Choosing a cyber security solution

Your guide to getting it right

FIELD EFFECT™

What we believe

No matter the size of your business or the industry you work in, your company is a target for cyber criminals. It's more important than ever to have effective defences in place — but cyber security can be an overwhelming topic.

That's why Field Effect exists.

We believe all businesses deserve powerful, cost-effective, and easy-to-use cyber security to protect their operations from cyber threats. Regardless of your security knowledge, resources, or budget, cyber security should be approachable and attainable for you.

But with so many products and vendors to choose from, where do you start?

We created this eBook to highlight the challenges facing businesses like yours as they try to find cyber security solutions that deliver the defences they need.

More than anything, we want to stop cyber criminals from hurting businesses and people like you. We've got your back. If you have any questions, or if there's anything further we can do to help, please reach out.

Table of Contents

FIELD EFFECT™

Introduction

No two businesses are exactly alike, which means that, much like Goldilocks, too many organizations are stuck sorting between countless cyber security solutions to find one that's just right.

As companies scale their operations, staying ahead of these changes is hard and time-consuming, but it remains a critical necessity to ensure operations remain secure — which is easier said than done.

The good news is that a bit of knowledge goes a long way. After all, as a certain Saturday morning cartoon taught us, "Knowing is half the battle." When you understand what it is you're trying to protect, it becomes much easier to choose the right cyber security solution for your business.

Determining which option will best serve your business as it grows is challenging. You need one that will deliver effective, efficient defence without taking more time out of your already busy day.

Evaluating cyber security solutions for your company

Organizations everywhere are using a growing number of tools[1] to secure their operations, data, and workers — and it's causing problems. The sheer volume of technologies and solutions may introduce serious complexity, both in terms of IT budget and the time needed to manage and integrate each individual tool.

As a result, IT teams and Chief Information Security Officers (CISOs) are facing unprecedented challenges. Organizations with large tech stacks frequently struggle to detect and respond to an attack,[2] compared to those with fewer tools to manage. What's more, used in isolation, many of these tools can create silos that make it harder to get a handle on security issues.

UNDERSTANDING WHAT TOOLS ARE COMMONLY USED AND WHAT FUNCTIONALITIES THEY PROVIDE IS VITAL FOR NAVIGATING TECH STACK COMPLEXITY.

Breaking down the cyber tech stack: common tools and solutions

01 Antivirus (AV)

Antivirus (AV) software is a host-based solution that looks for attributes of known malicious code. Once deployed, AV attempts to stop attackers from compromising your organization's endpoints and servers, traditionally using signature-based detection[3] to keep the host secure with regular system scans. When AV software finds a match, it attempts to quarantine or remove the infected code. Modern AV, sometimes referred to as next-generation AV, focuses on threat activity instead of digital code in a process known as heuristic detection, attempting to spot the irregular behaviour typical of malware.

AV is one of the most recognizable cyber security tools. It dominated the industry throughout the 1990s through to the early 2000s when malware developers came up with new ways to evade detection methods. When used alone or as the core tool in a stack, AV software often lacks the comprehensive functionality needed to address the many threats businesses face.

02 Security information and event management (SIEM)

Security information and event management (SIEM) software is a tool that collects, processes, and centralizes security-related data from multiple sources, compiling it into a single dashboard. SIEMs are designed to simplify how a security team analyzes information, identifies suspicious events, and responds to incidents. It accomplishes this by deploying agents on systems, applications, devices, and other security tools, collecting and processing data before surfacing it in a dashboard.

SIEMs rely on curated rules to help the system identify suspicious activity. When anomalous activity is detected (such as multiple failed password attempts or other irregular user behaviour), it generates an alert on the system's dashboard. While log-based SIEMs offer powerful monitoring capabilities, they can be costly and difficult to maintain, especially for smaller businesses, and the sheer volume of data and alerts generated can be overwhelming for IT teams stretched thin.

03 Endpoint detection and response (EDR)

Endpoint detection and response (EDR) works by installing agents on endpoint devices to collect data and forward it to a centralized platform for analysis. This allows for greater visibility into the processes, connections, and activity occurring on endpoint devices, allowing EDR to detect signs of suspicious behaviour and respond accordingly.

Though powerful, EDR activity still requires analysis by a security team. Because these solutions generate a significant amount of information and alerts, managing EDR solutions can be a time-consuming process for even highly experienced security personnel. What's more, these tools may create security gaps unless used in tandem with a solution that protects your entire IT infrastructure.

04 Security orchestration, automation, and response (SOAR)

Security orchestration, automation, and response (SOAR) solutions are a response to increasingly complex tech stacks. SOAR platforms attempt to integrate often incompatible tools by establishing communication between disparate technologies, coordinating messy tech stacks and establishing better processes for security teams. They also aggregate activity and threat data from multiple sources and automate certain operational tasks,
even providing incident response.

These solutions use "playbooks" — organizational workflows outlined step by step — to carry out security-related tasks. By automating simple jobs, such as quarantining low-level threats from devices, removing malware, or disabling access to compromised accounts, SOAR solutions attempt to free up a team's time. Unfortunately, these tools do not adequately address the real challenge of siloed security tools and must be carefully configured and maintained by a team of specialists to truly work effectively.

05 Security operations centre (SOC)

Large enterprises often rely on a security operations centre (SOC) to defend against cyber threats. A SOC is a centralized team of experts responsible for threat monitoring, detection, and response activities for an organization. This function may be run in-house by qualified employees or outsourced to an experienced third party. SOCs analyze raw data from systems and security tools such as SIEMs to identify and respond to threats. The team is responsible for other cyber security-related tasks as well, including:

- **Managing hardware, software, and applications**
- **Ensuring equipment is patched**
- **Confirming alerts**
- **Maintaining activity logs**
- **Carrying out incident response**

Unfortunately, hiring a team of cyber security experts is simply not feasible for many organizations. As a result, a SOC is simply off the table for numerous companies trying to improve their cyber security posture.

06 Managed detection and response (MDR)

Managed detection and response (MDR) refers to outsourced cyber security solutions that provide organizations with a qualified, experienced team that handles threat monitoring, detection, and response on their behalf. MDR solutions are designed to provide end-to-end coverage across every aspect of an organization's IT infrastructure — including endpoints, cloud services, remote users, and IT networks — as a managed service.

This eliminates the barriers imposed by cost and experience, allowing companies of all sizes to employ efficient, effective cyber security. MDR solutions can be installed on-premises or deployed in the cloud to monitor all aspects of IT infrastructure. They measure activity and search data for anomalies, vulnerabilities, and other potential threats, generating reports and alerts across IT environments, in turn helping eliminate many of the challenges resulting from a siloed approach to security.

MDR platforms are an attempt to overcome the challenges of tools working in isolation or focused on specific aspects of the IT environment. These platforms provide a comprehensive and complete security solution that delivers the visibility necessary to effectively defend businesses from cyber attacks.

Choosing the right solution

Trying to find the right cyber security solution to defend your IT operations can feel like trying to find a needle in a haystack. Not all solutions are created equally, which makes finding one that will meet your company's needs all the more challenging.

Solutions must keep pace with the rapid changes in the cyber security landscape. Any chosen software should provide functionality and capabilities to identify potential risks and active threats across your IT infrastructure, provide actionable alerting, and help you prioritize and remediate any issues.

WHEN ASSESSING ANY SOLUTION, THERE ARE FOUR FACTORS TO CONSIDER:

- **Scalability:** How will this technology adapt to changing needs?
- **Holistic approach:** How comprehensive is the solution's approach to security?
- **Expertise:** How experienced is the security team backing the solution?
- **Time:** Will the solution automate common, time-consuming security tasks?

Before choosing a solution, it's important to understand the threats facing your business. This starts with your threat surface: all the areas of your IT network where unauthorized users or attackers could exploit vulnerabilities to gain access to systems and confidential data to stage an attack.[4]

Your threat surface is always changing as new technology, users, and connections are introduced. Assessing and managing your threat surface while reducing the number of attackable points starts with the concept of cyber situational awareness (CSA), defined as:

- **Knowing your network.**
- **Knowing your threats.**
- **Knowing how to respond to these threats.**

Building your CSA also builds the knowledge base you need to assess, manage, and reduce your threat surface.[5]

From there, your threat surface assessment comprises three major steps:

01 — Conduct an inventory of your IT assets. What IT assets does your business use, and what may be of value to others? This can include hardware, software, and internet-facing assets, as well as personal data, sensitive information, intellectual information, and even your supply chain.

02 — Measure risk. What would be the worst-case scenario if your assets were compromised? How vulnerable to attack are these assets? Take time to assess the risks your assets may introduce and evaluate the protections you have in place.

03 — Improve security posture. Use the information you've gathered to review your security posture. What protections do you have in place now? Are they sufficient or do you need more resources? Who is responsible for protecting your assets? This approach can help you pinpoint the most relevant threats facing your IT infrastructure, allowing you to respond accordingly.

01

Scalability

Businesses are always changing and growing. Each new user creates a need for additional technology, which in turn expands the threat surface. Customers introduce additional requirements and concerns. Ensuring security is a monumental task but staying ahead of emerging threats is just as important.

This requires cyber security solutions that won't be rendered obsolete the moment new endpoints or technology are integrated with the existing tech stack. Look for those that deliver a range of capabilities, backed by a vendor that's committed to continual improvement, developing and releasing new features for a strong defence.

02

Holistic approach

While the techniques behind each cyber threat may share some overlap with each other, they're not all targeting the same component, and their end goals may differ wildly. If a solution focuses exclusively on one aspect of the threat surface at the expense of others, this may require deploying multiple solutions to solve each new issue.

Effective cyber security requires an end-to-end approach to monitoring, detecting, and responding to threats and risks across the entire IT environment. This holistic approach to security should protect endpoints, cloud services, and IT networks, 24/7, 365 days a year. Unfortunately, some vendors only deliver this coverage through modular add-ons, requiring additional IT investment to implement effective defences, as well as more time to integrate, manage, and maintain. Solutions that take this holistic approach can deliver effective security coverage without the sticker shock at renewal time.

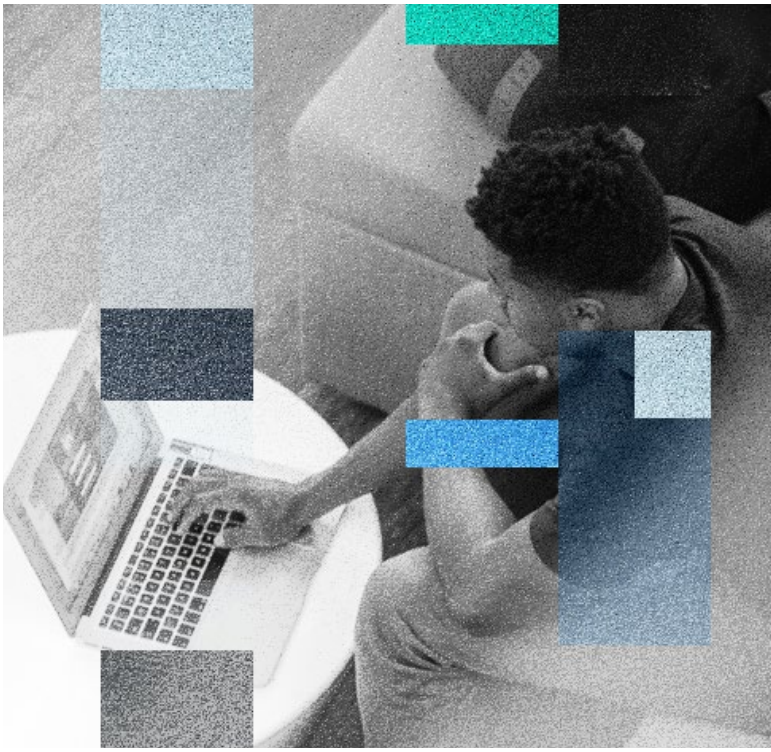
03

Expertise

The best technology still needs experience to back it up. At its core, cyber security is about knowing how threats work, how to spot them, and how to respond to them. Cyber security automation can provide some relief, but human analysis is still necessary to interpret the data gathered by any solution. Because hiring an in-house team is costly and time-consuming, many businesses choose to outsource some or all of their cyber security defence, relying on managed service providers and hiring experts.

Ensuring solution providers can back up their technology with the necessary expertise is vital. Take time to check credentials, review client testimonials, request references, and ask about the product roadmap — look for a team that brings deep experience in cyber security along with software development and management.

When it comes to threat monitoring, detection, and response, look for effective and efficient solutions that monitor the vast amounts of data activity from IT networks, endpoints, and cloud services. From there, narrow it down to tools backed by a team of cyber experts that not only thoroughly analyzes this data, but provides clear, actionable information to help prioritize and triage response and remediation. This functionality reduces the time required to investigate false positives and surfaces the threats that matter.



04

Time

Cyber security is time-consuming and challenging, and attackers know it. That's why techniques like business email compromise (BEC) continue to be effective — they rely on just how busy and overworked IT teams are. CISOs and IT teams are stretched thin from the constant demands and information overload of cyber security. Burnout is common, with teams struggling to handle security tasks on top of daily needs.

FIELD EFFECT™

Conclusion

We hope this eBook has given you valuable insight you can use when assessing potential cyber security solutions.

Finding the right solution can sometimes feel like a daunting task, especially as you deal with day-to-day security challenges and other critical IT priorities.

IF THERE'S ONE THING YOU TAKE AWAY FROM WHAT YOU'VE READ, WE HOPE IT'S THAT YOU UNDERSTAND NOT ALL SOLUTIONS ARE CREATED EQUALLY. FINDING ONE THAT WILL GROW WITH YOU WHILE PROVIDING COMPREHENSIVE, END-TO-END DEFENCE HAS NEVER BEEN MORE URGENT.

Cyber threats are always changing. You deserve protection that can keep pace. Taking a proactive approach to defending and securing your operations against new and emerging risks can help prevent cyber attacks.

And, remember, you're not alone. It's our mission to help protect small and mid-size businesses. If you have any questions, or need any help with your cyber security, get in touch with our Field Effect team. We've got your back..

[1] https://www.esg-global.com/blog/security-point-tools-problems

[2] https://newsroom.ibm.com/2020-06-30-IBM-Study-Security-Response-Planning-on-the-Rise-But-Containing-Attacks-Remains-an-Issue

[3] https://www.cisecurity.org/spotlight/cybersecurity-spotlight-signature-based-vs-anomaly-based-detection/

[4] https://www.cyber.gc.ca/en/guidance/cyber-threat-surface

[5] https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html

About Field Effect

Field Effect believes that businesses of all sizes deserve powerful cyber security solutions to protect them. Our threat detection, monitoring, and response solution, along with our training and compliance products and services are the result of years of research and development by the brightest talents in the cyber security industry. Our solutions are purpose-built for SMBs and deliver sophisticated, easy-to-use and manage technology with actionable insights to keep you safe from cyber threats.

FIELD EFFECT COVALENCE

The Covalence product line includes Covalence Remote Work, Covalence Cloud, and Covalence Complete.

Covalence threat monitoring, detection, and response platform

Covalence, Field Effect's threat monitoring, detection, and response platform, provides small businesses continuous visibility into their IT networks to identify potential threats, vulnerabilities, and malicious activities. By providing easy-to-understand, actionable insights, Covalence helps customers prioritize and resolve cyber security issues and improve their security. The end result is a powerful cyber threat detection system, delivering big business insights without the matching price tag.

Start Securing Your Business Today.

Contact us
hello@fieldeffect.com

Canada and the United States
+1.800.299.8986

United Kingdom
+44.800.0869176

Australia
+61.1800.431418