ManageEngine

Endpoint Central

Essential **cyber hygiene** for small and midsize businesses

Table of Contents

What is cyber hygiene?

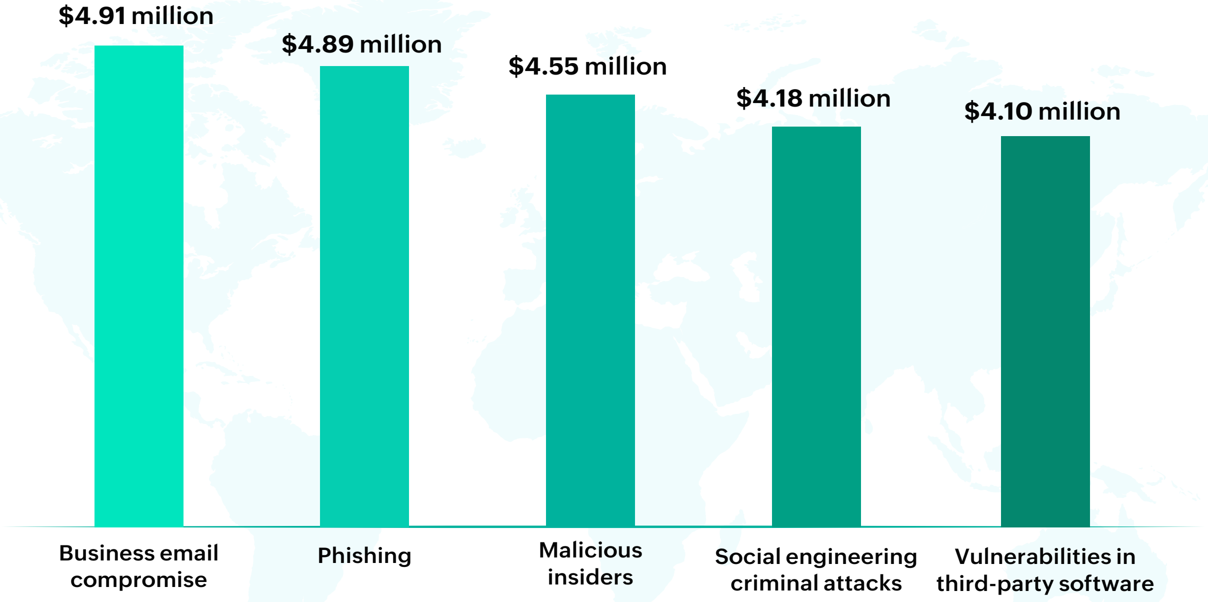
Cyber hygiene is the careful effort to protect yourself online. It's similar to personal hygiene, where you adopt routines that will keep you free from health issues. When it comes to an organization, cyber hygiene is a set of routine procedures for managing and maintaining the security of individuals, devices, data, and networks. They are essential cybersecurity best practices that all employees, not just security officials, should adhere to. The ultimate goal of cyber hygiene is to create a human firewall that makes it impossible for attackers to breach a network because everyone in the organization is alert on the security front.

Why does cyber hygiene matter?

In the onset of the pandemic, businesses turned to technology for survival. But so did the cybercriminals, being quick to take advantage of a chaotic situation. In 2022, 79% of organizations agreed that remote working had adversely affected their cybersecurity.[1] Now that remote working is here to stay, good cyber hygiene can help you prevent cybercriminals from doing their thing—or, at the very least, make it so difficult that they give up and move on to the next victim.

> "I am convinced that there are only two types of companies: those that have been hacked and those that will be."
>
> **Robert Meuller**
> Former FBI director

Up to one in four Americans stop doing business with a company after it suffers a data breach.[2] It's routine mistakes—failing to keep track of which endpoints are connecting to your network, failing to set the proper security configurations, losing control over patch updates, and failing to identify and fix breaches—that cause the majority of successful attacks.



2022’s top 5 expensive data breach vectors

It's not only heavy on the pocket, it can hurt a company's reputation too.[4] Financial loss, fines from the government, interruption of operations, organizational turmoil, loss of consumer trust, and legal liability are some dire effects of a data breach. Good cyber hygiene not only saves your organization from these struggles, it can also help your endpoints run at peak efficiency, meaning fewer complaints of slow systems or downtime.

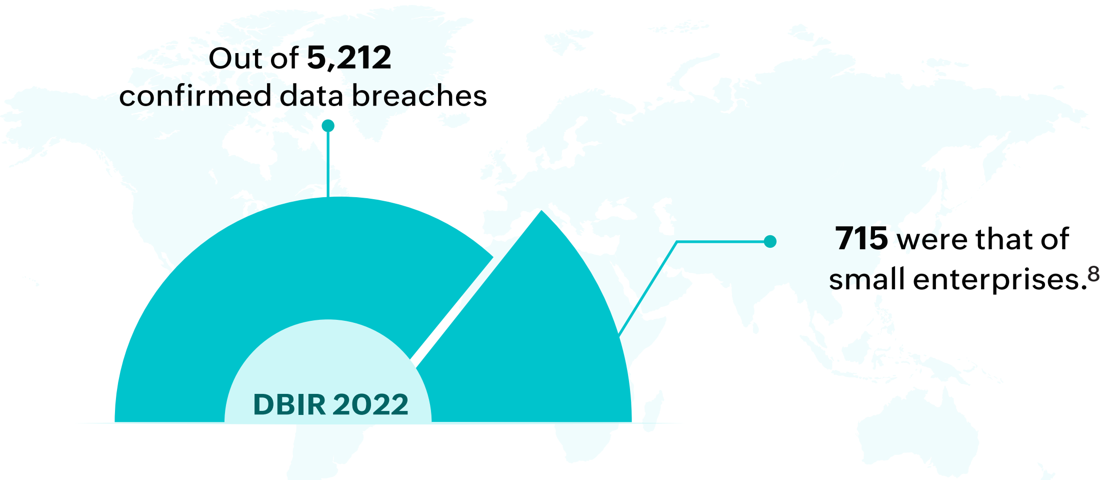
Why are SMBs prone to cyberattacks?

Today, small and midsize businesses (SMBs) account for 90% of all enterprises and are crucial to a country's economy, especially in developing countries. They account for 70% of employment and generate seven out of 10 jobs in the market, worldwide.[5] As a result of their capacity to create jobs at minimal capital costs, the number of SMBs have been growing in recent years.

Because of their impact, SMBs have minimal room for disruptive cybersecurity incidents. SMBs who get attacked pay the price of halted operations, ransom payments, reputational harm, losing customers, and a long, difficult recovery. SMBs that do recover are relatively uncommon; nearly two thirds of SMBs shut down within six months of being hacked.[6]

> **" When it comes to data protection, small businesses tend to be less well prepared. They have less to invest in getting it right. They don't have compliance teams or data protection officers. But small organizations often process a lot of personal data, and the reputation and liability risks are just as real."**
>
> Elizabeth Denham
> Former UK information commissioner

Companies now confront a more difficult struggle against cybercrime as more and more employees choose to work from home. Remote work has contributed dramatically to the rise in successful ransomware attacks,[7] as employees are now handling company data while away from the company's premises.



Here are five main reasons why SMBs should be extra cautious of cyberattacks:

They are weaker targets than larger companies

They might not have a specialized IT team

They act as a bridge to the larger companies

They can't afford pentesters due to high demand and cost

Their priority is R&D and marketing over security

> “ 90% of all CVEs discovered in 2021 so far can be exploited by attackers with limited technical skills. ”
>
> NIST NVD Analysis,
> Redscan Labs

Best practices for good cyber hygiene

The opposite of security isn't insecurity, its convenience. The convenience to do easy things rather than the right things.

Cybercriminals today are annoyingly good at finding under-protected and unprotected networks. SMBs must strengthen their security posture. The term "security posture" refers to a company's overall cybersecurity program and how well-positioned it is to face both current and future threats. As tedious as cybersecurity practices may be, security incidents happen when we least expect them.

End-user education

A chain is only as strong as its weakest link, and an organization is only as secure as its least-aware employee. It is important that your staff know the role they play in protecting the organization. They should receive training and education on how to generate secure passwords, spot phishing scams, and what to do if they find anything suspicious.

Access control

In a study, 74% of data breach victims admitted that cyber incidents involved access to a privileged account.[9] As workers change jobs or departments, it's simple to lose track of administrative privileges. Keep track of who has access to what information or resources. One compromised account with unnecessary access to sensitive data may serve as an easy entry for bad actors. Additionally, physical access to server rooms, datacenters, or admin rooms can be monitored via access control.

Password hygiene

User credentials were involved in more than half of all breaches in 2021.[10] Passwords still serve as a primary mode of defense against data theft. Use lengthy passwords that combine uppercase, lowercase, number, and symbol characters. Never repeat passwords, and use discretion when typing them. Combine your passwords with additional forms of authentication to make it more challenging for someone to get unwanted access.

Authentication

Authentication is the process of verifying that a user or device is who or what they claim to be. It's a critical part of cyber hygiene, and organizations can choose from various types of authentication. The most obvious authentication method is a username and strong password or PIN. Another foolproof option is multi-factor authentication (MFA), where one-time codes are generated to the user's phone or email address. It is a tried-and-true method of enhancing security because it denies access to hackers that may have just your login credentials. Biometric authentication uses biological identifiers, such as facial or fingerprint recognition. Other types of authentication include certificate-based, token-based, and single sign-on.

Patch management

Unpatched vulnerabilities are the primary attack vectors that ransomware groups use to access weak networks.[11] On any personal devices used for work as well as any company-owned devices, keep software upgraded with security patches. Using a specialized tool like Endpoint Central, you can identify missing patches and deploy them to all endpoints in your network without any manual intervention.

A dedicated cybersecurity team

Even though cybercrimes are fought with technology, there are people behind the fight. It is important to build up a team of professionals who are equipped and trained to tackle the threats of today. In general, outsourcing is the more cost-effective and useful option for SMBs. But smaller organizations should consider allocating a budget to building a cybersecurity team that can continually probe the security state of the network.

Incident response plan

Create an incident response plan, then implement it as necessary. Conduct reviews following every incident or simulation to inform your staff, strengthen your network, and enhance future responses. Last but not least, evaluate the success of your network's ability to sustain digital resilience using metrics that track more than just how busy your cyber teams are, but also measure their effectiveness.

Modern endpoint protection tool

Any software can be weaponized. Take malware, which is written using the same language as a useful software, but with malicious intent. Malware today can cause serious damage like data leaks or network breakdowns. Since endpoints are the easiest entry points for attackers, businesses must have robust endpoint protection in place. With Endpoint Central, SMBs can monitor and protect their endpoints while keeping costs down. For small enterprises with less than 50 endpoints, this software is absolutely free of cost.

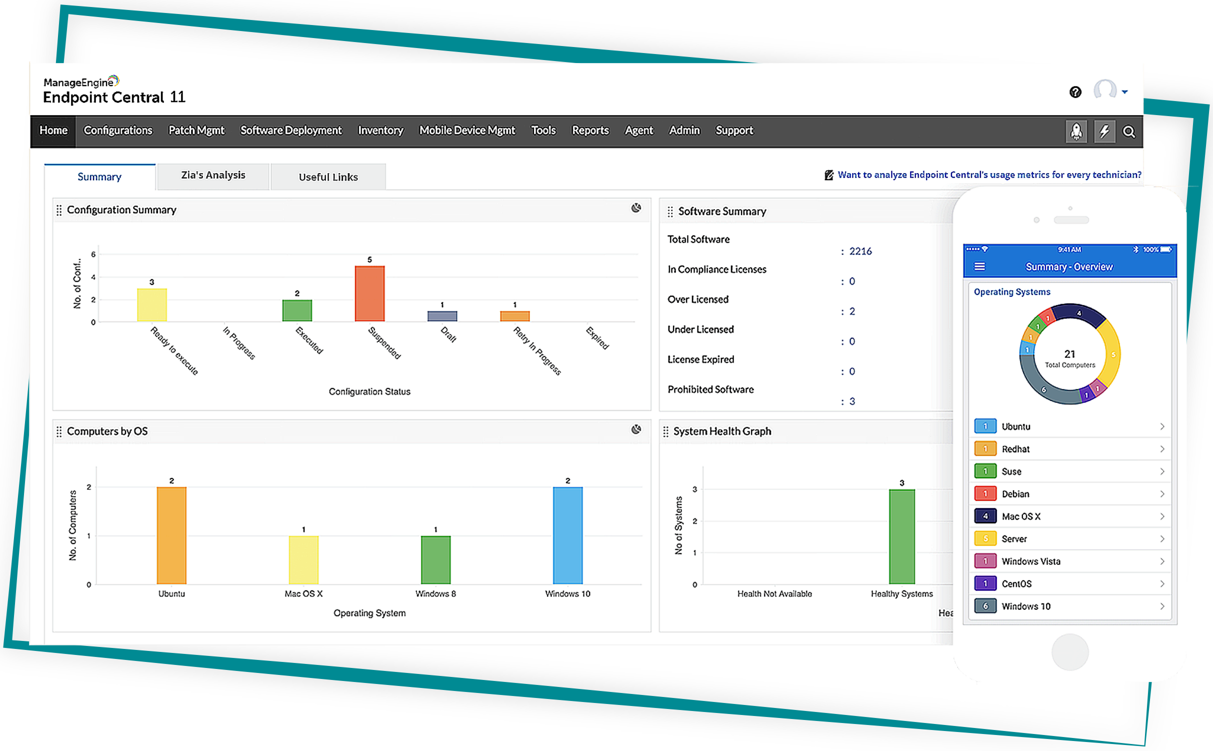
The tool SMBs love using

In a Cisco survey, 95% of SMBs admitted to not having the right technology solutions to detect a cyber attack or threat in their network. Many felt that there were too many technologies, which they struggled to integrate.

We agree! Using an endpoint protection solution should not come at the cost of having to deal with 10 different types of software, which may not even be compatible with each other. This is where Endpoint Central can help. It has the capabilities of 10 different software in one. Endpoint Central not only helps you get real-time visibility for both physical and digital assets, but also helps you manage your endpoints right from onboarding to retirement, across hybrid workspaces and highly heterogeneous OS ecosystems—all from a single console!

Endpoint Central is loved by SMBs because of its extreme affordability, wealth of functionality, and easy-to-use design. It also does not require extensive coding skills, which makes it perfect for organizations who cannot afford to employ IT specialists. Using this software will also help you prepare for compliance with regulatory standards. Recognition from IDC, Gartner®, and Forrester year-on-year validate the fact that Endpoint Central is doing things right!

VISIT ENDPOINT CENTRAL PAGE



Total Software : 2216

In Compliance Licenses : 0

Over Licensed : 2

Under Licensed : 0

License Expired : 0

Prohibited Software : 3

1	Ubuntu
1	Redhat
1	Suse
1	Debian
4	Mac OS X
5	Server
1	Windows Vista
1	CentOS
6	Windows 10

Try the fully functional product for free

GET FREE TRIAL

" Endpoint Central has helped us to manage our patch updating in a central location. As well as push out new software and hardware from one location. Yes the deployment is virtually unnoticeable to the end user and the cost per user/pc is very low. We are a small IT team and it has automated a lot of the smaller tasks so that the staff can do other things. Cost, ease of deployment and features for the money "

Richard Pasley,
IT Systems Specialist, Alabama Board of Nursing

Explore the no-effort demo server

TRY ONLINE DEMO

Recognized by

References

1. Verizon, 2022 Mobile Security Index Report

2. Security.org, Public Awareness of Major Data Breaches

3. IBM, Ponemon Institute, Cost of a Data Breach Report

4. Cisco, Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense

5. The World Bank, Small and Medium Enterprises Finance

6. Inc., 60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack

7. Ransomware Task Force, Combating Ransomware

8. Verizon, 2022 Data Breach Investigations Report

9. Centrify, Privileged Access Management in the Modern Threatscape

10. Verizon, 2021 Data Breach Investigations Report

11. Ivanti, Ransomware Spotlight Year End 2021 Report