CROWDSTRIKE

CrowdStrike eBook

Small Business Cybersecurity Survival Guide

Learn about the most common types of cyberattacks, assess your organization's cyber risk and take four important steps to stop breaches

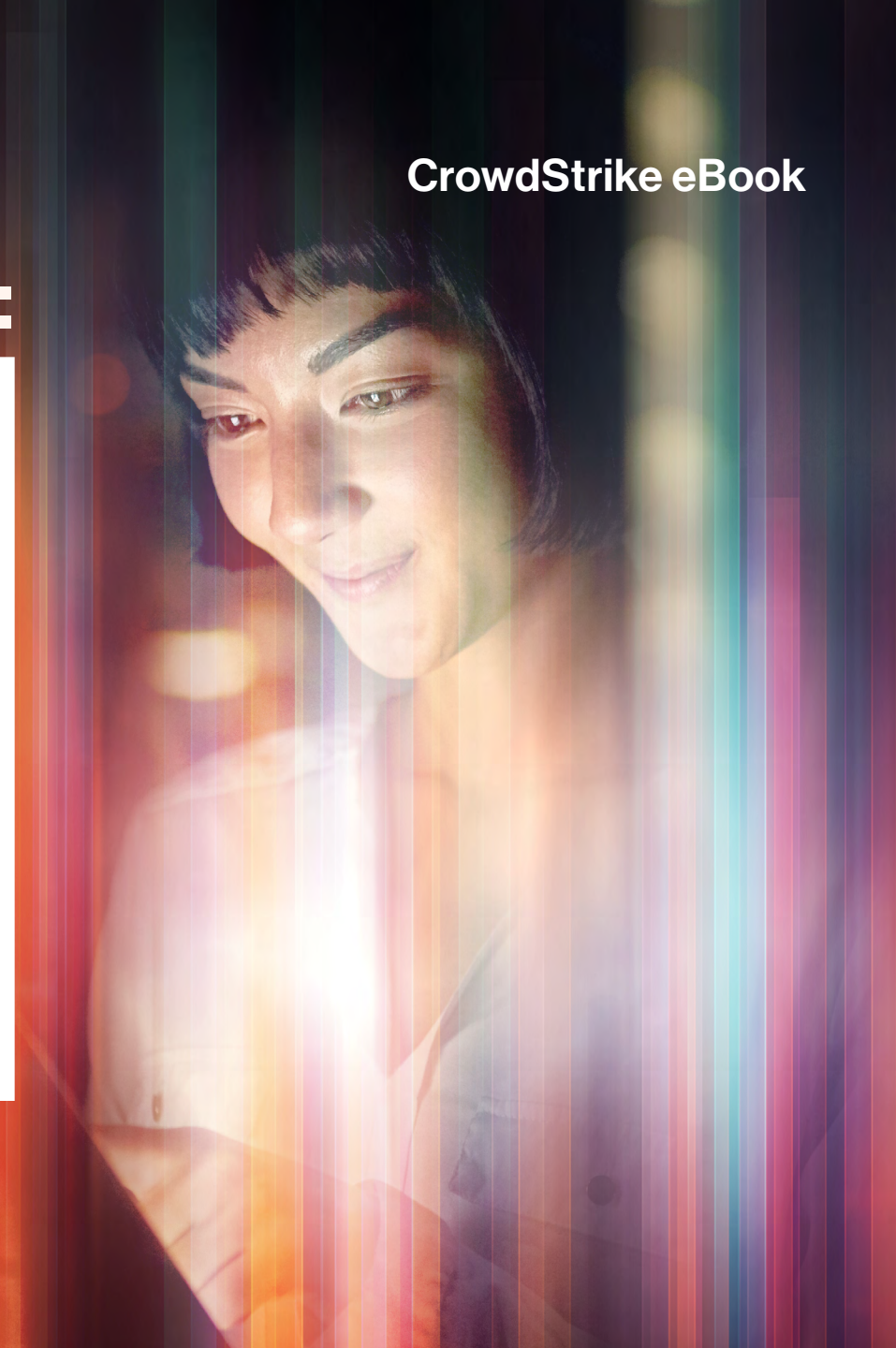


Table of Contents

Small Businesses Are Targets of Opportunity 3

SMB Cybercrime by the Numbers 4

How Modern Cyberattacks Evade Legacy Tech 5

Four Steps to Protect Your Business from Modern Cyberattacks 6

- **Step 1:** Understand the Reality of Cyberattacks 6
- **Step 2:** Implement Basic Cybersecurity Hygiene Practices 7
- **Step 3:** Train and Continuously Test Employees 9
- **Step 4:** Invest in Modern Endpoint Protection 9

Overcoming Limited Resources and Expertise 10

Complete Protection, Managed for You 10

Confidence that You'll Stay Breach-Free 12

Small Businesses Trust CrowdStrike to Keep Them Secure 13

Protect Your Business with CrowdStrike Falcon Complete 15

Small Businesses Are Targets

It's easy to assume cybercriminals only target major enterprises. These large organizations have mountains of valuable and sensitive data across their environments and critical operations that, if disrupted or taken down, can result in millions of dollars in lost revenue and reputational damage.

But while breaches of large organizations make news headlines, small and medium-sized businesses (SMBs) are also at risk. An SMB often lacks a dedicated cybersecurity team, and it may not have the modern cybersecurity software, skills or resources to protect itself. And SMBs, like larger businesses, also hold valuable, sensitive data such as employee and customer records, financial transaction information, intellectual property and access to business finances and larger networks critical to their success.

Cybercriminals recognize both the vulnerability and value of SMBs, viewing them as easy prey ripe for compromise, ransomware and data theft. As governments and organizations around the globe increase funding for cybersecurity, the market and regulatory pressure to avoid the spotlight continues to mount, making SMBs ideal targets for various threat actors and cybercriminal organizations.

Cyberattacks come in many forms:

from ransomware and phishing attacks, to the theft of sensitive data such as intellectual property and personal information.

SMB Cybercrime by the Numbers

Cyberattacks always carry significant consequences, but to SMBs they can be devastating. In 2021, IBM found the average cost of a data breach to a small business was $2.98 million USD.[1] Such impact can be more than enough to end the life of a company.

- In 2019, SMBs represented 43% of all data breaches[2]
- 50% of SMBs lack the resources or tools necessary to protect their business 24/7[3]
- 61% of small businesses experienced a breach in the last year[4]
- 70% of ransomware attacks in 2021 hit businesses with <500 employees[5]

Cyberattacks come in many forms, from ransomware and phishing attacks, to the theft of sensitive data such as intellectual property and personal information of employees and customers.

Below are some of the common attacks cybercriminals use to gain access and compromise your systems and data:

- **Malware:** Malicious programs and code developed by attackers to manipulate or otherwise compromise computer systems, networks, applications and data.
- **Malware-free attacks:** Fileless infections that don't write anything to disk and use built-in tools to move laterally and compromise your environment.

1 Cost of a Data Breach 2022: A Million-Dollar Race to Detect and Respond

2 CNBC Main Street Overconfidence: America's Small Businesses Aren't Worried About Hacking

3 2022 Study: 50% of SMBs Have a Cybersecurity Plan in Place

4 Verizon 2022 Data Breach Investigations Report

5 IST Ransomware Taskforce, Blueprint for Ransomware Defense, August 2022

According to the 2022 Falcon OverWatch Threat Hunting Report,

71%

of breaches forgo malware entirely to evade legacy antivirus software searching for known file- and signature-based malware.

- **Vulnerabilities:** Weaknesses in systems and applications that cybercriminals exploit to gain unauthorized access to a computer system.
- **Phishing:** Primarily email-based scams that impersonate credible people and organizations to steal credentials or sensitive information.
- **Compromised credentials:** Stolen identity and account data (e.g., username and password) used to access systems and networks masked as legitimate users and perform various attacks.
- **Insider threats:** Employees who wittingly or unwittingly misuse, harm or otherwise exploit critical systems, networks or data.
- **Zero-days:** Previously unknown vulnerabilities and exploits that attackers leverage in planned and targeted attacks.

How Modern Cyberattacks Evade Legacy Security Technology

While many small businesses are familiar with malware and may have installed antivirus to combat such attacks, cybercriminals are evolving their strategies to bypass traditional security tools. Now, many employ human-engineered methods to break into businesses of all sizes.

According to the **2022 Falcon OverWatch Threat Hunting Report**, 71% of breaches forgo malware entirely to evade legacy antivirus software searching for known file- and signature-based malware.

This finding underscores how criminals are using increasingly sophisticated and stealthy techniques tailor-made to evade autonomous detections like those produced by antivirus software.

Once inside the network, cybercriminals can begin moving laterally across your systems and infrastructure, compromise your systems, and exfiltrate your data.

Once inside the network, cybercriminals can begin moving laterally across your systems and infrastructure, allowing them to compromise your systems and exfiltrate your data in the following ways:

- **Data theft:** When an attacker extracts and then sells valuable employee data or intellectual property.
- **Ransomware:** A type of malware that disables access to your system and data until a ransom is paid.
- **Extortion:** When an attacker extracts and threatens to expose sensitive information on the internet unless the victim makes an extortion payment.
- **Hacktivism:** Intrusion activity undertaken to gain momentum, visibility or publicity for a cause or ideology.

Four Steps to Protect Your Business from Modern Cyberattacks

Step 1: Understand the Reality of Cyberattacks

MYTH 1: Cyberattacks come from amateur hackers.
FACT: Malicious hackers are highly organized, disciplined and specialized cybercriminals who act fast.

MYTH 2: Cybercriminals don't care about my data.
FACT: Small businesses don't fly under the radar of cybercriminals. Sensitive data is valuable, regardless of company size. Moreover, SMBs often lack modern cybersecurity technology and personnel, making SMBs quick and easy targets for attackers.

MYTH 3: Antivirus and a firewall will protect my SMB from cyber threats.
FACT: Antivirus is designed to identify and stop viruses and malware; however, it's incapable of detecting and stopping sophisticated techniques employed by today's attackers. For example, traditional antivirus solutions won't detect attacks that are malware-free or that involve the use of valid identity credentials that have been stolen. Cybersecurity tools are a major component of an effective defense, but you also need mature processes and people to run them.

MYTH 4: I'll know if I've been breached.
FACT: Ultimately, yes, at some point this is true, you will know you were breached. But it could take weeks or even months before you know you've been hit. IBM's **Cost of a Data Breach Report** found that it takes an average of 212 days to identify a data breach and an average of 75 days to contain it. And the longer cybercriminals linger in a target environment, the more damage they can inflict.

MYTH 5: My company will bounce back after an attack.
FACT: The process of recovering from a data breach is arduous.

Factoring in business downtime, decreased profitability, legal fees and more, severe attacks can even cause small businesses to shut down for good.

Step 2: Implement Basic Cybersecurity Hygiene Practices

The following practices don't cost any money and can have a huge impact on helping build up your defenses.

- **Create a strong password policy:** Never share passwords or use the same password for multiple applications, cloud apps or servers. Managing passwords will allow you to watch for suspicious behavior and shut down access if needed.

- **Enforce multifactor authentication (MFA):** MFA requires a password and a token to access your critical applications, adding an important layer of protection. Google, Symantec and Microsoft all offer free authentication tools and seamlessly connect popular apps.

- **Perform regular backups of critical data:** Whether on-premises or in the cloud, having a backup of your data will help you recover faster in the event of a breach. However, your backups could be encrypted if criminals have had access to your systems without your knowledge. While backups are essential, it's far more important to establish a resilient defense up front.

- **Keep current with software patches and security updates:** Many of the biggest breaches have started with exploited vulnerabilities. With the proliferation of open source and cloud applications, updating software is critical to ensure you are not the next victim of a major breach. The **U.S. Cybersecurity and Infrastructure Security Agency** (CISA) provides an updated list of all known exploited vulnerabilities.

- **Lock down your cloud environments:** Protect your cloud drives (such as Box or Google Drive) by implementing MFA and adhering to the principle of least privilege, which ensures employees only have access to the resources they need for their jobs.

- **Implement and test your threat detection and response**: Make time to analyze your environment and user behaviors for malicious or abnormal activities. Stay current on threat actors, tradecraft and indicators of attack. Define, document and test what a successful incident response looks like.

- **Secure your network:** Create a private VPN and keep your WiFi secure and hidden. Make sure to look for suspicious behavior and access points. This is essential for any business with remote employees and should be available at no additional charge from your internet service provider.

Step 3: Train and Continuously Test Employees

Educate your employees: Your entire workforce should be aware of the types of security threats and social engineering attacks they face at work, such as phishing, smishing, honey trapping and more. For definitions and tips, check out **10 Types of Social Engineering Attacks**.

Test and evaluate your employees' ability to identify fraudulent messages: Many breaches start with an employee falling for the bait of a phishing attack. Teaching your employees how to identify suspicious emails, URLs, text messages and other phishing signs is critical to preventing a breach.

For more guidance, visit **How to Create a Cybersecurity Awareness Training**.

Step 4: Invest in Modern Endpoint Protection

Endpoint protection platform (EPP) software offers modern security tools to protect **endpoints** — including computers, mobile devices, servers and other connected devices — from known and unknown threats and vulnerabilities.

Endpoint protection provides many security benefits, such as:

- Real-time, end-to-end visibility
- Improved threat detection and resolution
- Enhanced efficiency and improved outcomes

EPP has become an imperative component of stopping breaches for businesses and can also help achieve cyber insurance initiatives.

Managed detection and response (MDR)

MDR is a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring and response.

According to Gartner, by 2025, 50% of organizations will use MDR services for threat monitoring, detection and response functions.

Overcoming Limited Resources and Expertise

While EPP solutions provide autonomous protection, they still require a dedicated team to set policies and monitor, respond to and stop attacks.

Many small businesses simply don't have the budget or time to find, staff and pay for these resources 24/7. If this sounds like you, a managed detection and response (MDR) solution may be the best fit for your business.

MDR is a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring and response.

Complete Protection, Zero Uplift

CrowdStrike Falcon Complete™, CrowdStrike's industry-leading MDR service, provides all of the benefits of endpoint protection and antivirus, fully managed by a staff of dedicated security experts. The service delivers an effective and mature security program without the difficulty, burden and costs associated with building it internally.

With quick deployment and immediate expansion of your security team, impact is felt in days, not months. Gain actionable insights and consistent reporting for an immediate ROI.

- Saves over 2,500 hours per year from a reduction in security incidents[6]
- Provides the equivalent of five expert operations center analysts and five elite human threat hunters[6]

6 Total Economic Impact of Falcon Complete, February 2021 Forrester Wave for Managed Detection and Response, Q1 2021

Falcon Complete Expertise
Provides expert security analysts to manage, monitor, respond to and remediate threats

Falcon Discover™: IT Hygiene
Provides visibility into assets, systems and applications for a comprehensive topography of your IT environment

Falcon Prevent™: Next-gen AV
Provides the ideal AV replacement solution by combining the most effective prevention technologies with full stack visibility and simplicity

Falcon Insight XDR™: Detection and Response for Endpoint and Beyond
Delivers continuous, comprehensive endpoint visibility that spans detection, response and forensics to ensure nothing is missed and potential breaches are stopped

Falcon OverWatch™: Managed Threat Hunting
Adds a human threat detection engine that operates as an extension of your team, hunting relentlessly to see and stop the most sophisticated hidden threats

Falcon Identity Threat Protection™
Enables hyper-accurate threat detection and real-time prevention of identity-based attacks by combining the power of advanced AI, behavioral analytics and a flexible policy engine to enforce risk-based conditional access

"Falcon Complete lets me sleep far better at night."

Customer
Forrester TEI Report

Confidence that You'll Stay Breach-Free

The **2022 Falcon OverWatch Threat Hunting Report** found it only takes an average of **1 hour 24 minutes** for cybercriminals to break into your systems.

With Falcon Complete, you'll have the confidence that experts are on the job with 24/7 threat hunting, monitoring, responding and remediating to keep your business breach-free.

We stand behind our mission to stop breaches. Falcon Complete is backed by a unique breach prevention warranty that covers breach response expenses for a security incident within the protected environment.

"Partnership is part of my DNA and I see CrowdStrike as a true and trusted partner. CrowdStrike is an extension of my team and one that is so efficient and advantageous, I don't need to contact it every day. I trust that CrowdStrike is making sure our business is supported and protected."

Azunna Anyanwu
CTO, Aronson, LLC

Small Businesses Trust CrowdStrike to Keep Them Secure

Company: Aronson, LLC
Industry: Financial Services
Number of Endpoints: 350

Challenges:

- Cyberattacks are increasing in volume and sophistication
- The company had a diverse mix of legacy IT, business systems and applications
- Existing security tools and products don't support integrated endpoint security
- Small IT and security team

Solution:

Aronson uses the CrowdStrike Falcon platform and managed services (Falcon Complete) to mitigate security threats and protect highly sensitive data held and managed on behalf of its government, business and public sector clients.

Business Outcomes:

- 90% decrease in time spent resolving cyber threats
- 75% reduction in time spent on security operations
- The solution deploys in less than two weeks, with no impact on users

Read the full case study here: **Aronson LLC Case Study**

"CrowdStrike performed as if I had someone onsite 24/7 monitoring our assets all the time, even at three o'clock in the morning. It gives me the ability to go home and relax."

Rusty Haferkamp
CISO, Central National Bank of Waco

Company: Central National Bank of Waco
Industry: Bank
Number of Endpoints: 200

Challenges:

- Reactive, labor-intensive cybersecurity strategy
- Manual threat management
- High cost of cybersecurity services

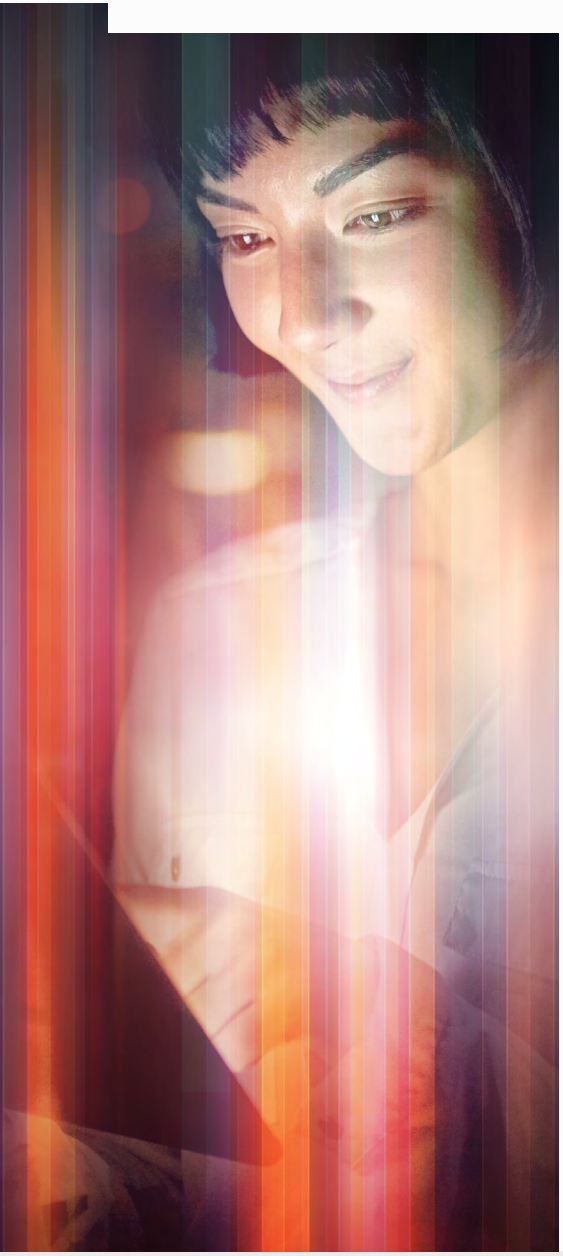
Solution:

CrowdStrike Falcon Complete managed detection and response ensures customer data is protected by cloud-delivered, next-generation endpoint protection.

Business Outcomes:

- Improved visibility into security operations
- Facilitated compliance and auditing operations
- Instilled confidence in customers' asset protection
- Reduced mitigation time from two days to seconds

Read the full case study **here**.



Protect Your Business with CrowdStrike Falcon Complete

Speak with our small business security experts about what's right for you.

Attribution: Gartner, Market Guide for Managed Detection and Response Services, Pete Shoard, Craig Robinson and others, October 25, 2021.

Speak with an Expert →

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**