Lionfish
Tech Advisors

# Lionfish Tech Advisors Report for Evaluating Cybersecurity Solutions for Small Security Teams

# Introduction

This Lionfish Tech Advisors Evaluation Report is a detailed analysis of cybersecurity solutions currently serving small to medium security teams. This report provides an overview of the market as well as current trends, forward-looking analysis, and a detailed evaluation of the top competing vendors in this market that includes each provider's offering, as well as solution characteristics that have an impact on performance, scalability, and customer satisfaction. The outcome will provide clear and actionable recommendations on how to efficiently and effectively navigate the cybersecurity market and select the best solutions that will meet your organization's requirements.

## Industry Overview

Many small and medium-sized businesses (SMBs), and organizations with small to medium security teams struggle to evaluate cybersecurity solutions effectively to aid in the defense of their business operations and IT infrastructure. This is further complicated when multiple products are required, as well as the needed access through different consoles, interfaces, and APIs. It can result in sprawl, making it difficult to keep track of all the applications, their usage, and the corresponding costs, as well as the true value they bring to the cyber posture and maturity level the organization is trying to achieve. This may lead to overspending on solutions and buying tools that are not utilized to their full potential. Additionally, it can be challenging to maintain security and compliance standards across all these tools without centralized control.

Moreover, the pricing opaqueness of the software industry makes it challenging for businesses to know what constitutes a fair price for the application they are buying. Businesses negotiate for applications periodically, lacking deep per-vendor negotiation frameworks to deliver optimal commercial outcomes.

To overcome these challenges, we have created this evaluation report to help readers navigate this overwhelming market and help guide you to the best solutions to meet your needs.

## Current Trends

SMBs and organizations with smaller security teams face a daunting cybersecurity landscape in 2024, with an array of challenges that significantly compromise their ability to protect their firms against cyber threats. At the core of the problem is the acute shortage of skilled cybersecurity personnel, exacerbated by SMBs' limited brand appeal, less competitive compensation, and the perception of less exciting work, making it difficult to attract the necessary talent. This shortfall in expertise leads to a reliance on overtasked system administrators or employees who handle cybersecurity as a secondary task, often resulting in a reactive, "keep the lights on" approach that falls short against sophisticated adversaries.

Moreover, SMBs grapple with insufficient funding, which is not just a matter of budget constraints but also impacts their ability to hire skilled professionals and invest in effective tools and technologies. With regulatory frameworks imposing costs that can be prohibitive for SMBs, many find themselves unable to comply with regulations or maintain a robust cybersecurity program. The lack of funding also contributes to a reliance on basic technical controls and neglects more advanced security operations such as threat hunting and incident response, which are essential for a comprehensive defense. Unfortunately, even when SMBs turn to Managed Security Service Providers (MSSPs) and Managed Detection and Response (MDR) providers, they often encounter standardized services that fall short of a tailored, effective cybersecurity strategy. As a result, SMBs struggle to keep up with regulatory requirements and remain vulnerable to threats that can compromise their business continuity and integrity.

## Evaluation Criteria

The following is a comprehensive list of core use cases that should be considered when evaluating solutions in the marketplace that serve SMBs and small security teams.

1. **Asset Management**
    a. Cyber Security Asset Management (CSAM/CAASM)
    b. Device Management
2. **Threat Intelligence**
    a. Analytics
    b. Threat insights
    c. External Attack Surface Management
    d. Continuous Threat Exposure Management
    e. Generative AI; Copilot
3. **Vulnerability Management**
    a. Patch Management
    b. Vulnerability Prioritization and Configuration Management (Risk-Based VM)
4. **Threat Protection**
    a. Endpoint Security
    b. Infrastructure Protection
    c. Identity Protection
    d. Segmentation
    e. Ransomware protection
5. **Threat Response and Remediation**
    a. Endpoint Detection & Response (EDR); Detection and Response tools
    b. Incident Management
    c. Automated Remediation
    d. Incident Response (IR)
    e. Ransomware Mitigation
6. **Compliance**
    a. Continuous Control Monitoring

    b. Standards and Regulations
    c. Policy Compliance
    d. FIle Integrity Monitoring
7. **Services**
    a. Managed Services
    b. Professional Services
    c. Partner ecosystem

# Vendor Assessment

## Methodology

This evaluation was conducted within the scope of SMBs and organizations with small security teams.

Vendor product feature sets were assessed across three key foundational capabilities:

- **Key Differentiators**
- **Product Capabilities**
- **Services and Support**

Vendor customer satisfaction was assessed primarily across these key parameters:

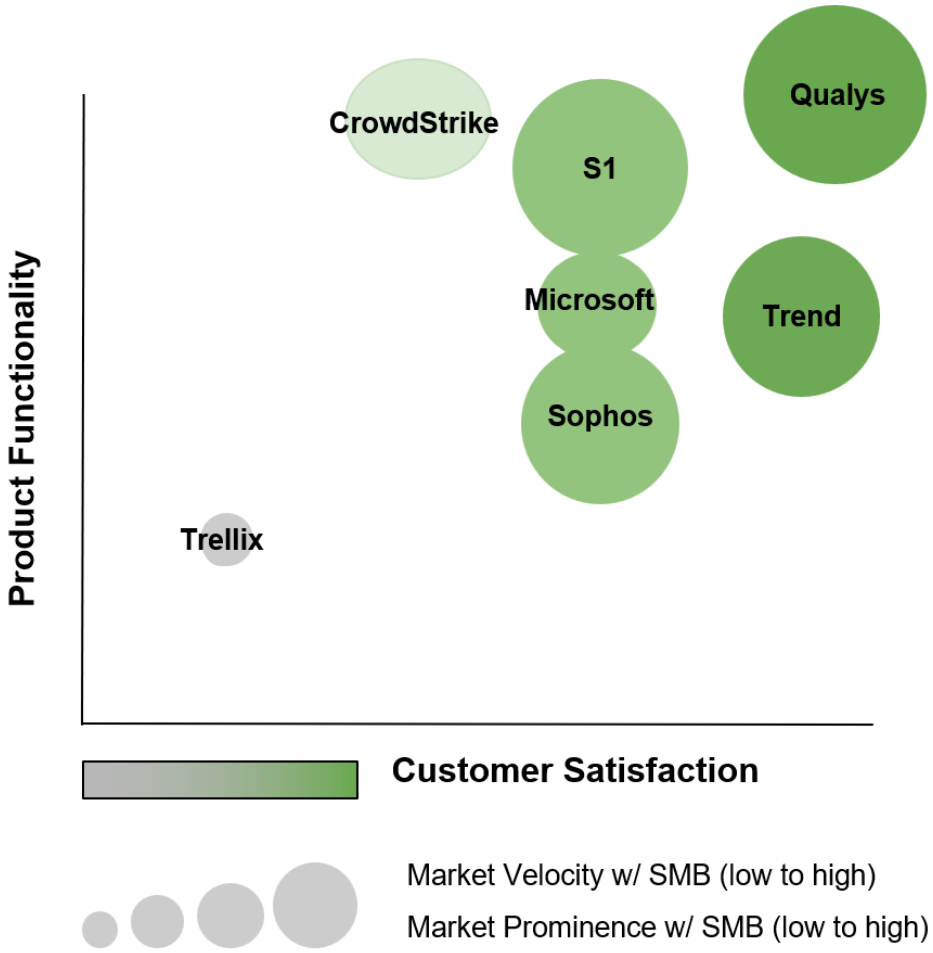
- **Saving outcomes and ROI**: What savings have been generated, how these compare to the projected ROI, how transparent the savings calculated actually are, and how it was delivered to the customer
- **Service excellence**: The proactiveness, efficacy, and stability of the services teams, any friction the customer experiences in engagement, and how readily vendors map to existing customer processes
- **Data insights**: The depth, relevance, recency of the data, vendor insights, and how easily these are actionable by the customer

Market velocity was assessed based on growth rates across customer acquisition, employee growth, regional expansion, brand development, and product innovation.

Market prominence was assessed based on size, funding, reputation, and brand awareness.

## Summary of Top Vendors

- CrowdStrike
- Microsoft
- Qualys
- Sophos
- SentinelOne
- Trellix
- Trend Micro



# Vendor Profile: CrowdStrike

**Overview:**

- **HQ Location:** Sunnyvale, California, United States
- **Founded:** 2011
- **Number of Employees:** 7,500+, 13% growth expected in the Q1 2024 (estimated)
- **Total Funding:** $485.6B
- **2023 Revenue:** $2.241B, a 54.4% increase from 2022 (estimated)

CrowdStrike is a global cybersecurity leader that operates on a cloud-native platform. The company's focus on innovation, AI-powered threat detection, and single-agent architecture has made it a trusted partner for organizations looking to protect their digital assets from cyber threats. The company's primary focus is on protecting critical areas of enterprise risk, which include endpoints and cloud workloads, identity, and data. Their platform is designed to identify advanced threats and targeted attacks, providing a comprehensive security solution for businesses.

The company's main product is the CrowdStrike Falcon, a tool designed to disrupt the cyber kill chain and contain the use of tools and protocols. This product is used in various sectors, including finance and insurance, providing identity security. CrowdStrike also offers services such as cyber incident response, the NSA has accredited. The company's approach to cybersecurity is centered on modernizing and securing cloud environments, protecting hybrid workforces, and exposing adversaries beyond the perimeter. CrowdStrike's Falcon platform provides a unified solution for cyber threat exposure management, vulnerability management, and external attack surface management.

CrowdStrike serves small security teams through five bundles across small businesses and enterprises. All bundles require a minimum purchase of five devices. Purchases of their entry-level bundle, Falcon Go, are limited to a maximum of 100 devices.

**Key Differentiators:**

- **Cloud-Native Architecture:** CrowdStrike's security platform is built from the ground up to be cloud-native, providing scalability, elasticity, and global reach.
- **AI-Powered Threat Detection:** CrowdStrike's Falcon platform uses artificial intelligence (AI) to detect and prevent threats in real-time without relying on signatures or indicators of compromise (IOCs).
- **Single-Agent Architecture:** CrowdStrike's Falcon platform uses a single lightweight agent to protect endpoints, servers, and cloud workloads, reducing complexity and improving performance.
- **Threat Intelligence:** CrowdStrike has a global team of threat hunters and researchers who provide continuous threat intelligence updates to the Falcon platform.

**Product:**

- **Falcon Platform:** CrowdStrike's flagship product is the Falcon platform, which provides a comprehensive suite of security modules, including endpoint protection, threat intelligence, incident response, and managed threat hunting.
- **Host Firewall Control:** Delivers simple, centralized host firewall management, making it easy to manage and control host firewall policies.
- **Device Control:** Provides the visibility and ability to control the safe usage of USB devices across your organization.
- **Asset Discovery:** CrowdStrike's Falcon platform discovers all internet-facing assets, including websites, domains, subdomains, and IP addresses, to provide a comprehensive view of an organization's external attack surface.
- **Vulnerability Scanning:** CrowdStrike's Falcon platform scans external assets for vulnerabilities, including web application vulnerabilities, SSL/TLS misconfigurations, and open ports.
- **Risk Assessment:** CrowdStrike's Falcon platform provides risk assessment capabilities to help organizations identify and prioritize their most critical vulnerabilities.
- **External Attack Surface Management:** CrowdStrike's Falcon platform helps organizations reduce their attack surface by identifying and mitigating vulnerabilities in their endpoints, servers, and cloud workloads.

**Services & Support:**

- **Partnership Network:** CrowdStrike boasts a well-established and internationally accessible market and network of partners, encompassing vendors that deliver a robust variety of managed services and professional expertise.
- **Professional Services:** CrowdStrike offers professional services to help customers with deployment, configuration, and ongoing management of the Falcon platform. Additional services for Incident Response assistance are sold standalone.
- **Support:** CrowdStrike provides 24/7 support to customers, including phone, email, and chat support.
- **Documentation:** CrowdStrike provides comprehensive documentation for its products and services, including user guides, technical documentation, and FAQs.
- **Community:** CrowdStrike has a vibrant community of users and experts who share knowledge and best practices through forums, blogs, and social media.

**Suitability:**

- Endpoint Protection, Vulnerability Management, CTEM, Asset Management, Platform, AI-Powered Threat Detection, Threat Intelligence, Partner Ecosystem, File Integrity Monitoring

**Incompatibility:**

- EDR, Identity Protection, MDR, Policy Compliance, File Access Monitoring, IR*

*CrowdStike EDR, Identity protection, MDR, IR are only available in Enterprise bundles, which are cost-prohibitive for small to medium businesses and smaller security teams that are on tight budgets.

- **Falcon Complete:** Falcon Complete is a MDR service that provides 24/7 monitoring and response to security incidents.
- **Falcon XDR:** Falcon XDR is a cloud-native extended detection and response (XDR) solution that integrates data from endpoints, networks, cloud workloads, and identity sources to provide a unified view of security threats.

## Vendor Profile: Microsoft

**Overview:**

- **HQ Location:** Redmond, Washington, United States
- **Founded:** 1975
- **Number of Employees:** 181,000+ employees
- **2023 Revenue:** $26B+ in cybersecurity revenue, 30% growth (estimated)

Microsoft Defender for Business is a cloud-based endpoint security solution that helps small and medium-sized businesses (SMBs) protect their devices from cyber threats. It provides comprehensive protection against malware, ransomware, phishing attacks, and other online threats.

**Key Differentiators:**

- **Cloud-native platform:** Microsoft Defender for Business is built on the Microsoft Azure cloud platform, giving it several advantages over traditional on-premises security solutions. These advantages include scalability, flexibility, and ease of use.
- **AI-powered threat detection:** Microsoft Defender for Business uses artificial intelligence (AI) to detect and respond to threats in real-time. This allows it to stay ahead of the curve on emerging threats and protect businesses from attacks that traditional security solutions may miss.
- **Endpoint Security:** Microsoft has a leading Endpoint Security platform.
- **Partner Ecosystem:** Microsoft was one of the largest list of partners worldwide.

**Product:**

- **Next-generation antivirus:** Protects your devices from known and unknown malware.
- **Defender for Endpoint:** Prevent, detect, investigate, and respond to advanced threats. Plan 1 is for SMBs and Plan 2 for enterprises.
- **Defender Vulnerability Management:** Add-on for Defender for Endpoint. Continuous vulnerability discovery and assessment, risk-based prioritization, and remediation.

- **Defender Extended Detection and Response (XDR):** Unified defense suite that coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection.
- **Purview Compliance Manager:** Provides multi-cloud regulatory assessments, continuous control assessments, regulatory updates, control mapping, and compliance scoring
- **File Integrity Monitoring (included with Defender for Cloud):** Examines operating system files, Windows registries, application software, and Linux system files for changes that might indicate an attack.

**Services & Support:**

- **Premier Partnership Ecosystem:** Microsoft is renowned for hosting the industry's largest, most well-known, and longest-standing marketplace and partnership network. It provides a global platform featuring providers known for an extensive range of top-tier managed services and professional capabilities.
- **Implementation services:** Microsoft can help businesses implement its security solution quickly and easily.
- **Managed services:** Microsoft offers various managed services through its vast partnership ecosystem that can help businesses manage their security posture, including 24/7 monitoring, incident response, and threat hunting. Organically, Microsoft only offers managed services with its enterprise-level offerings.
- **Support:** Microsoft offers a variety of support options, including phone, email, and chat support.

**Suitability:**

- Endpoint Security, EDR, XDR, AI-Powered Threat Detection, Threat Intelligence, Device Management, CTEM, Vulnerability Management, Partner Ecosystem, File Integrity Monitoring, Policy Compliance

**Incompatibility:**

- MDR, IR, Identity Protection, Cyber Asset Surface Management, File Access Monitoring

Microsoft Identity protection is only available in Enterprise bundles. MDR and IR are only available through partners, which are cost-prohibitive for small to medium businesses and smaller security teams on tight budgets.

## Vendor Profile: Qualys

**Overview:**

- **HQ Location:** Foster City, California, United States
- **Founded:** 1999
- **Number of Employees:** 2,630+, 12% growth expected in the Q1 2024 (estimated)

- **Total Funding:** $91M
- **2023 Revenue:** $555M+, a 13% increase from 2022 (estimated)

Qualys is a leading provider of cloud-based security and compliance solutions. The company's mission is to make security and compliance simple and accessible to every organization. Qualys's solutions are used by over 19,000 organizations worldwide, including many Fortune 500 companies. The company has a global presence with offices in over 60 countries, enabling it to provide local support to customers worldwide.

Qualys is committed to providing its customers with the best possible security and compliance solutions. The company's products and services are backed by a team of experienced security and compliance experts who are dedicated to helping customers stay protected from cyber threats and meet compliance requirements.

**Key Differentiators:**

- **Compliance:** Qualys is a pioneer in the cloud-based security and compliance market offering dashboards for PCI, GDPR, DORA, etc. and mapping for MITRE, CIS18, NIST, DoD Zero Trust, and more
- **Portfolio Breadth and Depth:** The company's cloud platform provides a comprehensive suite of security and compliance solutions that are easy to deploy and manage.
- **Innovation:** Qualys has a strong focus on innovation, investing heavily in research and development to stay ahead of emerging threats and compliance requirements.

**Product:**

- **Vulnerability Management:** Qualys's vulnerability management solution helps organizations identify and prioritize vulnerabilities in their IT infrastructure.
- **Asset Management:** Qualys offers a Cyber Asset Attack Surface Management solution that provides visibility into the entire attack surface, and allows customers to maintain their assets and track EOL/EOS software.
- **Identity Protection:** Qualys Identity Protection prevents credential misuse through real-time infrastructure defense.
- **External Attack Surface Management and Asset Discovery:** Qualys platform discovers all internet-facing assets, including websites, domains, subdomains, and IP addresses, to provide a comprehensive view of an organization's external attack surface.
- **Endpoint Security:** Qualys's endpoint security solution protects devices from malware, ransomware, and other threats. Qualys offers Multi-Vector EDR rather and XDR to correlate data across multiple context vectors such as asset management, vulnerability detection, policy compliance, patch management, and file integrity monitoring with a single agent and platform.
- **Policy Compliance:** Qualys's compliance management and automated remediation solution helps organizations meet a variety of compliance requirements such as PCI DSS 4.0, HIPAA 2023, CCPA, ISO, and GDPR. Includes integration with Qualys Endpoint Security to automate threat remediation.

- **File Integrity Monitoring:** A critical security and compliance solution that includes File Access Monitoring (FAM) and agentless network device support to flag suspicious file access and comply with PCI DSS 4.0, etc.

**Services & Support:**

- **Partner Ecosystem:** Qualys has a mature and globally available partner program and partnership ecosystem with providers that offer a healthy mix of managed and professional service offerings.
- **Professional Services:** Qualys offers professional services to help customers with the implementation, configuration, and management of its solutions.
- **Support:** Qualys provides 24/7 support to customers, ensuring that they can get the help they need quickly and easily.
- **Training:** Qualys offers training courses to help customers learn how to use its solutions effectively.

**Suitability:**

- Endpoint Security, Identity Protection, Vulnerability Management, CTEM, Asset Management, Platform, Threat Intelligence, Partner Ecosystem, Policy Compliance, File Integrity Monitoring, File Access Monitoring

**Incompatibility:**

- MDR, IR, AI-Powered Threat Detection, XDR

## Vendor Profile: Sophos

**Overview:**

- **HQ Location:** Abingdon, Oxfordshire, United Kingdom
- **Founded:** 1985
- **Number of Employees:** 4,500+, growth for 2024 is unknown, 10% Layoffs in 2023
- **Total Funding:** $119M
- **2023 Revenue:** Privately Held

Sophos is a leading provider of cybersecurity solutions, protecting over 500,000 organizations worldwide, including over 15,000 Managed Service Providers. The company's mission is to make cybersecurity simple and accessible to everyone. Sophos' solutions are used by firms of all sizes, from small businesses to large enterprises, as well as government agencies and educational institutions.

Sophos is committed to providing its customers with the best possible cybersecurity protection. The company's products and services are backed by a team of experienced cybersecurity experts who are dedicated to helping customers stay safe from cyber threats.

**Key Differentiators:**

- **Combined Network and Endpoint Protection:** Sophos as a wide range of offerings for customers that protect devices and networks from malware, ransomware, unauthorized access, DDoS attacks, and other threats. Includes File Integrity Monitoring for servers only.
- **Partner Ecosystem:** Sophos has one of the largest lists of partners worldwide with the largest number of MSPs.
- **MDR and Security Monitoring and Management:** Customers can use Sophos' managed security services to provide their customers with 24/7 monitoring and management of their cybersecurity infrastructure.

**Product:**

- **Endpoint Protection**: Sophos' endpoint protection solutions protect devices from malware, ransomware, and other threats.
- **Network security:** Sophos' network security solutions protect networks from unauthorized access, DDoS attacks, and other threats.
- **Device Management:** The Sophos platform allows organizations to easily configure, manage, and maintain their devices.

**Services & Support:**

- **Partner Ecosystem:** Sophos has one of the largest MSP ecosystems and is compatible with most leading cybersecurity and IT technologies.
- **MDR:** Sophos has a cost-effective offering that fits within SMB and small security team budgets.
- **Professional Services:** Sophos offers professional services to help customers implement, configure, and manage its solutions.
- **Support:** Sophos provides 24/7 support to customers, ensuring that they can get the help they need quickly and easily.
- **Training:** Sophos offers training courses to help customers learn how to use its solutions effectively.

**Suitability:**

- Endpoint Security, Network Security, MDR, Threat Intelligence, MSP Partner Ecosystem, File Integrity Monitoring (servers only)

**Incompatibility:**

- AI-Powered Threat Detection, Vulnerability Management, CTEM, Asset Management, Identity Protection, IR, Policy Compliance, File Access Monitoring

## Vendor Profile: SentinelOne

**Overview:**

- **HQ location:** Mountain View, California, United States
- **Founded in:** 2013
- **Number of employees:** 2,250+, 18% growth expected in the Q1 2024 (estimated), 5% layoffs in 2023
- **Total funding:** $697M
- **2023 Revenue:** $800m+ (estimated)

SentinelOne's primary focus is on providing autonomous cybersecurity solutions. Their main product is designed to protect the most sensitive data that resides on the endpoint and in the cloud. This product is aimed at fortifying the edges of a network with real-time autonomous protection, thereby safeguarding what matters most from cyberattacks. The company's mission is to protect organizations from cyber threats by delivering autonomous, AI-powered security solutions that prevent, detect, and respond to attacks in real time. SentinelOne's platform is used by over 4,000 organizations worldwide, including Fortune 500 companies, government agencies, and financial institutions.

The company also offers a platform called Singularity Marketplace, which is designed to maximize the value of security stacks. This platform is feature-rich and has a strong roadmap, indicating a focus on continuous development and improvement. SentinelOne's product is designed to be easy to deploy and integrate with leading cybersecurity and Information Technology tools, demonstrating a focus on user-friendly design and functionality.

**Key Differentiators:**

- **Singularity Platform:** SentinelOne is a pioneer in the cybersecurity industry, offering a next-generation endpoint protection platform that leverages artificial intelligence (AI) and machine learning (ML) to detect and respond to threats in real time.
- **AI-Powered Threat Detection:** The company's AI-powered platform, Singularity, is designed to autonomously detect and respond to threats, including zero-day attacks, ransomware, and advanced persistent threats (APTs). Enabled by robust static & behavioral AI engines, even when offline.
- **Managed Services:** SentinelOne provides four levels of MDR services with options to include Incident Response support. This is unique due to the fact that most vendors only have services as part of their Enterprise offerings.
- **Cloud-Native Architecture:** SentinelOne's platform is cloud-native, which enables it to scale and adapt to changing threat landscapes quickly.
- **Innovation:** The company has a strong focus on research and development, investing heavily in its AI and ML capabilities to stay ahead of emerging threats.

**Product:**

- **Singularity Platform:** SentinelOne's flagship product is the SentinelOne Singularity Platform, a next-generation EPP solution that leverages AI and ML to detect and respond to threats in real-time. The platform includes the following key features:

- **Autonomous threat detection and response:** SentinelOne's AI-powered platform autonomously detects and responds to threats, including zero-day attacks, ransomware, and Advanced Persistent Threats (APTs).
- **Identity Protection:** Singularity Identity prevents credential misuse through real-time infrastructure defense for Active Directory and deception-based endpoint protections.
- **Real-time visibility and control:** SentinelOne's platform provides real-time visibility into all endpoints on the network, enabling security teams to identify and respond to threats quickly.

**Services & Support:**

- **Partner Ecosystem:** SentinelOne has a mature and globally available marketplace and partnership ecosystem with providers that offer a healthy mix of managed and professional service offerings.
- **Managed Services:** Multiple tiers are available for organizations of any size or budget.
- **Professional services:** SentinelOne offers professional services to help customers with the implementation, configuration, and management of its platform. Incident Response services are available with MDR in the highest tier.
- **Support:** SentinelOne provides 24/7 support to customers, ensuring that they can get the help they need quickly and easily.
- **Training:** SentinelOne offers training courses to help customers learn how to use its platform effectively.

**Suitability:**

- Endpoint Security, MDR, IR, Platform, Identity Protection, AI-Powered Threat Detection, Threat Intelligence, Partner Ecosystem

**Incompatibility:**

- Vulnerability Management, CTEM, Asset Management, Policy Compliance, File Integrity Monitoring, File Access Monitoring

## Vendor Profile: Trellix

**Overview:**

- **HQ location:** San Jose, California, United States
- **Founded in:** 2022
- **Number of employees:** 3,400+, 4% growth expected in the Q1 2024 (estimated), layoffs in 2023 for an undisclosed amount
- **Total funding:** N/A; as a result of the merger of McAfee Enterprise and FireEye
- **2023 Revenue:** Privately Held; $2B+ (estimated)

Trellix offers a range of products and services designed to protect businesses from security threats and serves over 40,000 customers. The company's main product is Trellix XDR, a living

XDR platform that adapts at the speed of bad actors while propelling SecOps teams ahead of potential attacks. This product is designed to grow stronger, smarter, and more agile every day, providing businesses with the confidence to focus on their ambitions. Trellix's product offerings also include Endpoint Security and SecOps and Analytics solutions.

In addition to its product offerings, Trellix also provides a range of support services to its customers. These include Product Support, Downloads, and Product Documentation. The company also offers a Detection Dispute Form and a Submit a Sample service for its customers. Trellix's focus in cybersecurity is on providing a living, learning ecosystem that can adapt and evolve to keep businesses protected from the dynamic and sophisticated security threats they face.

**Key Differentiators:**

- **Combined Network and Endpoint Protection:** Trellix offers Endpoint and Network Security in a single portfolio
- **Strong Partner Ecosystem:** Wide range of partners that offer a mix of managed and professional services around the globe.
- **Threat Intelligence Depth and Breadth:** Threat Intelligence that encompasses endpoint and network threat data
- **Open Architecture:** Trellix's solutions are built on an open architecture, which enables them to integrate with a wide range of third-party security tools and technologies. This flexibility allows organizations to customize their security infrastructure to meet their specific needs and requirements.

**Product:**

- **Endpoint Protection**: Trellix’s endpoint protection solutions protect devices from malware, ransomware, and other threats. Includes limited policy compliance related only to status and not regulatory compliance.
- **Network security:** Trellix’s network security solutions protect networks from unauthorized access, DdoS attacks, and other threats.
- **Application and Change Control:** File Integrity Monitoring and protection against uninvited changes to or unauthorized control of applications, endpoints, servers, and fixed function devices

**Services & Support:**

- **Strong Partner Ecosystem:** Trellix has a strong partner ecosystem that includes MSSPs, VARs, and system integrators. This ecosystem enables Trellix to provide its solutions and services to a wide range of organizations, regardless of size or location.
- **Support:** Trellix provides 24/7 support to customers, ensuring that they can get the help they need quickly and easily.
- **Training:** Trellix offers training courses to help customers learn how to use its solutions effectively.

**Suitability:**

- Endpoint Security*, Network Security, Threat Intelligence, Partner Ecosystem, File Integrity Monitoring

*Trellix's endpoint products currently have 2 separate agents for protection and EDR. This should be considered when assessing the additional overhead required to manage this long-term when compared to other solution providers.

**Incompatibility:**

- AI-Powered Threat Detection, Vulnerability Management, CTEM, Asset Management, Identity Protection, MDR, IR, Policy Compliance, File Access Monitoring

## Vendor Profile: Trend Micro

**Overview:**

- **HQ location:** Tokyo, Japan
- **Founded in:** 1988
- **Number of employees:** 7,750+; growth for 2024 unknown
- **Total funding:** N/A
- **2023 Revenue:** $1.3B+ (estimated)

Trend Micro is a global cybersecurity company with over 35 years of experience in the field and serves over 500,000 customers. The company's primary focus is on delivering insights on known threats, vulnerabilities, and future predictions in cybersecurity. These insights are based on multiple areas of the network, including cloud, gateway, email, web, network, server, endpoint, mobile, and IoT/IioT. Trend Micro's extensive customer base and global reach allow it to provide the latest insights on the cybersecurity landscape across multiple regions, industries, and business types.

One of Trend Micro's key offerings is the Trend Micro Zero Day Initiative, the world's largest vendor-agnostic bug bounty program. This initiative allows Trend Micro to understand the latest vulnerabilities and potential exploits, providing instant protection to its customers through virtual patching technology. This technology shields applications and environments from potential threats from various sources, including Microsoft and Adobe.

In addition to its cybersecurity insights and the Zero Day Initiative, Trend Micro also offers centralized security policy, response, and visibility management. This includes centralized visibility into the network for informed decision-making and immediate action on potential threats to infrastructure or data. It also integrates with Trend Micro and complementary third-party solutions, enhancing a layered security approach. The company's centralized management provides a scalable, policy-based operational model, enabling straightforward management of for organizations at any size. Trend Micro's solutions are used by businesses of all sizes, from

small businesses to large enterprises, as well as government agencies and educational institutions.

**Key Differentiators:**

- **Portfolio Breadth and Depth:** Trend Micro is a global leader in cybersecurity, providing a wide range of solutions to protect organizations from cyber threats.
- **Platform:** The company's solutions are known for their high efficacy, ease of use, and comprehensive protection.
- **Innovation:** Trend Micro has a strong focus on innovation, investing heavily in research and development to stay ahead of emerging threats. Many of their offerings are engineered and built in-house versus through acquisitions.
- **Global Presence:** The company has a global presence with offices in over 60 countries, enabling it to provide local support to customers worldwide. Their strongest presence is in the Asia Pacific region.

**Product:**

- **Combined Network and Endpoint Protection:** Trend Micro as a wide range of offerings for customers that protect devices and networks from malware, ransomware, unauthorized access, DdoS attacks, and other threats.
- **Endpoint Security:** Trend Micro has a unified endpoint security solution that protects devices from malware, ransomware, and other threats. It includes features such as antivirus, anti-malware, intrusion prevention, and application control.
- **Network Security:** Trend Micro's Network Security products detect and block advanced threats, such as malware, ransomware, and phishing attacks. It uses a combination of machine learning and behavior analysis to identify and stop threats as well as advanced threats, such as zero-day attacks and targeted attacks. It includes features such as intrusion prevention, firewalls, and web filtering.
- **Device Control:** Provides the visibility and ability to control the safe usage of USB devices across your organization.
- Integrity Monitoring: Module that scans for unexpected changes to registry values, registry keys, services, processes, installed software, ports and files on Deep Security Agents.

**Services & Support:**

- **MDR:** Trend Micro provides organizations with 24/7 monitoring and response to cyber threats. It includes features such as threat hunting, incident investigation, and containment.
- **Professional Services:** Trend Micro offers professional services to help customers with the implementation, configuration, and management of its solutions.
- **Support:** Trend Micro provides 24/7 support to customers, ensuring that they can get the help they need quickly and easily.
- **Training:** Trend Micro offers training courses to help customers learn how to use its solutions effectively.

**Suitability:**

- Endpoint Security, Network Security*, MDR, IR, Vulnerability Management, Threat Intelligence, Partner Ecosystem, File Integrity Monitoring

*Network security is not included in Trend Micro's SMB and basic offerings but products can be purchased as an additional addon for additional cost. This may be too costly for most budgets.

**Incompatibility:**

- AI-Powered Threat Detection, CTEM, Asset Management, Identity Protection, Policy Compliance, File Access Monitoring

## Other Vendors

These vendors are generally local/regional or provide only part of the combined feature set across cybersecurity:

- Avira
- BluSapphire
- Broadcom Symantec
- ESET

## Recommendations

**To effectively manage the cybersecurity challenges, leaders responsible for managing solutions must:**

- **Address core use cases** by researching cybersecurity market dynamics and generally available capabilities and selecting leading cybersecurity providers that have product features, customer support, and pricing models that meet all your requirements.
- **Determine core requirements such as vulnerability management and endpoint protection, detection, and response for cybersecurity maturity against frameworks such as the National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), Zero Trust, Cybersecurity Maturity Model Certification (CMMC), etc. Also, file integrity monitoring and policy compliance requirements to ensure audit readiness for PCI DSS 4.0, HIPAA 2023, CCPA, GDPR, etc.**
- **Formalize a business case by comparing the costs** of cybersecurity and compliance solutions and resourcing against smart objectives that align with strategic value for your organization, with clear and agreed-upon measures of tangible and intangible benefits.
- **Maximize Return On Investment (ROI)** by engaging all key stakeholders, including but not limited to finance, procurement, line of business owners, asset management, IT security, digital workplace, and application leaders, to cover all phases of the cybersecurity solution life cycle.

# Conclusion

In conclusion, this Lionfish Tech Advisors Evaluation Report has provided a comprehensive evaluation of leading cybersecurity solutions tailored to the needs of small to medium-sized businesses and organizations with small to medium security teams. While each vendor presents unique strengths and innovative features, it's imperative that your organization aligns these capabilities with your specific cybersecurity and compliance demands and operational context. The varying pros and cons of the solutions from the leading vendors CrowdStrike, Microsoft, Qualys, Sophos, SentinelOne, Trellix, and Trend Micro underscore the importance of a meticulous selection process based on core use cases and success criteria most relevant to your enterprise.

Before making a commitment, it is crucial for decision-makers to engage directly with a short list of potential vendors—this is a pivotal step in the journey toward securing your digital assets. Initiating a dialogue, experiencing firsthand product demonstrations, and conducting a thorough proof of concept (POC) will illuminate the practical effectiveness of each solution within your unique environment. Lastly, a well-negotiated contract that aligns with your budget while fulfilling all business and cybersecurity requirements will ensure an investment that is cost-effective and robust in safeguarding against the evolving threat landscape.

By carefully considering the insights provided in this guide, your organization will be well-equipped to select a cybersecurity solution that delivers both protection and value. Remember, the goal is not just to purchase a cybersecurity product but to forge a partnership with a vendor that will empower your small security team to achieve a strong and resilient cybersecurity posture for the long term.

# About Lionfish Tech Advisors

Lionfish Tech Advisors offers advice to help businesses with their digital enterprise and IT initiatives. They work with enterprise and finance leaders, CIOs, CxOs, and technology organizations to give practical and strategic advice that can help modernize and transform their businesses. Their advice is aimed at helping businesses understand and meet the changing demands of their customers. Lionfish Tech Advisors uses proven methodologies and industry best practices to help businesses overcome complex challenges and make decisive actions with confidence. Their analysts have decades of extensive experience working with a range of global and industry-leading clients. Lionfish Tech Advisors takes an unbiased approach and connects with subscribers on a deep level.

# Methodology

*Lionfish Tech Advisors Report: Evaluating Cybersecurity Solutions for Small Security Teams* is for buyers considering their purchasing options in a technology marketplace and is based on our analysis and opinion. To offer an equitable process for all participants, Lionfish Tech Advisors follows a publicly available methodology, which we apply consistently across all participating vendors.

# Copyright