CROWDSTRIKE

CYBERSECURITY FOR SMALL BUSINESSES:

PROACTIVE SOLUTIONS THAT MEET YOUR NEEDS

Introduction

If you're shopping for a cybersecurity solution for your small business,

you already know you're not immune to ransomware and other sophisticated threats. In fact, cybercriminals exploit crises and change. Cyberattacks have steadily increased, especially in recent years with the COVID-19 pandemic and ongoing global tensions.

In 2021, cybersecurity proved to be an important issue:

82%

increase in ransomware-related data leaks[1]

57%

of IT teams who experienced a ransomware attack didn't have a response strategy in place[2]

62%

of attacks comprised non-malware, hands-on-keyboard activity[3]

60%

of organizations reported a cybersecurity staffing shortage is placing their organizations at risk[4]

Hands-on-keyboard activity occurs during a compromise when a hacker is already inside, silently dwelling in an environment. The adversary types commands in real time to cautiously move laterally across the network, jumping between accounts, elevating privileges and ultimately looking for critical data to monetize for ransom.

1. https://www.crowdstrike.com/global-threat-report/
2. https://www.crowdstrike.com/resources/reports/global-security-attitude-survey-2021/
3. https://www.crowdstrike.com/global-threat-report/
4. https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

Cybercriminals are constantly improving and diversifying their exploits. Small businesses can't afford to use reactive approaches that require reboots, on-premises management and waiting for a blatant threat to appear — and they may not have the skilled staff required to detect and stop today's sophisticated, stealthy attackers before damage is done.

Today's constantly evolving cyber threats require a cloud-based, proactive solution that can detect even the slightest hint of activity before it turns into a breach.

This guide was created to help you choose the best proactive cybersecurity solution for your needs, so you can feel safer and keep up with a changing threat landscape.

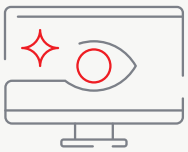
You'll gain a better understanding of the types of cyber threats your business might face, and how to make the best decisions when it comes to cybersecurity.

Look for the following capabilities when evaluating a cybersecurity platform:

Antivirus protection that proactively detects known and unknown malware threats and analyzes trusted behaviors

Endpoint detection and response to prevent modern threats like file-based and fileless malware attacks and malicious activity, and to provide investigation and remediation capabilities

Managed threat hunting from a team of real people to elevate detection beyond automation



IT hygiene to prepare and strengthen the environment before an attack occurs

Antivirus Protection

Antivirus solutions have changed a lot over the years.

Traditional antivirus software was designed to reactively detect, prevent and remediate known malware infections on individual systems or computers. As security breaches and ransomware continue to evolve, legacy antivirus has stayed the same.

Next-generation antivirus (NGAV) proactively protects against evolving cyber threats such as **polymorphic malware** with one solution, even when offline. It uses a combination of tactics so both known and unknown threats can be anticipated and immediately prevented. As adversaries diversify their strategies, NGAV evolves with them without slowing you down.

Polymorphic malware is a type of malware that constantly changes its identifiable features to evade detection. Common forms include viruses, worms, bots, trojans and keyloggers.

Reactive Antivirus

- Relies on signatures, which are hard to update and ineffective against fileless attacks, making it unable to protect your devices against new, emerging threats
- Requires scans, updates and reboots, which consume high percentages of resources and slow down devices
- Takes weeks to months to implement, depending on how many devices you need to protect

Proactive Antivirus

- Uses a combination of artificial intelligence, behavioral detection, machine learning algorithms and exploit mitigation, enabling protection of your devices from the latest emerging threats
- Uses a cloud-based architecture that does not impact endpoint performance or require additional hardware or software, so it will not slow down your devices
- Takes only hours to implement, no matter how many devices you need to protect

The ideal antivirus solution should:

- ☑ Use a cloud-based infrastructure to ensure quick installation, always-on protection, little to no impact on **endpoints** and no reboots required after installation
- ☑ Use powerful methods like artificial intelligence (AI) to prevent against modern tactics, techniques and procedures (TTPs) that make cyberattacks successful
- ☑ Protect against commodity malware, zero-day malware, exploits, and fileless and malware-free attacks
- ☑ Have the ability to quarantine malicious files
- ☑ Use **machine learning (ML)** on the endpoint for pre-execution prevention of both known and unknown malware
- ☑ Provide protection across across operating systems and OS versions
- ☑ Submit quarantined files to sandbox for automatic analysis

Endpoints are any physical device that can be connected to a network, including computers, laptops, mobile phones, tablets and servers.

Machine learning (ML) is a branch of artificial intelligence (AI) and computer science that uses data and algorithms to imitate the way that humans learn, gradually improving its accuracy and servers.

Endpoint Detection and Response

The most important aspect of cybersecurity is visibility.

You need insight into activity in your environment, devices, files and important internal data. You can't stop what you can't see, and endpoint security is the eyes and ears of your environment.

Endpoint detection and response (EDR) provides the information you need to uncover attackers as quickly as possible. Think of EDR as a security camera that gives you visibility into the virtual environment of your business. A proactive EDR solution should not provide just a "motion sensor" type of view, but high-quality visibility that gives you continuous forensic context of everything happening in your environment.

EDR solutions that use cloud-native architecture should be able to quickly collect and retain all of the necessary endpoint events, even if endpoints are unavailable, destroyed or have been deleted.

They provide both real-time and historical information that helps you resolve incidents quickly. This approach stops attackers before they do damage, essentially eliminating the risk of **silent failure**.

EDR is seen as one of the most important aspects of cybersecurity because of the data and context it provides. Many cybersecurity insurance providers will not allow businesses to renew their policies if they don't have an EDR solution in place.

Endpoint detection and response (EDR) is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats such as ransomware, malware and fileless attacks. It also provides remediation suggestions to restore affected systems.

Silent failure happens when an adversary is able to dwell in an environment for an extended period of time — normally up to 200 days.[5]

5. https://www.crowdstrike.com/blog/prevention-continuum-preventing-silent-failure/

The ideal EDR solution should:

- ☑ Deliver real-time and historical endpoint visibility that both detects and prevents advanced threats as they happen, without requiring users to write and fine-tune detection rules
- ☑ Use a **ZeroTrust** framework to analyze behavior in the environment and address securing remote workers, hybrid cloud environments and ransomware threats
- ☑ Integrate with threat intelligence to enrich detected events and incidents so security operations teams can more effectively detect threats and make better, faster decisions

Zero Trust is a security framework that requires all users, in or outside the organization's network, to be authenticated, authorized and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes there is no traditional network edge; networks can be local, in the cloud or a combination or hybrid with resources and workers in any location.

Managed Threat Hunting

In 2021, the majority of successful cyberattacks were done by adversaries who used stolen credentials instead of writing malware to the endpoint.[6]

These adversaries were able to dwell in environments for days, weeks or even months, which gave them time to access information about real accounts. This is why proactive threat hunting is a must if you're looking to achieve or improve real-time threat detection and incident response.

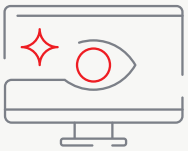
Managed threat hunting provides an essential human element that ensures nothing gets missed. It plays a critical role in the early detection of attacks and adversaries. It uses a proactive, expert-led approach that continuously searches for suspicious activities and dwellers rather than relying on automatic detections and alerts.

Unfortunately, a lack of resources and a shortage in security expertise makes proactive threat hunting unattainable for a majority of small businesses, who are unable to monitor 24/7 for adversary activity. Longer investigation times with fewer alerts being handled quickly enough ultimately result in longer dwell times and a bigger chance that attackers will be successful.

The ideal managed threat hunting solution should:

- ☑ Provide an elite hunting team of cybersecurity experts
- ☑ Proactively find and analyze malicious activities that automated security systems could miss
- ☑ Provide users with thorough, expedited response guidelines

6. https://www.crowdstrike.com/global-threat-report/



IT Hygiene

True security starts with closing gaps to effectively face threats. This requires understanding which systems and applications are vulnerable and who and what are active in your environment.

That's where vulnerability management and IT hygiene come in. They provide the actionable information businesses need to implement preemptive measures and make sure they are prepared to face today's evolving, sophisticated threats.

Knowing who and what is on your network can help address unknown elements or gaps within your security architecture. IT hygiene solutions offer the ability to pinpoint unmanaged systems or those that could be a risk on the network, such as unprotected "bring your own" devices (BYOD) or third-party systems. This solution should also be continuously monitoring for changes within your assets, applications and users.

An effective IT hygiene solution should:

- ☑ Provide robust visibility over the existing vulnerabilities, assets, applications, usage trends and accounts in the environment, all without impacting endpoints
- ☑ Display real-time visibility into who and what is in the network and can identify rogue, unprotected and unmanaged systems, such as BYOD or third-party systems
- ☑ Show logon trends (e.g., activities, duration) across your environment, wherever existing credentials are being used or new administrator credentials are created
- ☑ List all applications being used on a specific endpoint and across all of the endpoints in the environment
- ☑ Not require a network scan or additional sensors

The CrowdStrike Approach

CrowdStrike offers a proactive approach to cybersecurity in critical areas including NGAV, EDR, managed threat hunting and IT hygiene that save businesses time, resources and money. With a single-agent solution that stops breaches, ransomware and cyberattacks, CrowdStrike protects the people, processes and technologies that drive modern business.

As long as you have a **CrowdStrike Falcon®** sensor deployed, you are part of the "Crowd" in CrowdStrike that benefits from community immunity from cyber threats. All of the data **CrowdStrike** sees from customers, including the latest threat indicators and techniques, contributes to your protection.

Award-Winning Protection

FORRESTER®

Forrester recognized that CrowdStrike **"offers superior endpoint security with a cloud-native architecture."** [7]

Gartner®

CrowdStrike Named a Leader in the Magic Quadrant for Endpoint Protection Platforms. [8]

IDC

CrowdStrike Ranked #1 for Modern Endpoint Security 2020 Market Shares [9]

7. https://www.crowdstrike.com/press-releases/crowdstrike-named-a-leader-in-endpoint-security-software-as-a-service/
8. Magic Quadrant for Endpoint Protection Platforms, 5 May 2021
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
9. IDC, Worldwide Corporate Endpoint Security Market Shares, 2020: Pandemic and Expanding Functionality Propelled Market Growth, doc #US47768021, June 2021

Helping Businesses at Every Level

Compared to other products the best part is during the deployment stage. It is light weight and takes only a matter of seconds and there is no need to run a server as everything is managed by CrowdStrike on the cloud. Deployment for a device takes less than five minutes and works like a charm."

Administrator, Education Management

Gartner Peer Insights™

"I have been impressed with its features and the convenience with which the agents may be installed without disrupting operations. We were able to save a significant amount of money by cutting a number of expenses on Infrastructure Maintenance."[10]

Program and Portfolio Manager, Consumer Goods Industry

Gartner Peer Insights™

"I am very happy with the CrowdStrike Falcon sensor since moving to from our previous anti-virus software, their suite is very easy to use and it was a seamless integration into every device we needed protection for."[10]

Analyst, Professional Services Industry

10. Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.
https://www.gartner.com/reviews/market/endpoint-protection-platforms/vendor/crowdstrike/product/falcon/review/view/4161130
https://www.gartner.com/reviews/market/endpoint-protection-platforms/vendor/crowdstrike/product/falcon/review/view/4288626

Choose the Right Product For Your Business

Falcon Go

Build Your Security Strategy

This is the perfect starting point for your security strategy with scanless, proactive antivirus protection, along with visibility and granular control over USB devices in your environment.

What You Get:

- Next-generation antivirus
- Device control

Falcon Pro

Optimize Your Defenses

Falcon Pro provides superior protection from cyberattacks, detects malicious activity, and offers immediate response capabilities for your small business.

What You Get:

- Next-generation antivirus
- Device control
- Integrated threat intelligence
- Firewall management

Falcon Enterprise

Assess the Attack

Increased data visibility and threat response from automated detections and real experts enables you to detect and stop breaches faster.

What You Get:

- Next-generation antivirus
- Device control
- Integrated threat intelligence
- Firewall management
- Endpoint detection and response
- Threat hunting

Falcon Premium

Fortify the Business

Enhanced visibility allows you to prepare for an attack before it occurs by revealing areas of exposure that you otherwise wouldn't see.

What You Get:

- Next-generation antivirus
- Device control
- Integrated threat intelligence
- Firewall management
- Endpoint detection and response
- Threat hunting
- IT hygiene

CrowdStrike Services
Express Support — **Included With All Bundles**