FORTRA™

GUIDE (TRIPWIRE)

Foundational Controls Buyer's Guide

Introduction

If you're like most security professionals, you must feel positively inundated with the volumes of material made available to you about the challenges of enterprise cybersecurity and the serious consequences of malicious hacking to business, governments and society. Quite frankly, the variety of tech tools and security options are dizzying—it's hard to know where to start. Do we jump on the latest advanced malware AI machine learning craze? Or is it big data security analysis in the cloud that we need? Or maybe we just need better network filtering with data-loss protections to ensure our organization is kept secure and compliant. The one thing that's definitely needed is a simplified guide to the numerous frameworks and security regulations out there in order to cut through the noise and hype around securing today's modern enterprise.

The solution rests simply in making sure that our security practice is built on a solid foundation of controls. But what are the "Foundational Controls"?

Foundational controls include:

- Asset Discovery
- Security Configuration Management
- File Integrity Monitoring
- Vulnerability Management
- Log Management

This Foundational Controls Buyer's Guide can help you choose new or replacement solutions that serve as the foundation of your organization's security and compliance programs. Its goal is to tease out the differences between the various types of capabilities available, and to identify the most important features.

Asset Discovery

In very large networks, it's likely that despite your best intentions your visibility into the assets that you've been tasked to protect is incomplete or outdated. Often, enterprise security teams don't directly control the assets they are chartered to protect, and gaining deep insight into these devices can be a challenge. Cloud, virtual and mobile device adoption trends continue to add to the complexity of corporate networks, with the result being blind spots in security risk visibility. And those blind spots are the ideal places for adversaries to launch and advance their attacks. The first step deploying foundational controls is an accurate hardware and software inventory. This step is essential because a complete view of your asset inventory is necessary for subsequent foundational controls, such as vulnerability management.

CIS Control 1 – Inventory of Authorized and Unauthorized Devices offers a good explanation as to why an incomplete view of asset inventory is problematic:

The Asset Discovery Process

When you initiate asset discovery, there are several tasks that run in background depending on the solution you are using and how it is configured. These tasks may include:

- **NAME RESOLUTION:** During Name Resolution, the IP Addresses are resolved to host names using DNS Servers
- **PING:** Pinging hosts is a portion of host discovery; however, it is usually separated into its own task. Typically there are database-specific configurations that can be applied to the product around ICMP timeout and max requests.
- **HOST DISCOVERY:** Specific TCP and UDP ports are contacted in an attempt to determine if a host is up and responsive.
- **NetBIOS NAME RESOLUTION:** NetBIOS Name Resolution uses a very specific NetBIOS packet to attempt to determine the NetBIOS Name of a host.
- **CREDENTIAL SET CREATION:** Credentials that were provided via the user interface are turned into specific credential sets that can be provided to rules when requested.
- **CIFS SHARE ENUMERATION:** Available shares on the host are enumerated.
- **PORT SCAN:** Ports are scanned based on a configurable known port list. Typically there are settings related to retry attempts and timeouts that can be configured in the user interface.
- **APPLICATION SCAN:** Application rules are executed against ports that are discovered to be open. Advanced solutions will associate various protocols to specific ports and will only scan for those protocol-to-port pairings and execute protocols, applications, and rules in a specific order to limit the intrusiveness of a scan. Typically, solutions will also allow you to scan for protocols and applications on non-standard ports.

- **OS FINGERPRINT SCAN:** Traditional stack fingerprinting techniques are applied to assist in determining the operating system. Stack fingerprint rules are executed against a host and then compared with a database of known operating system responses.
- **OS COMPUTATION:** The most likely operating system is determined based on the results of previous tests.

> *"Attacks can take advantage of new hardware that is installed on the network one evening but is not configured and patched with appropriate security updates until the following day. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal jump points or victims."*
>
> www.cisecurity.org/critical-controls/

What to Look For

- **DYNAMIC HOST TRACKING:** The ability to track portable hosts by uniquely identifying systems as they connect, disconnect and reconnect to different networks is crucial for accurate and reliable data collection. Many solutions track hosts over time using IP addresses. However, because IP addresses can change frequently, this can lead to inaccurate results and misrepresentation of network risk posture. For example, changes to a host's IP address may cause some solutions to report on two hosts rather than the one that really exists. Leading edge discovery solutions have overcome this issue by using agents or additional dynamic information (such as DNS name, NetBIOS name, operating system, IP address, port signature, OS fingerprint or MAC address) to track and uniquely identify hosts. These solutions use that detailed data to dynamically track hosts as they move from group to group, and immediately reflect those changes in the reporting and asset management parts of the solution. This approach ensures that data collected from a given host or group remains accurate.
- **ASSET TAGGING:** Solutions should provide the ability to tag assets by group, technical owner, regional location or criticality. Advanced solutions may automatically assign rules-based asset tags to devices to automate workflows and capture unique characteristics of your organization.
- **CREDENTIALED SCANNING:** Ideal solutions offer both credentialed and uncredentialed assessment capabilities, making it easy for you to choose which method to use for assessments and adjust as your needs change over time.
- **HIERARCHICAL ASSET ORGANIZATION:** It can be useful to organize hosts and networks in a business-aligned structure; for example, the capability to group assets in business unit categories (like finance and sales, or geography like North America or EMEA) should be offered. This helps the solution apply business context when calculating and trending security data.
- **DEVICE SUPPORT:** The solution should support discovery of all the device types in your environment including wired and wireless devices, virtual machines, cloud instances, etc.
- **SOFTWARE AND APPLICATION SUPPORT:** The solution should also support discovery all the software and applications in use in your environment including desktop applications, operating systems, ports, services and protocols.

Security Configuration Management

Security configuration management (SCM) exists at the point where IT security and IT operations meet. It's a software-based solution that combines elements of vulnerability assessment, automated remediation, and configuration assessment. SCM enables IT security professionals to reduce their networks' attack surfaces by proactively and continuously monitor and hardening the security configurations of operating systems, applications, and network devices. At the same time, SCM enables compliance auditors to monitor compliance with mandated policies.

The Security Configuration Management Process

At a high-level, the SCM process includes four steps:

1. **DISCOVERY:** First find the devices that need to be managed. Ideally you can leverage an SCM platform with an integrated asset discovery repository. You will also want to leverage categorization and asset tagging to avoid starting unnecessary services. Engineering workstations, for example, require different configurations than Finance systems.
2. **ESTABLISH CONFIGURATION BASELINES:** First define acceptable secure configurations for each managed device type. Many organizations start

with the benchmarks from CIS or NIST for granular guidance on how devices should be configured.

3. **ASSESS, ALERT, AND REPORT CHANGES:** Once devices are discovered and categorized, define a frequency for assessments. How often will you run a policy check? Real-time assessments may be available but are not required for all use cases.
4. **REMEDIATE:** Once a problem is identified, either it needs to be fixed or someone needs to grant an exception. You are likely to have too much work to handle immediately, so prioritization is a key success criterion. You will also need to verify that expected changes actually took place for the audit.

What to Look For

- **OS AND APPLICATION SUPPORT:** Your configuration management offering should support the operating systems and applications in use in your environment.
- **STANDARDS AND BENCHMARK SUPPORT:** The more available policies and configurations offered by the solution, the better your chance of finding something you can easily adapt to your own requirements.
- **POLICY EDITING:** Policies generally require customization to satisfy your requirements. Your configuration management solution should offer a flexible policy editor to define policies and add new baseline configurations and/or benchmarks.
- **SCALABILITY:** Scanning each device for configuration changes can be demanding on endpoints and the network, so understand how to distribute scanners effectively and make sure scanning frequency, impact and scope is flexible.
- **REMOTE DEVICES:** How does assessment work for a remote device? This could be a field employee's laptop or a device in a remote location with limited bandwidth. What kinds of recovery features are built in to ensure the correct remediation is implemented? And finally, can you be alerted to devices that haven't been recently assessed, perhaps because they haven't connected?
- **INTEGRATION WITH OPERATIONAL PROCESS:** Make sure any identified configuration issues are reported to the central help desk system to close the operational loop in order to ensure a proper process for authorizing and applying changes.
- **PROCESS TO DEAL WITH POLICY EXCEPTIONS:** As mentioned above, there may be situations where a configuration change represents an authorized exception. To complicate things further, authorization is often granted after configuration management detects (and perhaps reverses) the change. You must be able to reduce the possibility of false positives.

File Integrity Monitoring

File integrity monitoring (FIM), also called change monitoring, means monitoring files to see if and when they change, how they changed, who changed them, and what will it take to change them back. Obviously many files do legitimately change over time, particularly during patch cycles. But most files are generally static, and changes to core functions (such as the IP stack and email client configuration) often indicate some type of problem. This active security control allows you to define a set of files (including both system and other files), gather a baseline for what they should look like, and watch for changes. FIM is particularly useful for detecting unauthorized changes and malware, as well as compliance with regulations such as PCI.

The File Integrity Monitoring Process

A process for implementing file integrity monitoring typically includes:

- **SET POLICY:** Start by defining your policy, identifying which files on which devices need to be monitored.
- **BASELINE FILES:** Then ensure that the files you assess are in a known good state. This may involve evaluating version, creation and modification date, or any other file attribute to provide assurance that the file is legitimate.
- **MONITOR:** Next, actively monitor changes. This is easier said than done because you may see hundreds of file changes on a normal day on a single system, so knowing a good change from bad is essential. You need a way to minimize false positives by auto-promoting expected changes.
- **ALERT:** When an unauthorized change is detected you need to let someone know.
- **REPORT:** FIM is required for PCI compliance. So you may need to substantiate effective usage for your assessor. That means generating reports for a compliance audit.

What to Look For

- **LIGHTWEIGHT AGENT:** In order to implement FIM you might install an agent on each protected device. Agents should be flexible to turn off functionality when not in use, and pluggable to be able to add functions as they become necessary.
- **MONITORING FREQUENCY:** You need to determine whether you require true continuous monitoring of files, or whether scheduled assessment is acceptable.
- **INTEGRATION WITH THREAT INTELLIGENCE SOURCES:** Additive to internal research is integration with third-party threat intelligence sources as they likely have the most up to date information on new attack vectors and indicators of compromise.
- **RESEARCH AND INTELLIGENCE:** A large part of successful FIM is identifying a good change from a potentially bad one. Besides integration with threat intelligence sources, it requires integrated operational intelligence.
- **CHANGE DETECTION ALGORITHM:** Is a change detected based on file hash, version, creation date, modification date and/or privileges? Or all of the above? Understanding how the vendor determines a file has changed enables you to ensure all your threat models are factored in.
- **VERSION CONTROL:** Remember that even a legitimate file may not be the right one—for example, you're updating a system file, but an older legitimate version gets installed instead.
- **FORENSICS:** In the event of a breach you'll want forensics capability, such as a log of all file activity. Knowing when different files were accessed, by which programs—and what was done—can be very helpful for assessing the damage of an attack and nailing down the chain of events which resulted in data loss.
- **CLOSED LOOP CHANGE AUDIT:** Thousands of file adds, deletes and changes happen—and most are authorized and legitimate. But for both compliance and operational reliability you should be able to reconcile the changes you expect against the changes that actually happened.
- **PLATFORM INTEGRATION:** There's no reason to reinvent the wheel, especially for cross-functional capabilities such as discovery, reporting, agents and agent deployment/updating/maintenance. So leverage your FIM platform to streamline implementation and facilitate operations.
- **POLICY MANAGEMENT:** For policy creation the system should provide baselines to get you started. Every environment has its unique characteristics, but the platform vendor should provide out-of-the-box policies to make customization easier and faster. All policies should be usable as templates for new policies. The more complex a policy, the easier it is to create internal discrepancies or accidentally define an incorrect remediation. Most administrators tend to prefer interfaces that use clear, graphical layouts for policies, preferably with an easy to read grid showing the relevant information for each policy.
- **POLICY GRANULARITY:** You will want to make sure your product can support different policies by device. For example, a Point of Sale device in a store (within PCI scope) needs to have certain files under control, while an information kiosk on a segmented internet-only network in your lobby may not need the same level of oversight.
- **SUPPORTED STANDARDS AND BENCHMARKS:** PCI DSS, NERC CIP, SOX, HIPAA, NIST 800-53, MAS TRM, IRS 1075, CIS Controls, Mitre ATT@CK, COBIT, ISO 27001 to name a few. The more built-in standards and/or configuration benchmarks offered by the tool, the better your chance of finding something you can easily adapt to your own requirements.
- **POLICY EDITING:** Policies generally require customization to satisfy your requirements. Your configuration management tool should offer a flexible policy editor to define policies and add new baseline configurations and/or benchmarks.
- **POLICY UPDATES:** Regulatory policies are updated constantly; systems should quickly (even automatically) update through content download for the solution.

Vulnerability Management

With new physical and virtual devices being added to corporate networks, altered and removed at a faster pace than ever, enterprise networks are in a state of constant and rapid change. Some of these changes are unauthorized and may introduce new vulnerabilities. Even if these vulnerabilities are temporary (as in dynamic containers or

elastic cloud instances) or on remote or business partner networks, they can still present an open door for attacks. IT security teams tasked with remediating these vulnerabilities need to be able to approach vulnerability assessment from several perspectives in order to get an accurate assessment of risks, minimize security threats and maintain compliance.

The Vulnerability Management Process

At a high-level, there are four stages to a vulnerability management program:

1. **THE VULNERABILITY SCANNING PROCESS:** This process determines the criticality of assets, the owners of assets, scan frequency, and timelines for remediation
2. **ASSET DISCOVERY AND INVENTORY:** The discovery and inventory of assets on the network
3. **VULNERABILITY DETECTION:** The discovery of vulnerabilities on the discovered assets
4. **REPORTING AND REMEDIATION:** The reporting and remediation of discovered vulnerabilities.

What to Look For

- **RISK SCORING:** Every organization is different, with different priorities, risk tolerance and threats targeting them. Standard industry vulnerability scoring systems, such as CVSS, may rate a vulnerability as an "eight," on a scale of 1–10, but for your specific organization the same threat may present a higher or lower risk. A quantitative score is a necessary baseline, but many organizations need the ability to weigh vulnerabilities based on the unique requirements of their specific business or industry. In order to allow security teams to quickly identify and remediate the most significant risks on their network, they need automated tools that allow them to customize vulnerability management data for their unique risk profile. This data should be used to provide comprehensive, prioritized remediation information. Risk scoring is a good example of how customization can help organizations tailor vulnerability management data to their specific business requirements. Many vulnerability management systems offer High/Medium/Low or 1–10 scoring. In organizations with thousands or tens of thousands of vulnerabilities, these rough scores lose meaning. Advanced vulnerability management solutions provide flexible, granular scoring systems that can be adapted to even the largest networks.
- **CREDENTIALED ASSESSMENT:** Assessment depth can significantly impact the accuracy of results—deeper assessments gather more detailed information, which the system can use to improve accuracy. Credentialed assessments use administrative credentials to inspect file system, registry and configuration files. Credentialed assessments take longer to run than uncredentialed assessments, but the additional information that is gathered dramatically improves both discovery and assessment accuracy. In contrast, more basic non-credentialed assessments piece together the simple information that a host provides to determine vulnerabilities, which can lead to inaccurate results and false positives. Both approaches have value for different reasons, and the best solutions offer both credentialed and uncredentialed assessment capabilities. Ideally, a vulnerability management control should offer both methods so that you can use the method that best balances your organization's requirements for assessment speed versus assessment depth.
- **IDENTITY AND ACCESS MANAGEMENT:** Without tight integration between an organization's directory service and vulnerability management system, administrators must manually create, update and delete accounts every time a change is needed. If those changes are not reflected in the vulnerability management system, then employees who need access to vulnerability data may not have it, and those who don't need it could gain access. In larger, multi-unit organizations or managed services provider companies, multi-tenant capabilities are required to optimize sub-account management from a master account. This additional capability makes it easy to segregate data and partition user access.
- **ACCURACY:** Accurate assessment results are critical, yet vulnerability management products deliver assessments with varying degrees of accuracy. Some solutions often identify vulnerabilities where they don't exist—and fail to find vulnerabilities that pose serious security risks. Vulnerability management controls should have a range of technologies to significantly reduce the identification of "suspected" vulnerabilities. This supports the most efficient use of your time and resources.

- **INDISCRIMINATE TESTING:** In this older vulnerability assessment method, the vulnerability management product scans through a defined range or list of host IP addresses and indiscriminately checks each host against a list of known vulnerabilities that are maintained by the vulnerability management vendor. This results in time-consuming checks for vulnerabilities that may not apply to the device being assessed. For example, this approach will result in checking a Linux machine for a Windows vulnerability. This scenario is also likely to occur when device and application inventory is inaccurate, such as when a NetApp filer running a UNIX-derivative OS is profiled as a Windows device because the device is running a Windows SMB/CIFS service.
- **TARGETED TESTING:** This vulnerability assessment method first inventories and profiles each host to determine the type of device, operating system and applications present. It then uses that information to intelligently and efficiently check for only relevant vulnerabilities, skipping checks that don't apply to a particular host, OS or application version.
- **IT AND SECURITY INTEGRATIONS:** Sharing change and vulnerability data between IT Operations and Security teams makes it easy to optimize resources for specific business goals, yet most vulnerability management data is not easy to share. Also, many vulnerability management tools waste valuable resources because they require manual effort to export and format data for consumption by other teams.
- **REAL-TIME DATA NAVIGATION:** Advanced vulnerability management products offer real-time data navigation and synthesis. These advanced tools make it easier for security professionals to assess network risk and focus their actions on areas of greatest importance. For example, they can produce a list of hosts that share a specific vulnerability, or compare two historical host assessments to identify new vulnerabilities or applications that have changed.
- **HISTORICAL TRENDS:** Demonstrating vulnerability identification and remediation trends over time provides insight into resource planning and allocation. Trend data provides crucial insight into specific areas of their networks where security risks are improving and where they are getting worse.
- **REPORTING SEPARATED FROM SCANNING:** Advanced solutions can consolidate information from multiple assessments into a single report. Less capable solutions combine assessments and reporting instead of collecting and storing assessment data over time to make it easily accessible in the future as an on-demand report. When reports are tied to an individual scans, you must configure a new scan and wait for it to complete to create a new report
- **DATA RETENTION:** Can the solution retain all assessment results within an administrator-specified timeframe and let the user easily view recent and historical assessments of a host?
- **REPORTING:** Can the solution provide reports with the appropriate level of detail to a variety of audiences? These could include auditors who may wish to see proof of compliance, and business executives who want an overview of the organization's risk posture, graphical views of risk trends, and visualization of risk data by organizational hierarchies or geographical location. Does it allow all users to create, save, and share report filters? Can the report be filtered to include or exclude data based on host score, vulnerability type or severity, operating system group, and other characteristics? Are reports automatically distributed to users based on their roles?
- **REMEDIATION ADVICE:** Does the solution offer advice on how to best correct vulnerabilities including accurate and complete remediation details, potential mitigations, links to patches, vendor advisories, and relevant vulnerability information?
- **VULNERABILITY INSTANCE DATA:** Details about how a vulnerability was detected can help system administrators can manually verify the existence of a vulnerability. A vulnerability may reappear in a report after a patch or other fix has been applied—or misapplied—because the machine is still vulnerable. This can also happen when the device requires a reboot for the patch to take effect. Information on how a vulnerability was discovered can help teams collaborate to find underlying causes that introduce additional risk to the organization.

Log Management

Much of securing an infrastructure relies on the ability to accurately determine both what's happening and what has happened in an environment. Much of the data about activity in an environment is recorded in logs of various types. Logs are produced by operating systems, applications and most other devices. The collection, storage and analysis of logs is a Critical Security Control, as per the Center for Internet Security (CIS). CIS explains the relevance of log management for security quite succinctly:

> *"Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attacks and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and particular damages done may be irreversible."*

Very simply, if you're not collecting, storing and analyzing log data for every asset in your organization, you have significant gaps in your security visibility.

The Log Management Process

A log management process has to consider a five basic parameters:

1. **COLLECTION:** Logs are collected using agent and agentless methods from a variety of platforms over encrypted connections
2. **STORAGE:** Logs are preserved, compressed, encrypted, stored and archived
3. **SEARCH:** Logs are indexed for searching via plain-text, REGEX, and API queries
4. **CORRELATION:** Correlation rules are applied to detect events of interest and perform automated actions
5. **OUTPUT:** Information is distributed using dashboards, reports, emails, and event forwarding to other systems

What to Look For

- **COLLECTION:** There are many considerations for secure and reliable log collection. Of course, missing log data can't be analyzed, so the ability to ensure logs get collected is primary to any log management project. Any log management product should offer multiple means to collect logs, but should recommend the most reliable method. Remote log collection, while sometimes necessary, is significantly less reliable than an agent-based approach. Using an agent for log collection increases both the security and reliability of the operation. Wherever possible, agents should be preferred over remote collection.
- **STORAGE:** Collected logs need to go somewhere, and the volume of log data makes storage a significant issue for any deployment. Log storage needs to address at a minimum the requirements for preservation and compression of log data. More advanced features include flexibility around where the data is stored geographically, for compliance requirements and scalability.
- **SEARCH:** Collected data is meant to be used, and log searching is an activity that applies across the use cases outlined above. In order for log search to be effective, it needs to provide the right balance of flexibility and performance. Users should be able to directly affect the search by providing better filtering, using classification tags. While it's preferred to search indexed, normalized log data, the ability to review raw logs is a key requirement as well. Log searching needs to facilitate very directed queries, as well as broad queries that allow an analyst to narrow down the results. For comparison purposes it's important that users be able to view the results of multiple queries at the same time.
- **CORRELATION:** Events, regardless of their use case relevancy, rarely occur in a single log entry on a single host. Much of what an analyst does is connecting the dots between disparate events. While not all of this manual effort can be automated, a correlation capability in a log management tool should alleviate the burden of the most obvious examples. A correlation capability is meant to provide the user with an ability to customize the events generated to their environment. While many events can be pre-populated with vendor supplied rules, the most powerful correlation capabilities come from patterns of events that are specific to an individual organization or department. Users should find an intuitive interface for creating new correlation rules, in addition to a library of pre-built correlation capabilities. Of course the correlation capability is only as good as the data elements on

which correlation can be run. Users should evaluate how correlation is performed on collected elements of log data. Finally, logs don't provide all of the data required for correlation. The log management tool should support importing additional data sources to facilitate more complete correlated events. Examples include vulnerability scanning results and asset context from other systems.

- **OUTPUT:** Finally, the ability to get data out of the system, whether from log searching or correlated events, is a core requirement for any log management system. While vendors may want to see their system as the ultimate destination for data, that's rarely the case. Whether that next stop is a human being or another system, it's vital that the log management tool facilitate the exchange of data. Customers should consider how search results are exported, whether they can be scheduled, how correlated events are delivered, and what options there are for destinations. The ability to forward logs is a key requirement as well. More and more investment is going into complex analytics on top of log and other data. A log management system should focus on the core requirements of collection and correlation, but preserve the ability to deliver the log data to other systems—either in its entirety or filtered to specific events.

Summary: 10 Questions to Ask Your Vendor

1. Which specific controls do you offer for security and compliance? Can the policies for all controls be managed via your console?
2. What products, devices and applications are supported by your offerings?
3. What standards and/or benchmarks are offered out of the box as part of your offering?
4. What kinds of reports are available out of the box? What's involved in customizing specific reports?
5. Does your organization have an in-house research team? How does their work make your product better?
6. What kind of agent is required for your product(s)? Is the agent persistent or dissolvable? How are updates distributed to managed devices? How do you ensure agents are not tampered with?
7. How do you handle remote and disconnected devices?
8. Where does your management console run? Does it require a dedicated appliance? What kind of hierarchical management does your environment support? How customizable is the management interface?
9. What is your plan to extend your offering to virtual desktops (VDI)?
10. What have you done to ensure the security of your platform? Is strong authentication supported? Have you done an application pen test on your console? Does your engineering team use any kind of secure software development process?

We could have written another 10 questions, but these hit the highlights of device and application coverage, research/intelligence, platform consistency/integration, and management console capabilities. This list can't replace a more comprehensive RFI/RFP, but it can give you a quick idea of whether a vendor's product family will meet your requirements.

Schedule Your Demo Today

Let us take you through a demo of Fortra's foundational control solutions from Tripwire® and answer any of your questions. Visit www.tripwire.com/demo

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.