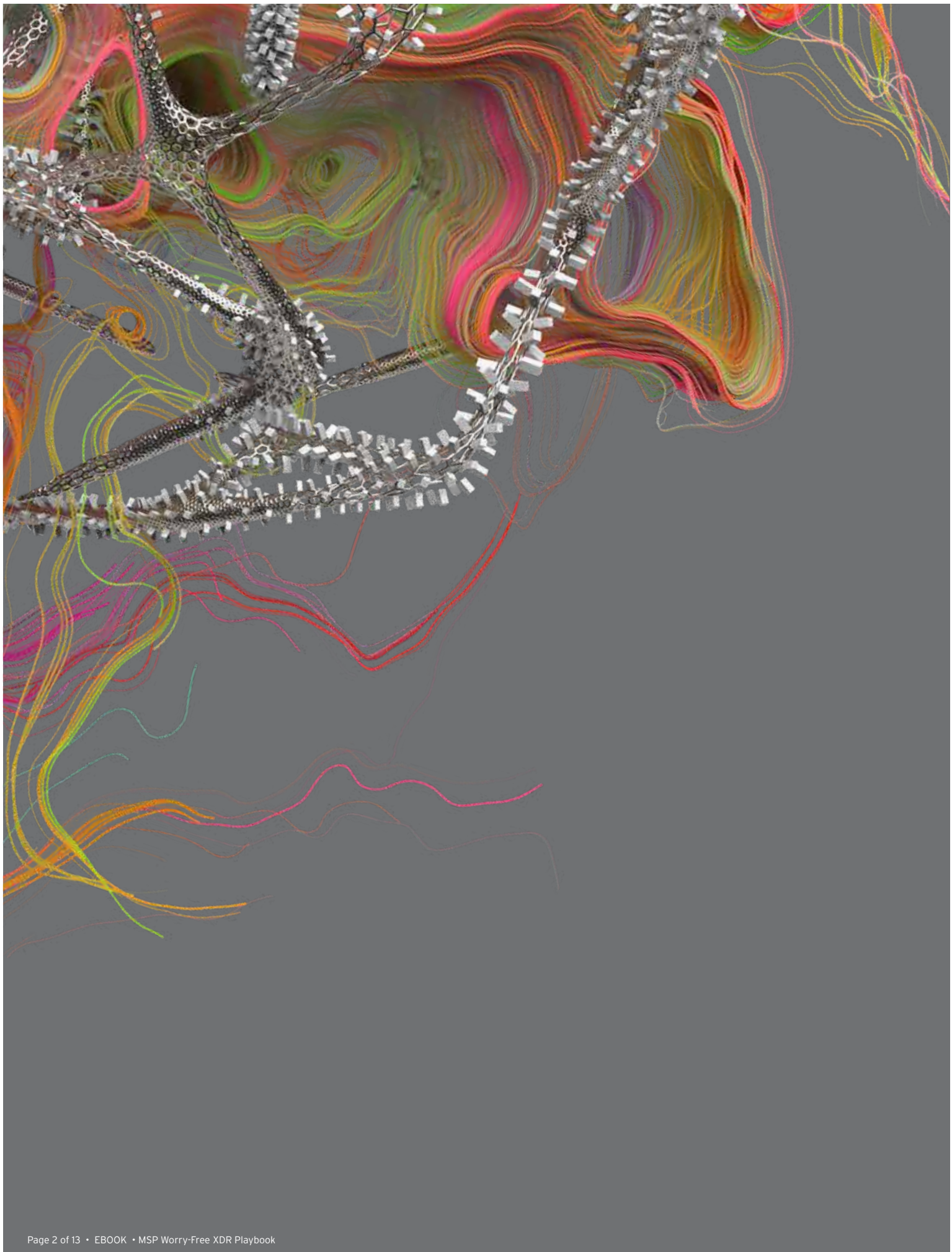


THE ART OF CYBERSECURITY

A complex, abstract digital graphic composed of numerous thin, overlapping lines in various colors (red, green, blue, yellow, pink) that form a dense, spherical structure. The lines appear to be data streams or network connections, creating a sense of depth and movement.

# MSP WORRY-FREE XDR PLAYBOOK

Do more. See more. Earn more.



## Table of Contents

<b>Part 1: What Issues are Your MSP Customers Facing?</b> .....	4
Ah, the good old days.....	4
The good old days are over. ....	4
But that doesn't mean the bad guys have won. ....	6
<b>Part 2: Why MSPs Need to Evolve Past EDR</b> .....	6
EDR is simply not enough.....	6
In comes Trend Micro™ Worry-Free™ XDR.....	7
Threat actors look beyond the endpoint, you should too. ....	7
Without the tools to identify threat indicators, detection is dangerously slow.....	9
The skills gap is widening, your clients need you more than ever.....	9
<b>Part 3: XDR Brings a World of Opportunities to MSPs</b> .....	10
Strengthen your reputation. ....	10
Increase profitability .....	10
Boost productivity.....	11
<b>Part 4: You Need More Worry-Free in Your Life</b> .....	12

## Part 1: What Issues are Your MSP Customers Facing?

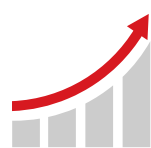
Once upon a time, strong cybersecurity could be achieved with a few simple actions. You would lock down your client's endpoints by employing antivirus protection, run a few scans, and bam! The customer is protected and all would be peachy.

Ah, the good old days.

Unfortunately, threat actors did not take the hint and just give up. Instead, they adapted, became more sophisticated and more dangerous in their quest to steal data, compromise vulnerabilities, and gain monetary rewards through methods like ransomware, phishing, and business email compromise (BEC). Due to unknown threats and the introduction of serverless and fileless malware, it is now harder to tell the good from the bad. In addition, corporate employees are now working remotely, from home and around the world, all the while utilizing a variety of devices and cloud services.

The good old days are over.

Despite advancements in cybersecurity over the past decade, data breaches are actually getting worse. Threat actors are becoming stealthier, more informed, and organized. According to a study conducted by Ponemon Institute, there has been a 67% increase in security breaches over the last five years, resulting in an 11% growth over last year<sup>1</sup>. Criminals recognize that there is a widening skills gap within the cybersecurity sector and that more organizations are becoming susceptible to poor security hygiene, and they are taking advantage of this.



There has been a 67% increase in security breaches over the last five years, resulting in an 11% growth over last year

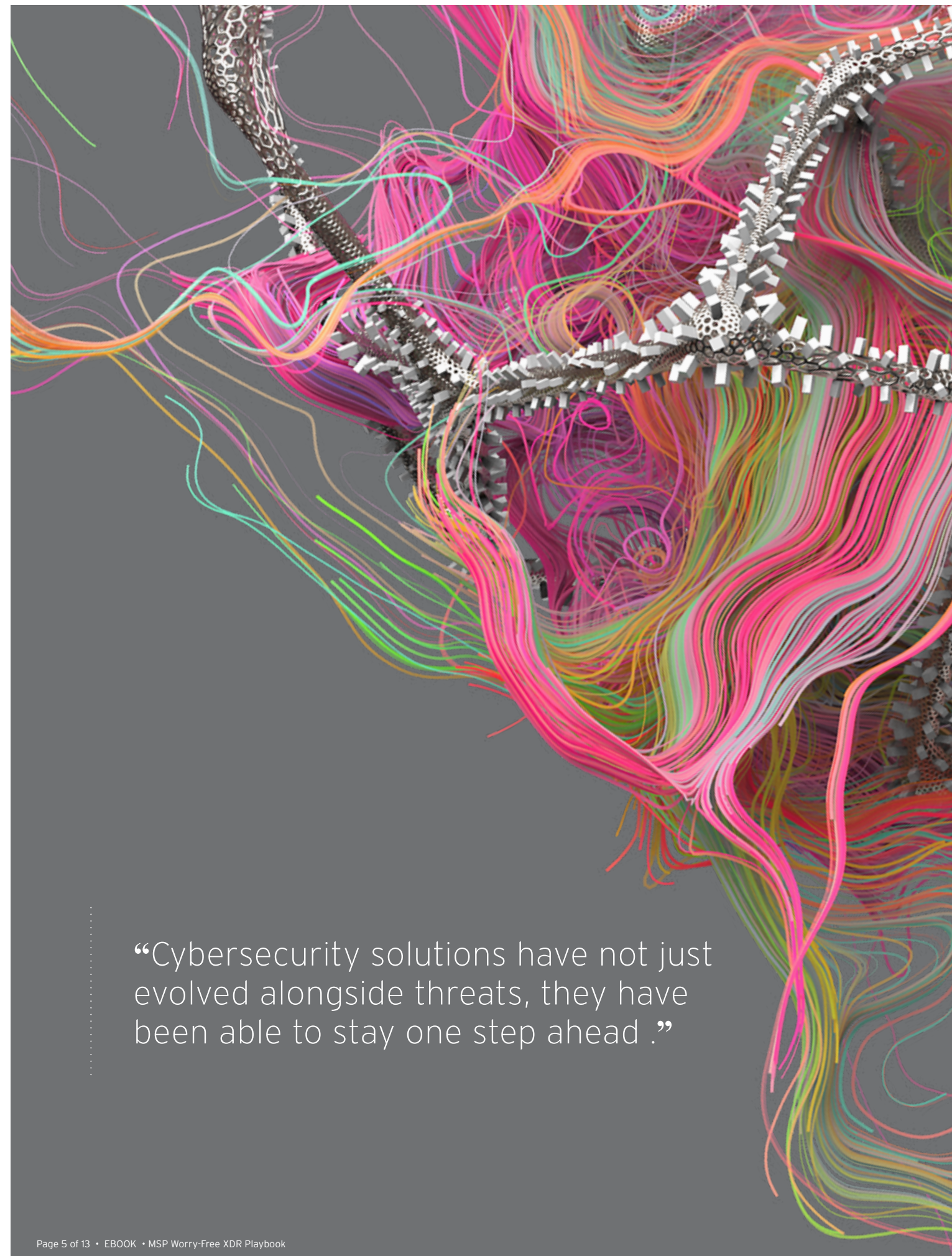
As of 2018, the average annual cost of a cyberattack has reached a whopping sum of US\$13 million, rising 12% from 2017's already-staggering number of US\$11.7 million<sup>2</sup>. Couple this with the fact that IBM Security has placed the average cost of a single data breach at US\$3.86 million, a 6.4% increase over a single year<sup>3</sup>—it is clear that MSPs need to become more diligent and proactive than ever.

Simply put, cybercrime is no longer child's play. It is big business for the criminals, not to mention potentially catastrophic for those who fall victim.

<sup>1</sup> [The Cost of Cybercrime, Ponemon Institute LLC & Accenture](#)

<sup>2</sup> [Ibid](#)

<sup>3</sup> [2018 Cost of a Data Breach Study, Ponemon Institute LLC & IBM Security](#)



“Cybersecurity solutions have not just evolved alongside threats, they have been able to stay one step ahead.”

But that doesn't mean the bad guys have won.

In fact, it is the contrary. Cybersecurity solutions have not just evolved alongside threats, they have been able to stay one-step ahead. Over the past few years, endpoint detection and response (EDR) has proven to be a game changer when it comes to security. Modern EDR does not just detect and respond to threats; it employs advanced detection capabilities, such as behavioral analysis, pre-execution machine learning, runtime machine learning, and vulnerability protection. Before EDR, an organization was left with very little visibility and context into a breach. It was difficult to determine where an attack originated, how long endpoints had been under attack, and who may have been affected by the attack.

## Part 2: Why MSPs Need to Evolve Past EDR

EDR is simply not enough..

Although EDR is an effective tool for detecting and responding to stealthy attacks, it only focuses on the endpoint, hence the "E" in EDR. Far too many MSPs utilize a variety of separate security tools to detect threats across multiple security layers. For example, EDR only has visibility on endpoints and possibly servers but does not perform detection and response throughout an organization's email. This lack of integrated contextual visibility results in an incomplete view of the breach and makes it impossible to properly respond to attacks.

This security gap can prove to be dangerous for many organizations as email is the number one entry point for malware. According to Verizon's 2019 Data Breach Investigation Report, 94% of malware detected by an organization was delivered via email.<sup>4</sup>



94% of malware detected by an organization was delivered via email

Utilizing standalone security solutions to spot threats often leads to siloed information and an overload of threats that prove to be too demanding to manually correlate and prioritize, increasing the probability of missing threats altogether.

<sup>4</sup> [The Cost of Cybercrime, Ponemon Institute LLC & Accenture](#)

<sup>5</sup> [2019 Data Breach Investigations Report, Verizon](#)

In comes Trend Micro™ Worry-Free™ XDR.

When it comes to a client's security posture, MSPs are responsible for keeping their organization safe. But a successful MSP must also demonstrate the ability to utilize the latest and most advanced security available. This improves your reputation, gives you the tools to be more productive, and allows you to increase revenue while ensuring your customers have the best protection possible against today's and tomorrow's threats.

“A successful MSP must also demonstrate the ability to utilize the latest and most advanced security available.”

The integrated, cross product, and unified security approach provided by Trend Micro Worry-Free XDR gives organizations the best protection, central visibility and monitoring, investigation capabilities, and automated response.

Utilizing artificial intelligence (AI) and machine learning, Worry-Free XDR, powered by XGen™ security, is designed to convert hundreds or even thousands of alerts into a digestible amount of high-confidence signals to correlate security events across an IT environment and respond to those threats.

Threat actors look beyond the endpoint, you should too.

Security breaches have increased 67% in the past five years, but only 33% of enterprises say they use multiple security tools<sup>5</sup>. Today's threats require organizations to look beyond the endpoint into email and other threat vectors. Worry-Free XDR enables that.



“We understand the telemetry from all of those systems incredibly well, so we’re able to derive deeper insights. We believe that will be an advantage for us in this market evolution towards XDR.”

Eric Skinner  
Vice-President for Market Strategy, Trend Micro

Without the tools to identify threat indicators, detection is dangerously slow.

Threat actors prey on organizations who are susceptible to slow responses to threats. Malware variants are stealthy for a reason, the longer it takes to discover that an attack is present within an organization, the more damage the threat can do.

The truth is, a majority of attacks have ample time to spread within an organization and steal data before sending it out to a command and control (C&C) server. According to Verizon’s 2019 Data Breach Investigations Report, 56% of breaches studied took several months or even longer to discover<sup>6</sup>. In that time, your client’s data and intellectual property could be severely compromised.



56% of breaches studied took several months or even longer to discover

The skills gap is widening, your clients need you more than ever.

The current cybersecurity skills gap is a bona fide crisis. In 2019, (ISC)<sup>2</sup> estimates the current workforce gap has topped 4 million employees globally<sup>7</sup>. Already significantly higher than the 1.8 million employee gap (ISC)<sup>2</sup> previously predicted for the year 2022<sup>8</sup>.

Due to this widening security gap, it goes without saying that cybersecurity professionals are scarce and expensive, in turn making it tougher for organizations to obtain the skill needed to combat threats. This is where MSPs can step in and offer their expertise and assistance providing clients with managed security solutions.

Trend Micro enables MSPs with Worry-Free XDR. This solution gives organizations detection and response beyond the endpoint—correlating data automatically across email and endpoint in a single console. MSPs will be able to offer clients the protection that today’s digital world demands through full visibility into customer’s environments. Visibility is the key to fending off threat actors, as giving your clients full visibility will set you apart from the competition.

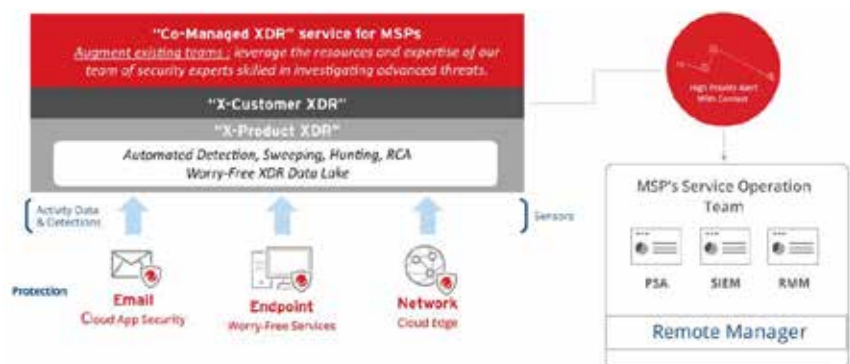
<sup>6</sup> [3 Reasons MSPs Must Evolve Beyond Endpoint Detection and Response](#)

<sup>7</sup> [2019 Data Breach Investigations Report, Verizon](#)

<sup>8</sup> [\(ISC\)<sup>2</sup> Cybersecurity Workforce Study, 2019](#)

## Part 3: XDR Brings a World of Opportunities to MSPs

With the evolution from EDR to XDR, as well as the introduction and quick rise of advanced malware such as ransomware and fileless malware, the small and medium businesses that make up the bulk of an MSP's customer base are in dire need of help when fortifying their cyber defenses.



Here's a look at the opportunities that come with moving your customers beyond EDR to Trend Micro Worry-Free XDR.

### Strengthen your reputation.

Keeping your customers protected from today's evolving threats is of utmost importance. There are very serious risks and costs associated with undetected or slow to detect threats in an organization. Reduce your customer's risk of a major breach and damage to your MSP's reputation.

*Trend Micro Worry-Free XDR solution provides:*

- **A clearer contextual view of threats** by inspecting more relative alerts across the endpoint and email. Events that seem benign on their own suddenly become meaningful indicators of compromise. This allows MSPs to connect more dots into a single view, enable more insightful investigations, and gives you the ability to detect threats earlier.
- **More effective analysis** with native integration between endpoint and email. Trend Micro Worry-Free XDR sensors benefit from a deep understanding of data sources. This results in more effective analytics compared to having data from different standalone products that aren't integrated together.
- **An ideal opportunity to keep customers safe and your reputation untarnished.** MSPs can fortify their clients against the cyber threats of today and tomorrow by taking advantage of the [Trend Micro MSP Program](#).

### Increase profitability

The formula is quite simple. Offer your customers more robust security services so you can better meet market demands. But not all MSPs follow this rule. Open the door for additional revenue-generating opportunities through proactive and reactive security services.

*Trend Micro Worry-Free XDR solution provides:*

- **Additional capabilities.** This includes email detection and response capabilities in addition to the endpoint, opening up additional revenue streams for MSPs looking to expand a client's EDR capabilities.
- **Co-managed XDR services.** MSPs are given the opportunity to leverage the resources and expertise of Trend Micro's team of security experts who are trained to investigate and respond to advanced threats on your behalf.
- **Avenues for MSPs to meet business objectives.** Trend Micro offers a number of options for MSPs to gain additional revenue, including:
  - Pay-as-you-go, usage-based licensing
  - No upfront capital or commitments
  - Aggregate billing
  - Upsell and cross-sell opportunities
  - [TrendSetters Rewards Program](#)
  - [Trend Micro MSP Partner Referral Program](#) Additional recurring revenue opportunities through broad product portfolio

### Boost productivity.

Prevent downtime, lost productivity, and eliminate angry phone calls from your customers. Sounds like a dream, doesn't it?

*Trend Micro Worry-Free XDR solution provides:*

- **MSPs with a better position to resolve security issues before they become catastrophic.** Since Worry-Free XDR can act on your behalf without sending data to the cloud or waiting for a response, organizations are given the ability to respond faster with fewer resources, while MSP teams become free from labor-intensive investigations.
- **Actionable and complete visibility for spotting active intrusions.** One console delivers native integration between endpoints and email, providing you with cross product, contextual information that gives you immediate visibility.
- **Prioritized view of threats across the organization** by correlating threats across the organization and adding expert threat intelligence, AI, and big data analytics, security personnel will get fewer, more meaningful, and richer alerts—prioritized by severity.

## Part 4: You Need More Worry-Free in Your Life

Since cyberattacks have become more rampant, sophisticated, and stealthy MSPs need to take the next step to stay one-step ahead of the bad guys. Trend Micro Worry-Free XDR is that next step.

According to a recent study conducted by Ninja RMM, only 51% of MSPs are currently using EDR<sup>9</sup>. With 35% of MSPs citing that the major hurdle keeping them from adopting detection and response is that the market is crowded and confusing<sup>10</sup>.



Only 51% of MSPs are currently using EDR.

Trend Micro Worry-Free XDR is designed to make detection and response simple, offering centralized and automate licensing and billing, multi-tenant management across solutions, third-party integration with remote monitoring and management (RMM) and professional service automation (PSA) tools, dedicated 24/7 MSP technical support, along with channel account and technical account management.

As an MSP, your clients rely on your knowledge, expertise, and ability to stay one-step ahead of the bad guys. Trend Micro does all of this for you - easily, effectively, and Worry-Free.

<sup>9</sup> [Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher](#)

<sup>10</sup> [Ibid](#)

