Cyber CAQ

Trend

Cyber Insurance Common Application Questions (CAQs)

The cyber insurance application process can be arduous and time consuming, especially for first time buyers. Our team has pulled together the most common application questions to help you understand what it means and how Trend products or solutions fit into the equation.

Have confidence in knowing Trend has your back. Our solution, Trend Vision One™, along with other Trend Micro solutions meets many of the security control requirements that cyber insurance carriers and brokers are looking for.

Is multi-factor authentication (MFA) deployed?

Why is this important?

It is an essential security control required by most insurers today, along with being required by PCI, and many other regulatory entities. It makes exploiting passwords obtained through phishing attacks more challenging and credential dumping a less valuable tactic. MFA is also seen as an early warning systems to detect and respond faster. Underwriters also want MFA enabled for webmail access.

How to respond

If your organization is using MFA for product, employee, and administrative logins for operating systems and applications *(using one-time passwords for example)* respond "yes". Specifically they'll want to see MFA enabled on all systems that are remote accessible or require privileged or admin users, and systems with critical or sensitive data.

How Trend can help

While MFA is not a capability provided by Trend,we do report on it. Utilize the reports in the platform to communicate this information with your carrier or broker.

Trend Vision One™ Identity Security is a blend of Identity Security Posture Management (ISPM) and Identity Threat Detection Response (ITDR) which allows you to discover and inventory identities, and so much more!

What endpoint protection software is deployed? Is it next-gen AV?

Why is this important?

Strong endpoint protection on employee endpoints and servers is paramount to slowing attackers and detecting early attack stages and impact phases (such as ransonware encryption). "Next-gen" modern endpoint protection uses behavioral detection, machine learning, AI, and other non-signature techniques. Using signatures alone is an outdated approach, ineffective against modern threat actors.

How to respond

Most endpoint protection solutions today qualify as "next-gen". Trend's endpoint protection solutions support machine learning and behavioral detection. You can respond "yes" if you have these capabilities enabled. Ensure they are up-to-date prior to answering your application.

Insurance forms often list vendors to select from. If you don't see Trend Micro write us in, as we are an acceptable answer. **You are not required to deploy a vendor from that list.**

How Trend can help

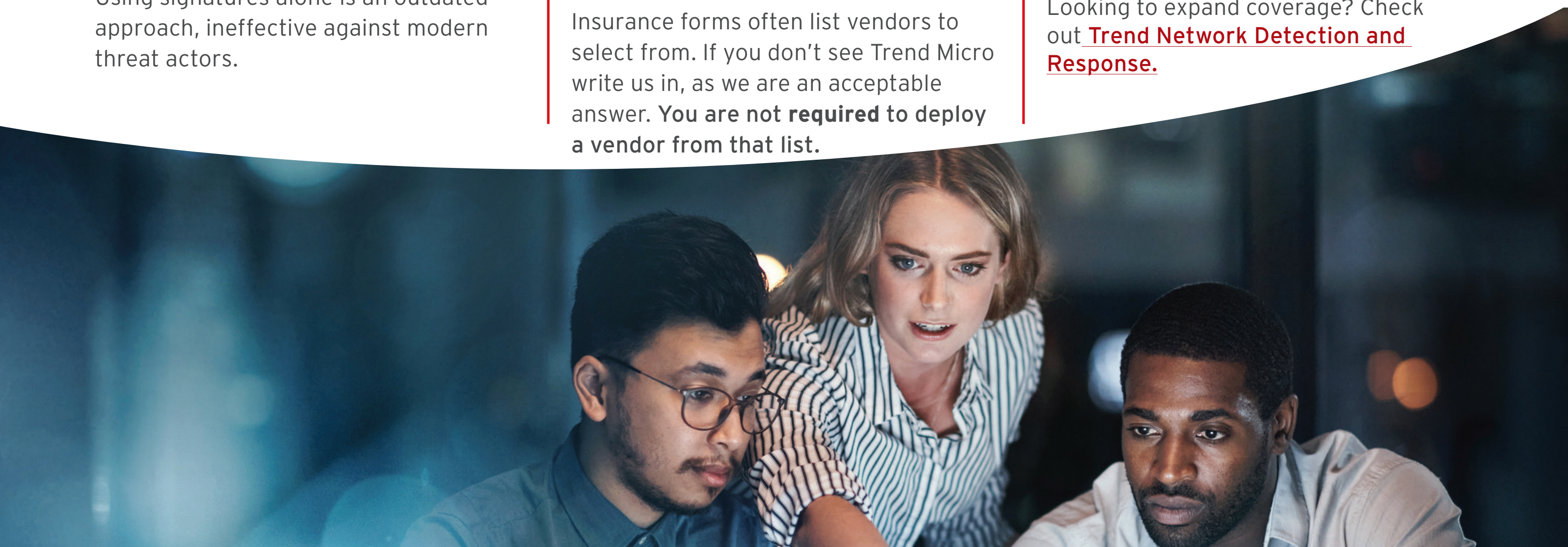
Our Attack Surface Risk Management module delivers ulitmate visbility and protection.

Trend Vision One@ Endpoint Security

Trend Server and Cloud Workload Security

Trend Vision One™ XDR

Looking to expand coverage? Check out Trend Network Detection and Response.



Is endpoint detection and response (EDR) deployed?

Why is this important?

Endpoints are the primary entry point for most malicious attacks. EDR is an important capability enabling IT security teams and managed service providers to better detect attacker activity. EDR can help detect threat actors in early stages by monitoring activity, detecting anomalies, and stopping that attack before it spreads to the wider network and systems.

Adding NDR (Network Detection & Response) to the mix will give visibility to attack behavior before it hits the endpoint.

How to respond

With EDR activated on your endpoints indicate "yes". Trend Vision One Endpoint Security is EDR technology. Make sure to highlight if you are using XDR within Trend Vision One, and the more information you can share about this, such as how many sensors have been deployed out of how many assets you have, can impact your approval for a policy.

Share reports available in the console with your broker to provide attestation of your environment.

How Trend can help

Trend Micro provides EDR and XDR capabilities with the following products:

Trend Vision One@ Endpoint Security

Trend Server and Cloud Workload Security

Trend Vision One™ XDR

Looking to expand coverage? Check out Trend Network Detection and Response.

TIP: **Aim to have more than 90% deployment across your devices and asset inventory. This is the percentage insurance carriers and brokers are looking for to reduce their risk by taking on yours.**

Do you have asset discovery tools or solutions that protect EOL systems?

Why is this important?

Being able to show your insurance provider your total assets is key to defining your overall risk as an insured. They are looking to see if 90% or more of your assets are protected with something. In addition, they want to know what protections you have in place for those unsupported or EOL systems in your environment. Why? Because they pose the biggest risk and gateway for threat actors to gain access to your systems.

How to respond

If you are using Trend Vision One ASRM, then you have visibility to your assets and protection for those older systems. When answering select "Yes", but make sure to go in detail on what solutions you are using or provide a report to show your asset inventory and just how many have endpoint protection. If it's over 90% you're in a good spot. If not, you will have to explain why.

Also you'll want to make sure you have an up-to- database of all of your organization's assets that you can share if required.

How Trend can help

Our Attack Surface Risk Management module delivers ulitmate visbility and protection.

Trend Vision One@ Endpoint Security

Trend Server and Cloud Workload Security

Trend Micro™ TippingPoint™

Provides protection at the network layer, reduces blindspots, and delivers additional protection to older systems.

Does your organization utilize and MDR service or do you have 24/7 monitoring?

Why is this important?

Insurance carriers recognize that having a "second set of eyes" or a full 24/7 monitoring protocol in place on security environments represents lower risk to them, and lowers your risk of having an incident. In the latest research, 40% of breaches are identified by a benign third party. More eyes on the prize = less surprises.

How to respond

Using Trend Service One™ (Essentials or Trend Service One Complete™) is worth highlighting on an insurance application. Insurers see MDR as a **PROACTIVE** security control that reduces the likelihood of a severe security event and lowers the risk of your organization.

How Trend can help

Trend Managed XDR

Trend Service One™

Additional solutions that provide more visibility: Attack Surface Risk Management.

What is your vulnerability assessment/patch management process?

Why is this important?

Attackers are quick to take advantage of remotely exploitable vulnerabilities within your environment and use them to their advantage. Once in they infiltrate your network by moving laterally to gain access to other areas of the network.

An effective risk assessment process shows insurers you are able to quickly detect and respond to to these threats. In addition, a well-defined patch management process highlights your capabilities to resolve critical vulnerability patches in a timely manner.

How to respond

Insurers are looking for organizations who have solutions that help them prioritize vulnerabilities, to address the most critical first. In addition, insurers want to understand what your Mean Time to Patch (MTTP) is. This indicates to them if you are speedy or lax in your patch management process.

Trend Vision One provides all this information, which you should and can share with your broker or carrier. Additionally, if you have an IPS solution in place be sure to highlight that on your application.

How Trend can help

Trend Vision™ One Attack Surface Management delivers ulitmate visbility and protection. The operations dashboard provides insights into all vulnerabilities in your environment, MTTP, misconfigurations and more.

Trend Micro™ TippingPoint™

Provides protection at the network layer, reducing blind spots and effectively blocking threats undetected by traditional security solutions.

Trend Micro™ Deep Security™ Software

What is your backup strategy?

Why is this important?

Data backups are an important defense against ransomware, reducing your time to recoverand resume normal business operations. However, your strategy behind this is equally important, as backups can be targeted if they are not separated from the network or have not been through adequate testing etc. It's important to note that less than 30% of backups survive a ransomware event.

How to respond

Insurers require you to provide a description of your backup strategy. Be sure to provide as much in-depth detail as you can about your backup practice, including if it's cloud-based, if they are offline, encrypted and if you have immutable backups. Also highlight how often you test your backups and what your estimation is on how long if would take to restore all your data. *(NOTE: The average time frame currently is 21 days)*

How Trend can help

Trend Vision One™ Endpoint Security provides "rollback" of encrypted files as part of a behavioral detection by uncovering the encryption behavior for initial files, suspending the process and restoring files.

Our partner, Grypho5 offers a managed backup service where they select, manage, configure and deploy a redundant solution followed by fully managing and monitoring all backup activities.

Describe the security controls/processes you have in place for your email security?

Why is this important?

Phishing (16%) and stolen credentials (15%) are the two most prevalent attack vectors that also coincide with being in the top four of the most expensive. Coincidentally they are take the longest to resolve.

Tapping into advanced emaiil security capabilities are essential to the security controls insurance carriers look at. Implementing a solid solution to detect these attacks before they reach the endpoints and proliferate the network are vital to protecting your organization, reducing your risk exposure, and increasing your security posture.

How to respond

Answer the questions as best you can on the application, but follow up with more detail in the comments section on exact configuration. Describe what controls you have in place for incoming emails - How often you train employees and the types of training you provide, and how you handle those who fail phishing simulations.

The questions on the insurance application might not offer full insight into your practice, which is why providing additional details in the comment section or providing a separate document will be helpful to the underwriter.

How Trend can help

Trend offers several solutions in the email security space:

Trend Micro Email and Collaboration Security

Trend Cloud App Security

Trend Micro Email Security Advanced

Phish Insights

On-premise solutions:

Deep Discovery Email Inspector

InterScan Messaging Security

ScanMail Suite for MS Exchange