


# Beat Cybercriminals at Their Own Game

A Guide to Winning the Vulnerability Race and Protecting Your Organization



# Contents

- 3 Introduction: Staying ahead of cybercriminals
  - 4 Chapter 1: Vulnerabilities and how they are exploited
  - 7 Chapter 2: A by-the-numbers look at vulnerabilities
  - 8 Chapter 3: How vulnerability research works
  - 10 Chapter 4: The leader in the vulnerability research market
  - 12 Chapter 5: Wanted: Security researchers
  - 13 Chapter 6: Protection before and after vulnerabilities are disclosed
  - 15 Chapter 7: Greater security for everyone
  - 16 Next steps
- 

## INTRODUCTION

# Staying ahead of cybercriminals

Stealth is the watchword in vulnerability research. That's why relatively few people know the true extent of the value that ethical vulnerability research delivers to individuals, companies, governments, and software vendors.

The truth is that vulnerability researchers—those who report vulnerabilities to vendors for mitigation—continually race to stay ahead of cybercriminals and malicious actors. The goal? To identify vulnerabilities in our vast network of systems before they can be discovered and exploited for malicious purposes.

This e-book shines a spotlight on the expanding, increasingly essential market that is vulnerability research today. You'll gain an understanding of what vulnerability research can accomplish, and at the same time, be introduced to the industry-leading role that Trend Micro plays within the world of vulnerability research.

More importantly, you'll learn not only how this research helps everyone better protect their systems against exploitations of vulnerabilities, but specifically how Trend Micro customers can take advantage of protection far ahead of actual public disclosure of vulnerabilities.

## DID YOU KNOW ?

The number of vulnerabilities published every year continues to grow. MITRE's Common Vulnerabilities and Exposures (CVE) List included 894 CVEs in 1999, 23,269 CVEs published in 2020, and 28,695 in 2021.

Source: Common Vulnerabilities and Exposures List, The MITRE Corporation

## CHAPTER 1

# Vulnerabilities and how they are exploited

What is ...



### **A vulnerability?**

It's a programming error or flaw that can potentially be exploited by cybercriminals to bypass security and gain access to a system or network. Given the complexity and amount of software today, vulnerabilities are widespread and difficult to identify.



### **An exploit?**

When cybercriminals want to attack using a vulnerability, they may create an exploit—that is, code that can be used to take advantage of the vulnerability. Exploits are often sold on the underground market to would-be attackers who use them to control or damage a device, network, or application.



### **A zero-day attack?**

When an attack is launched that exploits a previously unknown vulnerability, it is called a zero-day attack, or simply a zero-day.



### **A zero-day vulnerability?**

A vulnerability that has been newly disclosed but is not yet patched is a zero-day vulnerability. That's because the vendor essentially has zero days to fix the issue or has chosen not to fix it.



### **An undisclosed vulnerability?**

This is a vulnerability that has been discovered by a security researcher and reported to a bug-bounty program (a rewards program for reporting vulnerabilities). The vulnerability is disclosed to the affected vendor but is not disclosed to the general public until a patch is issued.

## Which organizations are impacted?

Any organization that has systems (with vulnerabilities) that are:

- Not yet patched
- Obsolete, and therefore no patch will be developed
- Unpatchable because of device policies and restrictions (a.k.a. forever day)
- Not protected by countermeasures empowered by the latest vulnerability research

## What are the risks?

Cybercriminals actively seek to use vulnerabilities to:

- Gain access and escalate privileges in systems
- Conduct denial-of-service attacks
- Exfiltrate data
- Install malware
- Modify files and databases
- Take control of systems

## How can exploited vulnerabilities impact your business?

- Loss of consumer/customer trust
- Revenue loss
- Decreased shareholder value
- Mitigation costs
- Potential fines for non-compliance with data protection regulations

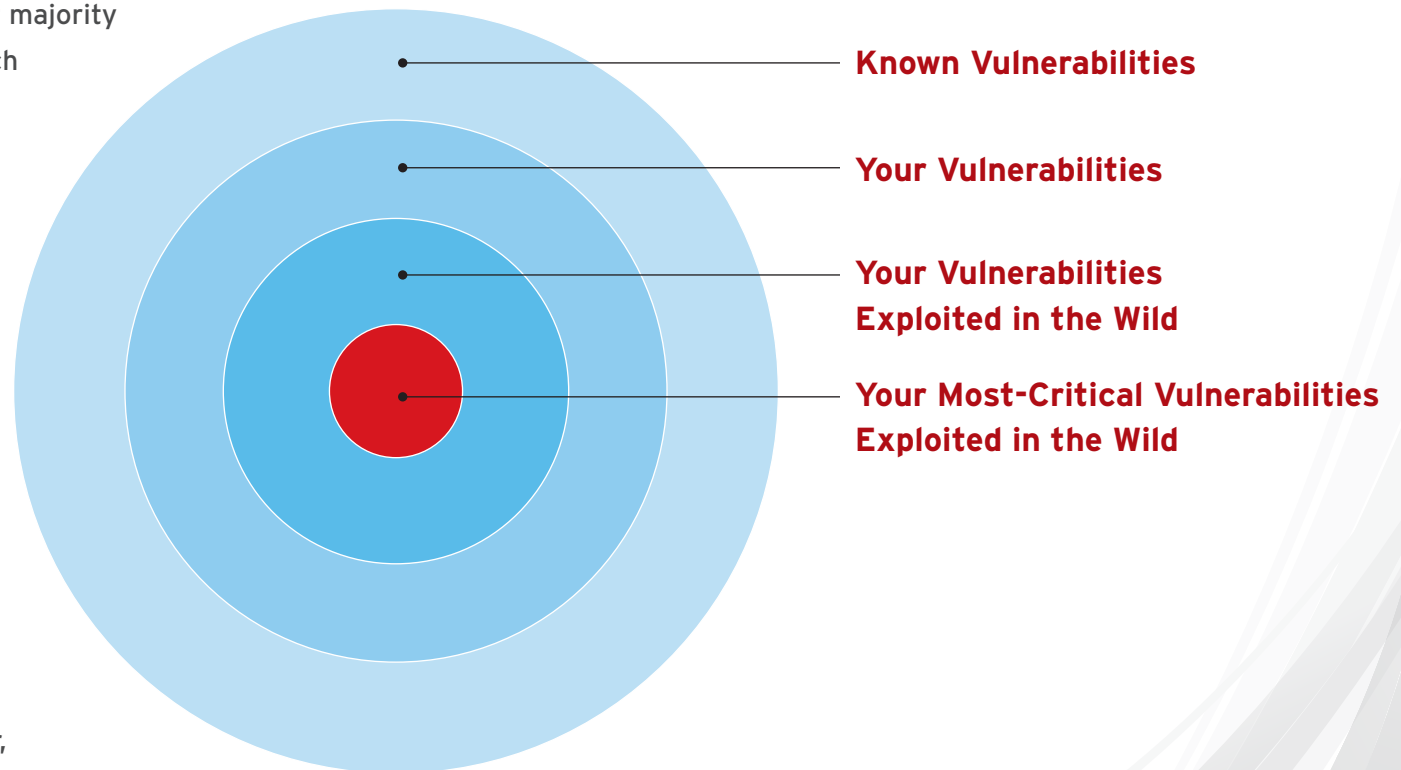


# Creating a prioritized patching process

According to research and analysis firm Gartner, vulnerabilities and their exploitation are still the root cause of most information security breaches.<sup>1</sup>

Yet patching every vulnerability immediately throughout your ecosystem is impossible for the vast majority of organizations. Instead of trying to patch all vulnerabilities as quickly as possible, Gartner and other industry analysts recommend focusing on aligning vulnerability management priorities with the biggest security threats.

One way to do this is to focus first on those vulnerabilities that are present within your operating systems, devices, and applications that are also actively being exploited in the wild. This significantly reduces the number of vulnerabilities that you need to patch while mitigating risks for your business. Another factor to consider, of course, will be the level of potential impact associated with any given vulnerability. Those that are not only being exploited in the wild but also designated as “critical” or “important” due to the degree of compromise they enable (providing remote access to a system, for example), will certainly warrant attention before all others.



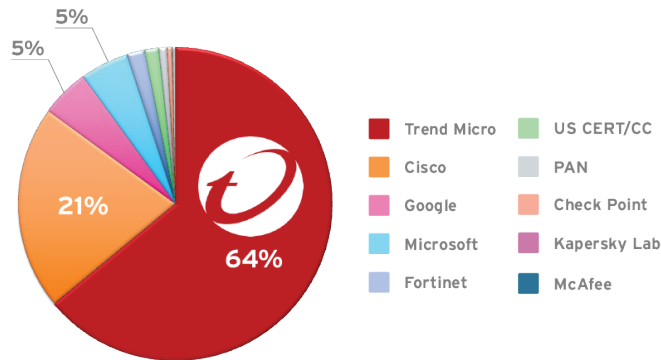
1. [Focus on the Biggest Security Threats, Not the Most Publicized, Gartner](#)

## CHAPTER 2

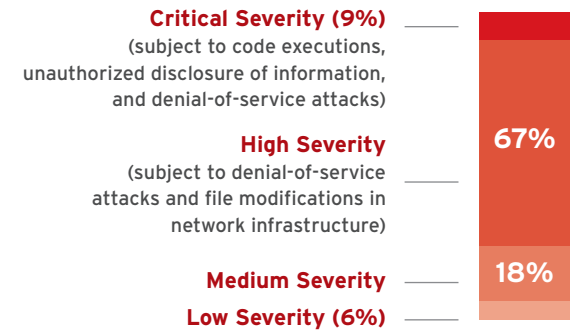
# A by-the-numbers look at vulnerabilities

**1,543** total number of vulnerabilities disclosed by public vulnerability reporting organizations (a subset of the total number of published vulnerabilities and exposures) in 2021.

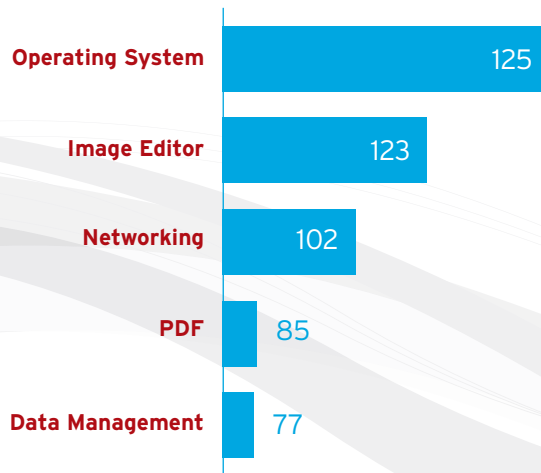
**IHS Markit Vulnerability Disclosure Market 2022**



### Severity of All Vulnerabilities Disclosed in 2021



### Top Five Vulnerability Types in 2021



### In 2021, Trend Micro Disclosed:

**63.9%**  
of the publicly reported vulnerabilities

**68%**  
of the 1,168 critical and high-severity vulnerabilities reported

## CHAPTER 3

# How vulnerability research works

Vulnerability research is a critically important, yet chronically misunderstood, part of protecting users, companies, and governments from cyberattack. The discipline encompasses all the various processes that engineering teams and security researchers use to pinpoint and disclose flaws in software programs that could lead to security issues. These efforts include reverse engineering, fuzzing, source code analysis, and an array of other techniques to uncover potential vulnerabilities.

However, not everyone conducting vulnerability research is law-abiding. In fact, the total vulnerability research market includes:



### **Vulnerability**

Bug bounty programs, hacking contests, and security researchers identify vulnerabilities and use responsible disclosure to create accountability.



### **Government market**

Some legitimate companies operate in a legal ambiguous zone within the zero-day market, selling exploits to governments and law enforcement agencies in countries across the world.



### **Underground market**

In the underground market, flaws are sold to the highest bidder. They can then be used to create exploits for disrupting private or public individuals, businesses, and groups.

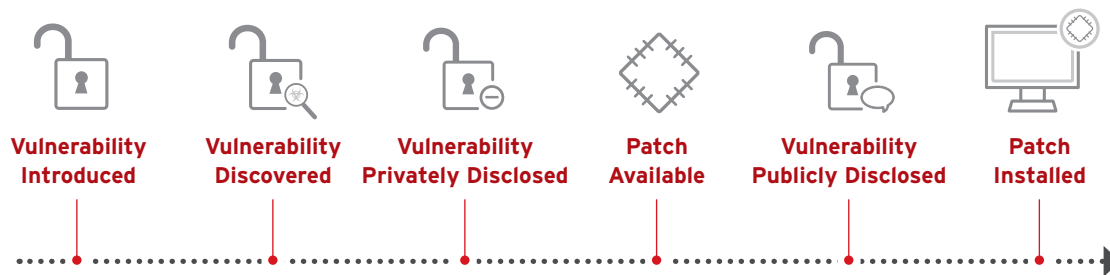


## The countdown to public disclosure

Organizations such as Trend Micro follow a coordinated disclosure process to report vulnerabilities to manufacturers privately, giving them (in Trend Micro's case) 120 days to address the issue before it is made public.

The countdown-clock nature of responsible disclosure pushes companies to handle the issue quickly and effectively, fostering accountability and transparency across the software ecosystem.

### Vulnerability Life Cycle



## DID YOU KNOW ?

A bug bounty is a rewards program for reporting vulnerabilities. Reputable vendors such as Intel, Yahoo!, Snapchat, and many others encourage ethical hacking of their software through bug bounty programs. Some of the top bounties paid by companies for bugs (programming flaws) include:

- **Dropbox™**: Offers between \$12,167 and \$32,768 for a discovered vulnerability
- **Apple**: Will pay \$200,000 to the bug bounty hunter who can extract data protected by Apple's Secure Enclave technology
- **Yahoo!**: Offers to pay as much as \$15,000 for detecting important bugs in its system
- **Google**: Will pay \$31,337 for design and implementation issues in its Google applications
- **Microsoft**: Will pay a maximum of \$250,000 for a critical and important vulnerability in its Online Services

Source: [Guru99, "Top 20 Bug Bounty Programs in 2022"](#)

## CHAPTER 4

# The leader in the vulnerability research market

At Trend Micro, our entire focus is on making the world safe for exchanging digital information. Protecting more than 500,000 companies, so they can go further and do more, we dedicate significant resources to:

### **In-house research**

The threat researchers and data scientists in Trend Micro Research labs around the world identify and disclose new vulnerabilities across a wide range of platforms, including operating systems (Windows, Linux, Mac, and others), applications (consumer and business), and mobile platforms and devices. Our extensive capabilities include vulnerability analysis, malware and exploit analysis, security product development, and custom research. Using workflows and techniques refined through years of collaboration with our partners, our highly skilled team of researchers can reverse engineer a security threat and provide protection to our clients quickly.

### **Bug bounty program**

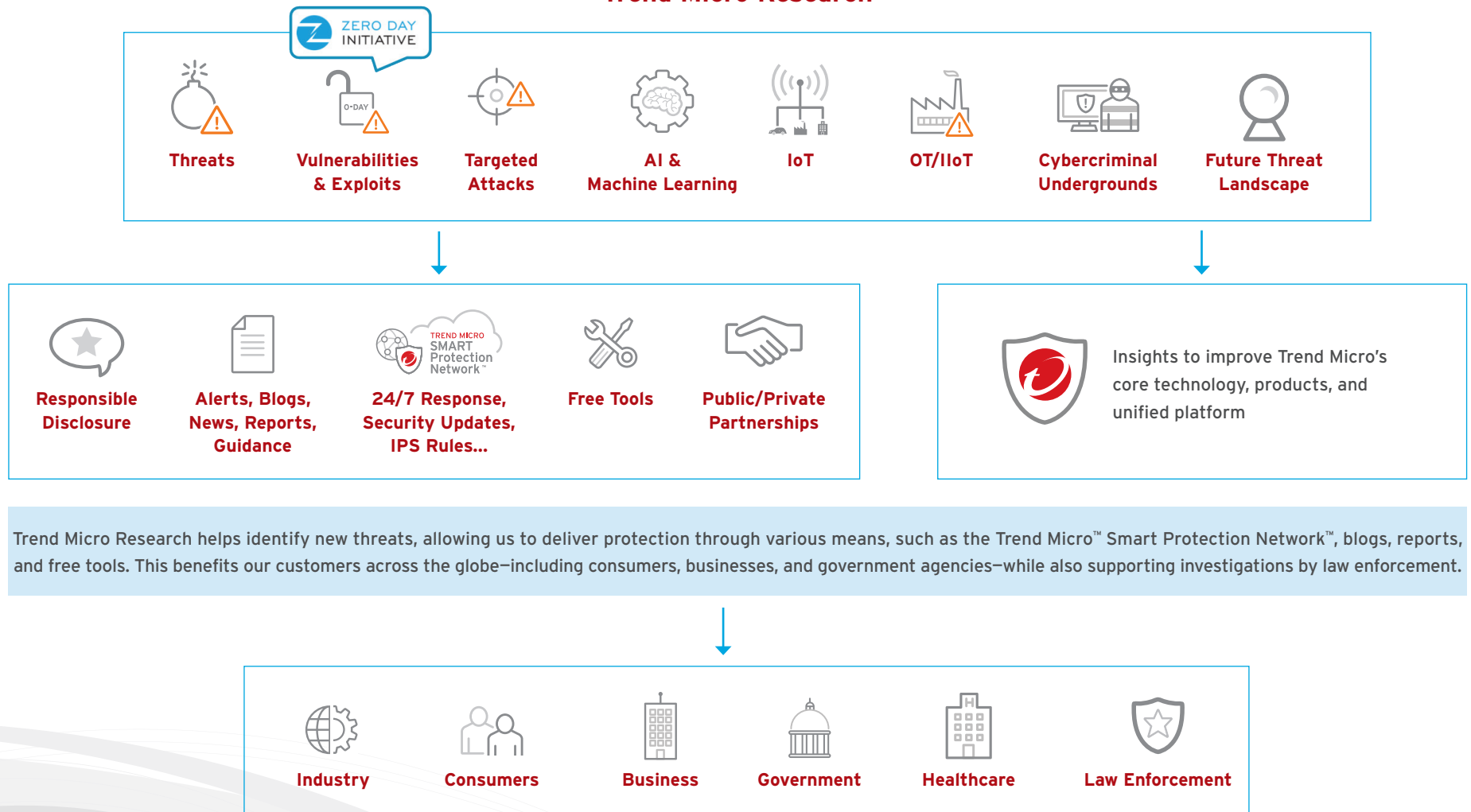
Bug bounty program: The world's largest vendor-agnostic bug bounty program, Trend Micro™ Zero Day Initiative™ (ZDI) is the leader in global vulnerability research and discovery. More than 10,000 independent researchers across the globe contribute to the [Zero Day Initiative](#) program.



## Internet of Things (IoT), industrial IoT (IIoT) and operational technology (OT) research

Trend Micro actively invests in research that identifies how devices and the processes they use could be exploited by threat actors and then determines how to protect them. For example, our research includes identifying vulnerabilities in robotic manufacturing equipment, medical devices used in healthcare facilities, and communication protocols used by drones approved for use over large groups of people. It also includes active research into consumer devices such as kitchen appliances, smart TVs, smart homes, and more, all of which are increasingly connected to the internet.

### Trend Micro Research



## CHAPTER 5

# Wanted: Security Researchers

The world's largest vendor-agnostic bug bounty program, Trend Micro Zero Day Initiative (ZDI), was founded in 2005 to encourage the coordinated disclosure of zero-day vulnerabilities to affected vendors by financially rewarding researchers through incentive programs. It pioneered the vulnerability market with a focus on disrupting the underground market by legitimately purchasing vulnerability research that can then be disclosed to affected vendors. Vulnerabilities are taken off the market, away from possible abusers, enabling affected vendors to address them before the information is made public.

In addition to operating systems, devices, and applications, the ZDI also covers industrial control systems (ICS). ICS encompasses several types of control systems and technologies, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), human-machine interfaces (HMIs), and other control system configurations such as skid-mounted programmable logic controllers (PLCs) often found in industrial sectors as well as critical infrastructure. Like all forms of technology, ICS has its share of security vulnerabilities and can be a highly valuable target for cybercriminals.

## ZDI-sponsored hacking contests



### Pwn2Own Miami

In January 2020, Pwn2Own Miami debuted with a focus on vulnerabilities in industrial control systems, and Pwn2Own 2020 in March was held fully virtual, reflecting the current global reality for travel while continuing the important work of discovering multiple new issues.



### Pwn2Own Vancouver

ZDI has sponsored the Pwn2Own computer hacking contest since 2007. Contestants are challenged to exploit widely used software and systems using previously unknown vulnerabilities. The Pwn2Own contest demonstrates the vulnerability of devices and software in widespread use while also providing a checkpoint on the progress made in security since the previous year.



### Pwn2Own Tokyo

Created to address the growing attack surface on mobile devices and the IoT, Pwn2Own Tokyo shows that vulnerabilities exist and can be exploited on mobile and IoT devices to achieve compromises similar to those seen on more traditional platforms. Pwn2Own Tokyo seeks to harden these devices by identifying bugs and getting them fixed before they are actively exploited.

# DID YOU KNOW ?

## Facts about the Trend Micro Zero Day Initiative:

10,000+

researchers from more than 80 countries across six continents participate

9,000+

vulnerabilities have been published since inception

More than **US\$25 million** has been awarded since inception

It's a **top provider** of vulnerabilities to ICS-CERT, Adobe and Microsoft

## CHAPTER 6

# Protection before and after vulnerabilities are disclosed

Vulnerability research is critical to successfully defending against exploits by giving security companies the information they need to build protections into their products and services—especially ahead of patches being available or for systems that are not readily and immediately patchable.

While Trend Micro’s research and commitment to discovering and disclosing vulnerabilities helps make everyone more secure, customers using Trend Micro products experience the greatest benefit. That’s because with its exclusive access to vulnerability information from both its internal research, as well as the ZDI, Trend Micro can deliver both pre-emptive and post-disclosure coverage to customers of its security solutions.



### What is pre-emptive coverage?

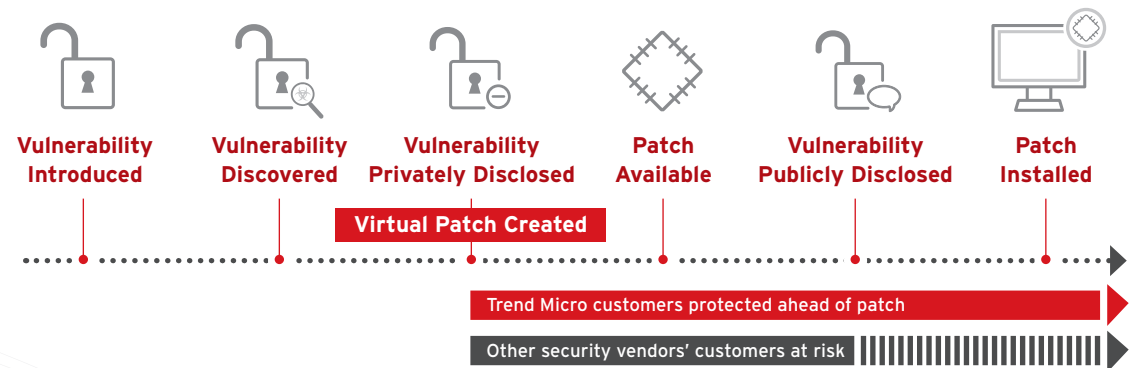
Using various means, such as virtual patching, filters, and policies, pre-emptive coverage provides protection against exploits of newly discovered vulnerabilities before a patch is available from the vendor.

### What is a virtual patch?

A virtual patch is a security policy, filter, or rule that prevents an exploit against a vulnerability from being used before a publicly disclosed patch is made available by the affected vendor. Virtual patches can also protect out-of-support software for which no patches will be created.

### What is post-disclosure coverage?

Virtual patches can also be used to protect organizations after a vulnerability is disclosed and a patch has been created, but before the patch has been applied.



Variants of an exploited vulnerability may not be protected by traditional exploit signatures from other vendors and may leave their customers susceptible to future attack.

# Protecting your organization

## Network protection

**Trend Micro™ TippingPoint™** provides network-based intrusion prevention against the full range of threats at wire speed anywhere on your network to protect your critical data and reputation. TippingPoint solutions deliver preemptive protection for vulnerabilities through a virtual patch before the publicly disclosed patch is made available by the affected vendor.

## Server protection

**Trend Micro Cloud One™ - Workload Security** provides comprehensive detection and protection in a single solution that is purpose-built for server, cloud, and container environments. Workload Security allows for consistent security, regardless of the workload. It also provides a rich set of application programming interfaces (APIs), so security can be automated and won't impact your teams.

## Endpoint protection

**Trend Micro Apex One™** provides earlier, stronger endpoint protection by supplementing desktop anti-malware and threat security with proactive virtual patching. Trend Micro™ Worry-Free™ Standard also provides virtual patching alongside anti-malware security, web reputation, and integrity monitoring. A high-performance engine monitors traffic for new specific vulnerabilities using host-based intrusion prevention system (IPS) filters as well as zero-day attack monitoring.

## Advanced threat protection

**Trend Micro™ Deep Discovery™** is an advanced threat detection platform that blends specialized detection engines, custom sandboxing, and global threat intelligence from the Trend Micro™ Smart Protection Network™ for the highest detection rate possible against attacks that are invisible to standard security products. TippingPoint integrates with Deep Discovery to detect and block targeted attacks through pre-emptive threat prevention, threat insight and prioritization, and real-time enforcement and remediation.

## Timeline for CVE-2018-8373

Using heuristics and in-depth analysis, ZDI discovered a high-risk Internet Explorer vulnerability in the wild. In less than one week's time, Trend Micro delivered pre-emptive protection from the new vulnerability for its customers. Trend Micro customers were protected nearly an entire month (29 days) ahead of the public disclosure by Microsoft and the availability of a Microsoft-provided patch.



Trend Micro Customers Protected 29 Days Prior to Public Disclosure by Microsoft

DID YOU  
KNOW ?

## CHAPTER 7

# Greater security for everyone

By combining Trend Micro's industry-leading vulnerability research with its award-winning technology for host, network, and endpoint security, we're helping protect hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. We do that by:

- Identifying unknown vulnerabilities and discouraging their sale on the underground market for nefarious purposes.
- Helping vendors of operating systems and applications used by enterprises and organizations to create patches against vulnerabilities ahead of public disclosure.
- Delivering pre-emptive protection to Trend Micro customers ahead of a vendor patch through exclusive access to vulnerability information submitted to the ZDI, as well as added protection for legacy, out-of-support software.
- Committing to long-standing relationships with leading software vendors and the research community to influence the importance of security in the product development life cycle.
- Using insights from newly discovered vulnerabilities to build new heuristics into Trend Micro products to stay ahead of cybercriminals, detect new zero-day exploits, and give customers the best possible protection.

## DID YOU KNOW ?

Trend Micro customers received:

**1,604**

zero-day filters delivered in 2021

**65**

days average of zero-day prediscovered filter coverage for 2021 Microsoft Bulletins

**21**

days average of zero-day prediscovered filter coverage for 2021 Adobe Bulletins

**102**

days average of zero-day prediscovered filter coverage for 2021

# Next steps

Through its vulnerability research, Trend Micro helps protect everyone on the internet from potential attacks. We do this by committing significant resources to the hard work of discovering vulnerabilities before the bad guys.

Our findings are put to work in two very important ways. First, responsibly disclosing new vulnerabilities to the vendors of the affected software and systems allows them to proactively provide corresponding patches in a timely manner. Then, for our customers, Trend Micro extends protection to cover the gap between vulnerability discovery and patch availability, as well as out-of-support and unpatchable systems.

Trend Micro is the only vendor that offers the breadth and depth of vulnerability research integrated into its products and solutions to deliver maximum protection through:

- The world's largest vendor-agnostic bug bounty program
- Comprehensive coverage across operating systems, devices, and applications, as well as the IoT and IIoT including ICS/SCADA
- Pre-emptive protection such as virtual patching, filters, and policies
- Extensive research capabilities including vulnerability analysis, malware and exploit analysis, security product development, and custom research
- A range of products that protect customer networks, servers, and endpoints

Find out more about how Trend Micro can help your company do business safely with solutions for [intrusion prevention](#).

## About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our unified cybersecurity platform protects over 500,000 organizations and millions of individuals across clouds, networks, devices, and endpoints.

The Trend Micro One unified cybersecurity platform delivers advanced threat defense techniques, extended detection and response (XDR), and integration across the IT ecosystem, including AWS, Microsoft, and Google, enabling organizations to better understand, communicate, and mitigate cyber risk.

With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world.

[TrendMicro.com](https://www.trendmicro.com)