prevention:** Similar to an IPS, threat prevention monitors and inspects all incoming code, packets of data, visited websites, and program/command applications for suspicious and known methods of intrusion.
3. **Threat Detection:** In addition to threat prevention, this feature of an ATP system continues to monitor the network for indicators of intrusion or compromise that may have gotten past the first few layers of protection.
4. **Incident Response:** Identify and contain. This new feature included in an ATP system identifies and contains problems if the detection and prevention systems mentioned above find a threat in your system.

Framework for Large-Scale Enterprise IT Protection

5. **Continuous Monitoring:** Continuous monitoring is the baseline for ATP, assessing and improving your current security measures against the newest known threats and methods of attack.

In today's online world, threats to network security are evolving constantly, and without access to live updates or a large database of known and developing threats, traditional firewalls, anti-virus, and even sandboxing are not able to prevent infections they have not encountered and documented before.

As new cyber-threats become increasingly automated and intelligent, more flexible and in-depth measures of protection are warranted. Without a cloud-based ATP system in place, your business networks will be playing a game of perpetual catchup, where the stakes are higher than they have ever been before.

Secure Wireless Connection

Many businesses nowadays use wireless (Wi-Fi) networks to enable their laptops and other business-specific hardware to connect to the internet and do on-the-spot transactions and business processes. Unlike a traditional wired network, which requires a "rat-nest" of wires to connect all one's devices to the internet, Wi-Fi networks are much more convenient and practical as they allow for easy internet access and scalability of necessary bandwidth for small business owners.

However, these benefits are not without their shortcomings and unlike traditional wired networks, which are extremely difficult for someone to hack into and require a physical presence to do so, an unsecured Wi-Fi network exposes the business or network owner to unnecessary risk from outside intrusion.

Wi-Fi networks generally include a modem that is attached to the cable or telephone network and connected to a wireless router, which provides broadband internet service via a Wi-Fi signal.

The big problem with these wireless signals is that, if unsecured, they often give indiscriminate internet access to any device in range, which allows unauthorized users to access your network without your knowledge.

This unauthorized access presents three major, yet unnecessary, risks:

1. **It can increase your monthly Internet bill especially when you have to pay per byte of data transfer.**
2. **It can decrease your Internet access speed since you are now sharing the same internet connection with other users.**
3. **It can create a security hazard as others may hack your computers and access your personal files or download malware or illegal files through your own wireless network.**

For small business owners, many of whom may already be running on tight margins, these three risks can lead to catastrophic losses, data breaches, and ultimately, business failure if left unchecked. Fortunately, these risks can largely be mitigated, and in some cases even avoided, by taking proper precautions towards securing your network:

1. **Enable encryption on your access point.**

   WPA or WPA2 protocols are needed to replace the older WEP protocol that most wireless networks typically rely on (unless they are state-of-the-art.)

2. **Change your network's SSID name and password to something unique.**

   This makes it harder for malicious users to find your Wi-Fi network and attempt to gain access by impersonating you. Everyone uses 'Admin' or 'Linksys' and hackers know that. Also, most default factory setting passwords are publically known and if you're still using the same password, it's only a matter of time before someone gains access to your system.

3. **Check to make sure your router's firmware is up-to-date.**

   You can find the existing firmware version of your router from the router's dashboard at 192.168.1.1

4. **Disable remote login.**

   This is often the first strategy of a brute force attack by a router worm/virus attempting to gain access to your network.

5. **Disable wireless administrating.**

   Change the setting that allows administrating the router through a wireless connection to 'off' (meaning that you need to connect with a LAN cable for administration.) This disables any wireless hacking into the router.

In short, WPA2 encryption, using a (truly) complex passphrase, and up-to-date firmware should provide sufficient security for your wireless network against most common attacks. Not only will it be harder to find, but it will take more time and energy for an unauthorized user to gain access to your network.

However, **while this may stop your average mal-doer**, there is no guarantee that it will stop a dedicated hacker with the right tools and patience. Often, this type of attacker will not waste time on the common network, but **if your network is hiding something of value, like credit card information or sensitive data, they may be drawn to it like blood in the water**. If this is the case, more security may be warranted.

Data Leakage Protection

Small businesses today are exposed to two primary sources of data breaches; from the internet, as information travels from one user to another, and from malware that gets into their system from emails or masqueraded as some other downloadable software.

In fact, research from the Ponemon Institute, which tracks data surrounding digital privacy and security, shows that as larger enterprises increase their IT security and infrastructure, less-secure small businesses become more exposed to cybercriminals looking for a quick buck.

And as more and more methods of attack become automated, allowing more novice hackers to present a threat, small businesses are increasingly experiencing the majority of cyber breaches.

However, according to a recent poll by the U.S. Small Business Administration, **86% of small businesses say they are satisfied with the amount of security they provide** to protect customer or employee data.

Visa Inc. reports small businesses represent more than 90% of the payment data breaches reported to the company.

So, how can small businesses protect themselves from data breaches and cyber-attacks without breaking the bank?

While security technologies such as asymmetric-key encryption offer state-of-the-art protection for data in transit, most security breaches and threats come from within the system, allowing unauthorized users access to private keys and other decryption codes, thus rendering any sort of encryption useless.

Many of the malware threats circulating the Internet are designed to collect user names and passwords from victims' computers, and once the malware takes root, it often waits for the user to visit a banking or financial site and then automatically captures log-in information and sends it back to the cybercriminal, who can then use those credentials to wipe out an account.

Oftentimes this malware is 'invited' into the system by a user opening or downloading a bad link from an email or website - making it a user error, or PEBCAK (problem exists between chair and keyboard) situation - which, subsequently, makes it difficult for most prevention methods from catching or stopping the threat. **In fact, 98% of business data breaches happen this way.**

The solution to this is to implement a Data Leakage Prevention (DLP) system, which classifies a company's data based on its sensitivity and then prevents data breaches by monitoring, detecting, and blocking the sensitive data in endpoint actions, network traffic, and data storage.

With proper DLP policies in place, your business's sensitive data — such as account numbers, passwords, and client credit card information — are protected from accidental exposure and the financial risk that accompanies such breaches.

Staying Safe in a World of Identity Thieves, Hackers and Crooks

With the increasing frequency of data breaches and cyber-attacks suffered by small businesses today, you can't afford to leave your business or clients unprotected against these threats.

However, corporate-level protection — the kind of protection you need, since many hacking methods were developed for large companies and then repurposed for smaller, easier targets — is often unaffordable.

Likewise, common market solutions to small business IT security often produce a large drain on available bandwidth and leave the network slow and limping along. In an age of fast-paced consumerism and large-scale interconnectivity, security problems like this leave your systems handicapped against competitors, disabling you from taking advantage of the opportunities that being online provides.

My Digital Shield
Plug-and-play IT Security for small businesses

While it may seem like a lose-lose situation for small business owners, implementing the security features described in this e-book goes a long way towards mitigating the most common types of threats and forms of attack found online. Additionally, recent technological developments like **cloud computing makes adding these types of security features** to your outfit more practical and relatively **painless if you go the route of a plug-and-play solution designed specifically for non-tech savvy individuals**.

All it requires is a small, router-like device that plugs in to your internet connection and sits between any data collection device at your store (like a point-of-sale computer, desktop PC, or credit card terminal.)

Data entered into the credit card terminal or computer is funneled up to the secure Fortinet cloud (trusted by top enterprise organizations) where it is measured, analyzed for threats, and then made available again to defined and secure end points.

Basically, a solution like this keeps data safe within a closed system and prevents unauthorized infiltrations into secure networks, keeping sensitive digital files safe from hackers who attempt to gain access to information as it travels across the internet.

While no system is completely secure, and getting anywhere close to near perfect protection would be prohibitively expensive, the availability and relative low cost of cloud-based IT security solutions currently on the market promises to make the business world of tomorrow a much safer place for small businesses – at least for those taking the right precautions today.

Learn more about cloud-based IT security for small businesses