

# //PRODUCT PORTFOLIO

Complete Cybersecurity

data





# //WHO WE ARE

## Your Partner for all your Cybersecurity needs

Data Ally is a leading Cybersecurity Solutions distributor committed to safeguarding our resellers' customers from the ever-evolving threat landscape of the digital world. With a team of dedicated experts and state-of-the-art products, we provide comprehensive solutions that enable our partners to operate securely and confidently in today's digital age.

Our portfolio can help you to maintain and modernize your IT solutions services.

### // Our Mission

Our mission is to offer the best cybersecurity solutions, protecting our clients' digital assets, data, and reputation. We strive to build a safer digital world by delivering innovative, reliable, and adaptable cybersecurity solutions that address the most complex threats and challenges.

### // Industries Served

We serve a diverse range of industries, including finance, healthcare, government, manufacturing, technology, and more. Our cybersecurity solutions are adaptable to the unique requirements of each sector.



# A complete Cybersecurity Ecosystem



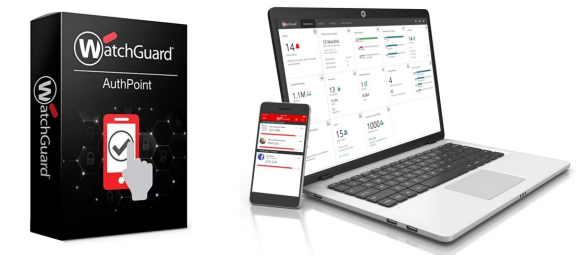
// WatchGuard Range of Hardware Devices

For 25 years, WatchGuard has pioneered cutting-edge cybersecurity technology and delivered it as easy-to-deploy and easy-to-manage solutions. With industry-leading network and endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence products and services, WatchGuard enables small and midsize enterprises from around the globe to protect their most important assets including over 10 million endpoints. In a world where the cybersecurity landscape is constantly evolving, and new threats emerge each day, WatchGuard makes enterprise-grade cybersecurity technology accessible for every company. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

## Network Security

WatchGuard offers a wide variety of network security solutions, including tabletops and 1U rack-mounted appliances, to Cloud and virtual firewalls. The Firebox supports a host of critical security services, from standard IPS, URL filtering, Gateway AV, application control, and antispam,

to services for combating advanced threats such as file sandboxing, DNS filtering, and more. High performance deep packet inspection (DPI) means the entire stack of WatchGuard services can be brought to bear on attacks attempting to hide in encrypted channels, like HTTPS. What's more, every Firebox offers SD-WAN right out of the box for improved network resiliency and performance.



## Multi-Factor Authentication

WatchGuard's AuthPoint® service is the right solution at the right time to provide effective authentication on an easy-to-use Cloud platform. MFA provides the strongest approach to user identification – requiring them to supply information they know, with information provided on something they have, to positively identify a specific person. With a simple push notification, the AuthPoint mobile app makes each login attempt visible, allowing the user to accept or block access right from their smartphone.



# Unleash the security of ONE



## Endpoint Security

WatchGuard Endpoint Security includes a wide range of extensible solutions to stop breaches, data theft, and cyberattacks. Our Cloud-based platform integrates the technology, intelligence, and expertise to deliver advanced prevention, detection, containment, and response capabilities via a lightweight agent. Get protection across the entire threat lifecycle by adding products like DNSWatchGO for endpoint DNS-level protection.

## Secure Wi-Fi

WatchGuard's secure, Cloud-managed Wi-Fi solutions are engineered to provide safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, Wi-Fi in WatchGuard Cloud delivers the competitive advantage businesses need to succeed.

## Enable Zero trust Security

With WatchGuard's Identity Framework layer, our Unified Security Platform architecture enables user authentication as a key factor in every security analysis. It simplifies zero trust adoption with a risk framework and authentication policy management, allowing for more granularity when creating rules and resources. As part of our Unified Security Platform approach, zero trust policies encompass device, application, and identity verification and

## It's time for a New Vision

enforcement, so you can apply micro-segmentation to limit the opportunity for insider threats, network infiltration, and lateral movement across your network.

**Boost Security Efficacy and Efficiency** with XDR WatchGuard ThreatSync® is the Cloud-based XDR layer within our Unified Security Platform architecture. It detects, correlates, and prioritizes threat intelligence from the platform for automated or manual remediation. Shared telemetry delivered via the Cloud gives our endpoint security solutions visibility into attacks against the network and firewalls along with awareness of attacks against endpoints. ThreatSync automatically consumes and correlates threat indicators originating across environments, users, devices, and applications to issue a definitive threat score.



# Everything MSSPs Need

## FLEXPAY

The dynamic MSSP Program for WatchGuard Partner Success.

WatchGuard's managed service providers (MSSPs) are equipped with a flexible program, a powerful and diverse product portfolio, and an ecosystem of technology integrations that enable you to leap ahead of the pack in an increasingly competitive and growing marketplace.

FlexPay Points are prepaid and can be used for any and all WatchGuard hardware and software at any time, and do not expire. They essentially work like WatchGuard currency. FlexPay Points are also a great way to remain flexible.




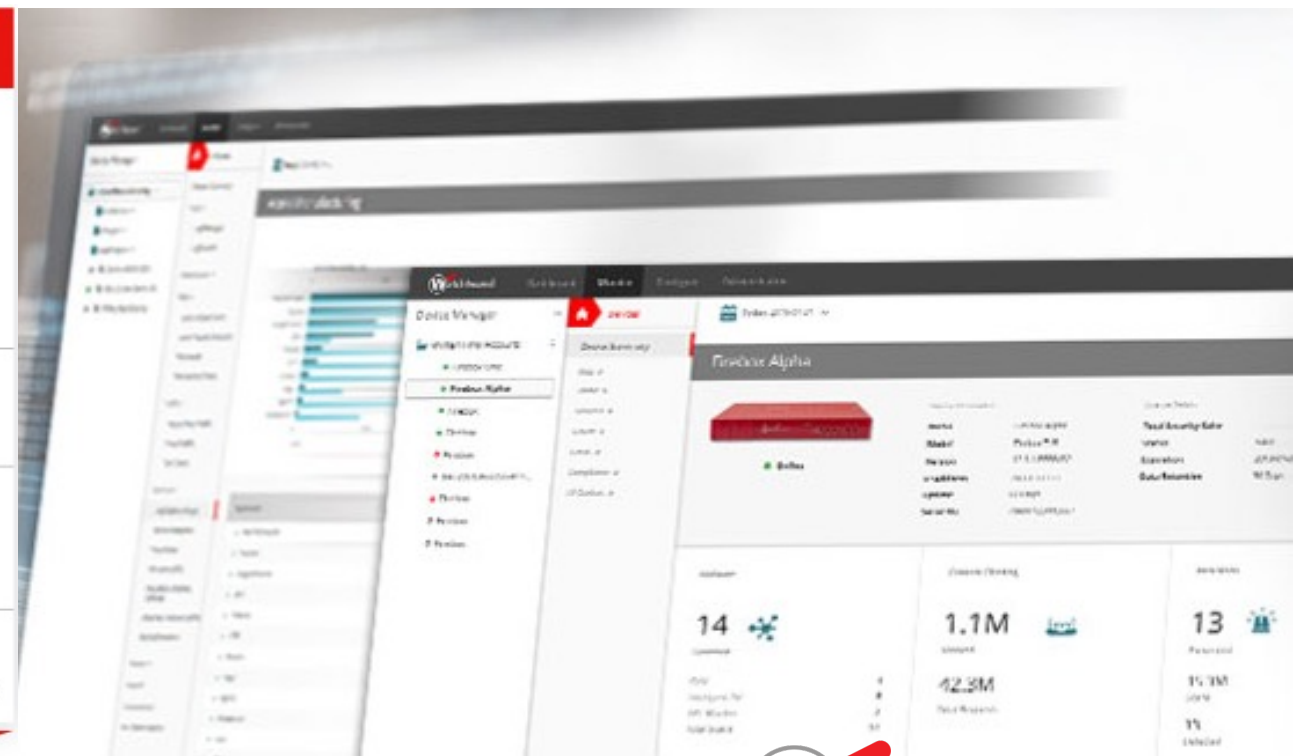
## MSSP Prepaid Points

WatchGuard ONE Managed Security Services Providers (MSSPs) can enrol in a flexible pricing prepaid points program called MSSP Prepaid Points. Partners can manage and allocate these prepaid points to tenants for most WatchGuard products.

Products that you manage in WatchGuard Cloud and purchase with points show as a subscription. At the start of each calendar month, WatchGuard automatically deducts points from the Total Points Available based on the service type and monthly point allocation for each managed device and service.

For example, if you don't necessarily have the commitment from an end customer for a term agreement, or if your business's cash flow varies throughout the year, you may want to consider FlexPay Points. This allows you to keep your business running steadily, despite the ups and downs of the market. Points can be purchased in "blocks" at your authorized WatchGuard Distributor. Once purchased, you can activate those points via MSSP Command in the WatchGuard Partner Portal.

FlexPay Points

Expense Type <b>CAPEX &amp; OPEX</b>
Supported Product Lines <b>All</b>
Contract? <b>No</b>
Purchase type <b>Purchase at will with a Points balance</b>





# Extend your Team with WatchGuard Experts



## MDR for MSPs, Without the Overhead

The WatchGuard SOC, operated by seasoned cybersecurity experts armed with security analytics, industry-leading machine learning/AI, and threat intelligence, keeps MSP customers safe. The team constantly monitors, hunts, detects, and contains threats lurking in their endpoints around the clock while assessing their attack surface to strengthen security posture and improve their resiliency to threats.

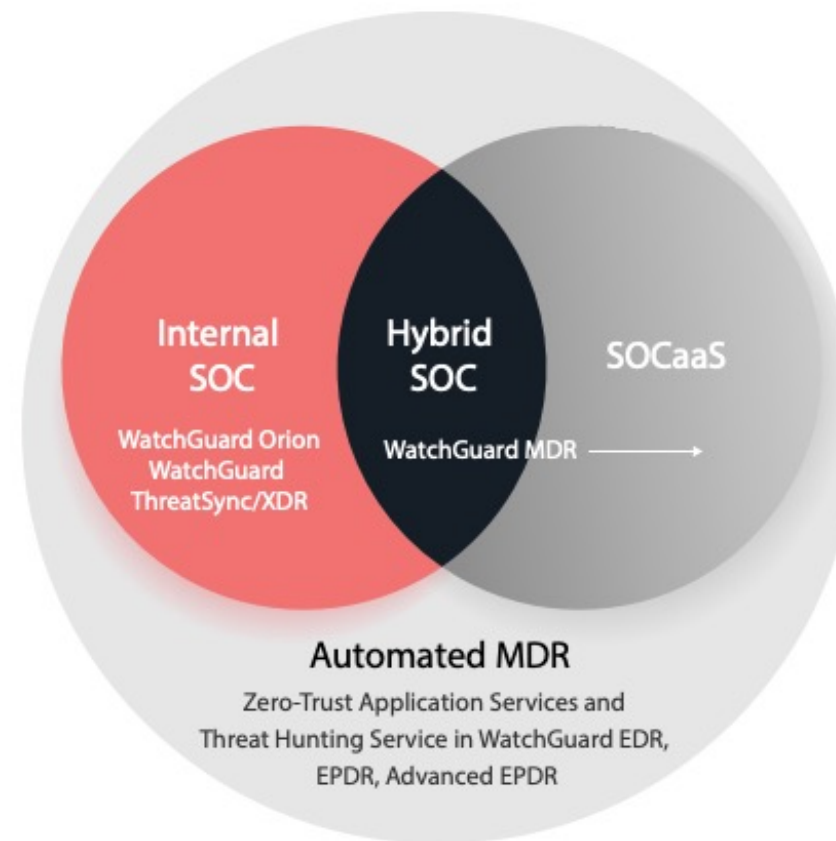
## Adopt MDR Without Huge Investments

We partner with you as the frontline of customer cyber defences. The service lets you concentrate on your core

business while we maximize your customers' proactive cybersecurity posture and take over the worry of threat actors slipping into your customers' environments.

## Extend Your Team with WG Experts

Our highly skilled security analysts and threat hunters are an extension of your team, always ready to stop attackers while keeping you in the loop. The team of experts knows how threat actors compromise organizations, keeps updated on attack techniques, and develops new analytics to detect them promptly.

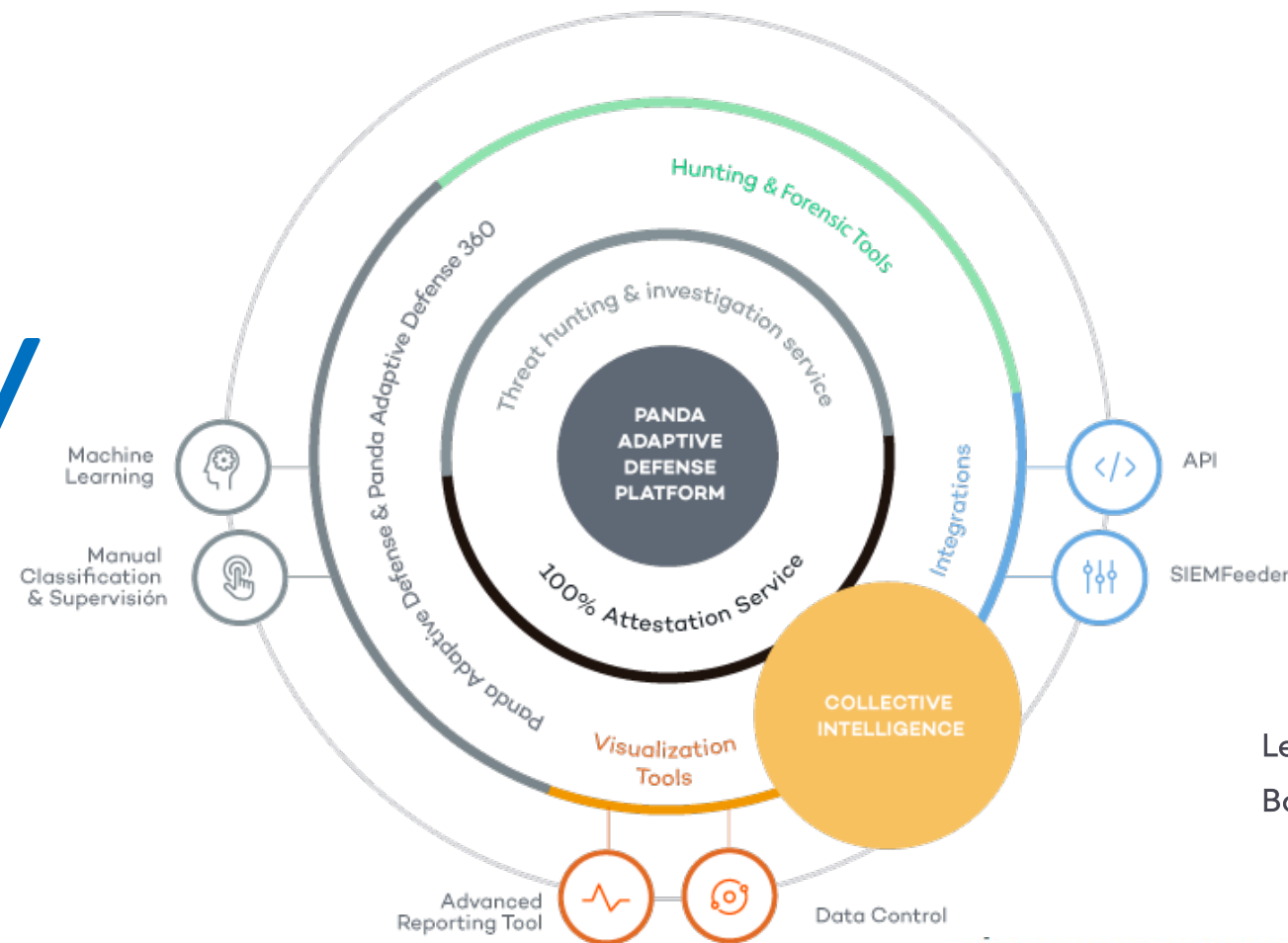


As the cyber threat landscape continues to expand and grow in sophistication, companies struggle with serious security risks, inefficient cybersecurity posture management, and a scarcity of skilled personnel. So, companies are looking to outsource their protection to managed service providers (MSPs) with the technology, staff, and expertise to address these challenges.

However, managing complex security challenges and the expanding threat surface most companies face today requires skilled people and a lot of investment, making it difficult for MSPs to offer managed detection and response (MDR) services in an effective, economical manner. That's why WatchGuard introduced WatchGuard MDR; a managed service that helps security service providers overcome these problems. By leveraging our thorough detection and response service in their offering, MSPs can meet customers' needs without the overhead of building and maintaining their own 24/7, in-house security operations centre (SOC).



# 30+ Years of Cybersecurity Innovation



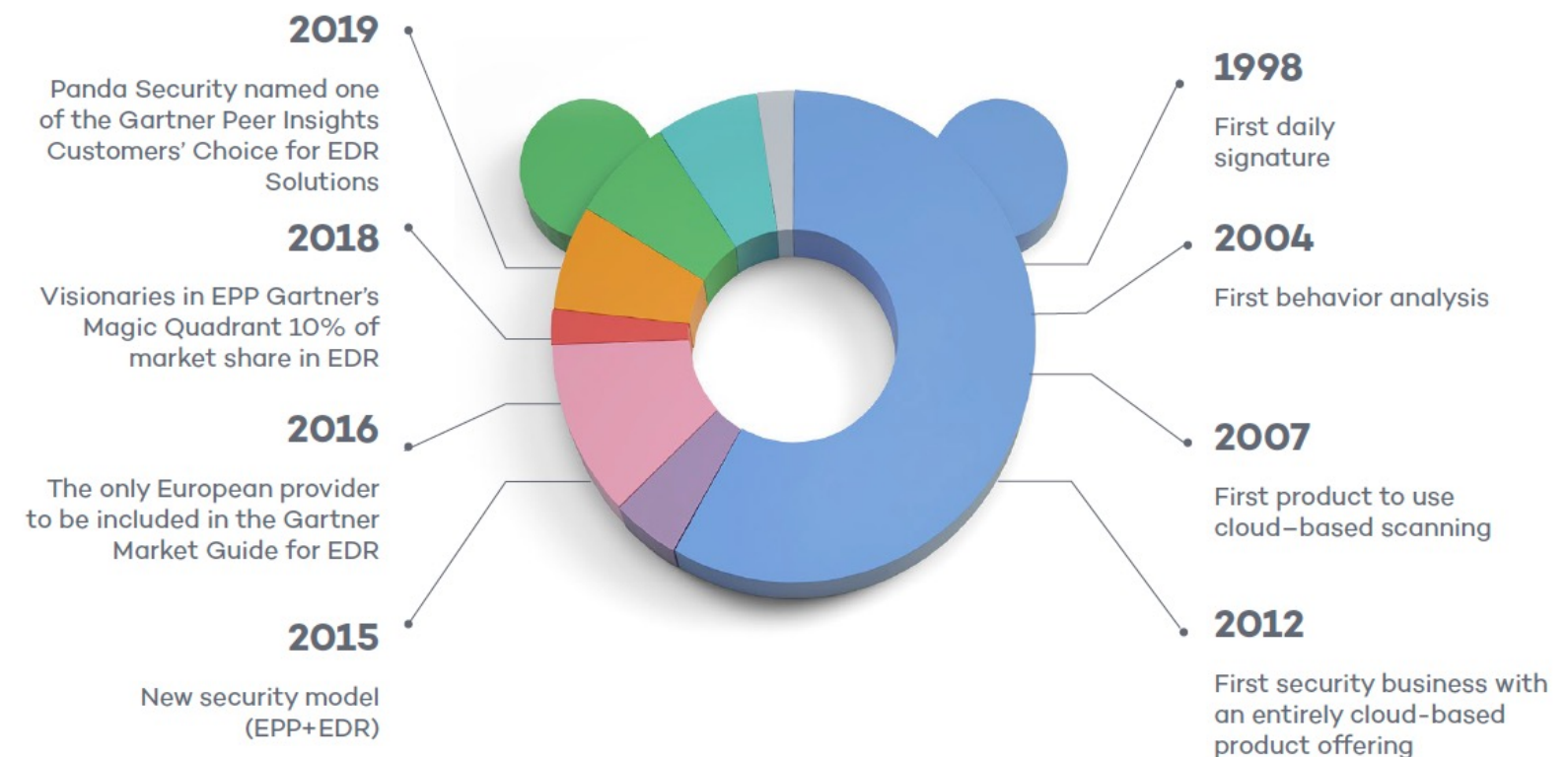
Panda Security is the leading European vendor of EDR systems, with experience developing advanced cybersecurity services to prevent cybercrime and to eradicate advanced threats in all size organizations. Its mission is to develop and provide security solutions to keep their clients' IT resources running optimally and safe from the damage inflicted by viruses, intruders and other Internet threats.

Left picture // The Endpoint Ecosystem

Bottom picture // Panda Milestones

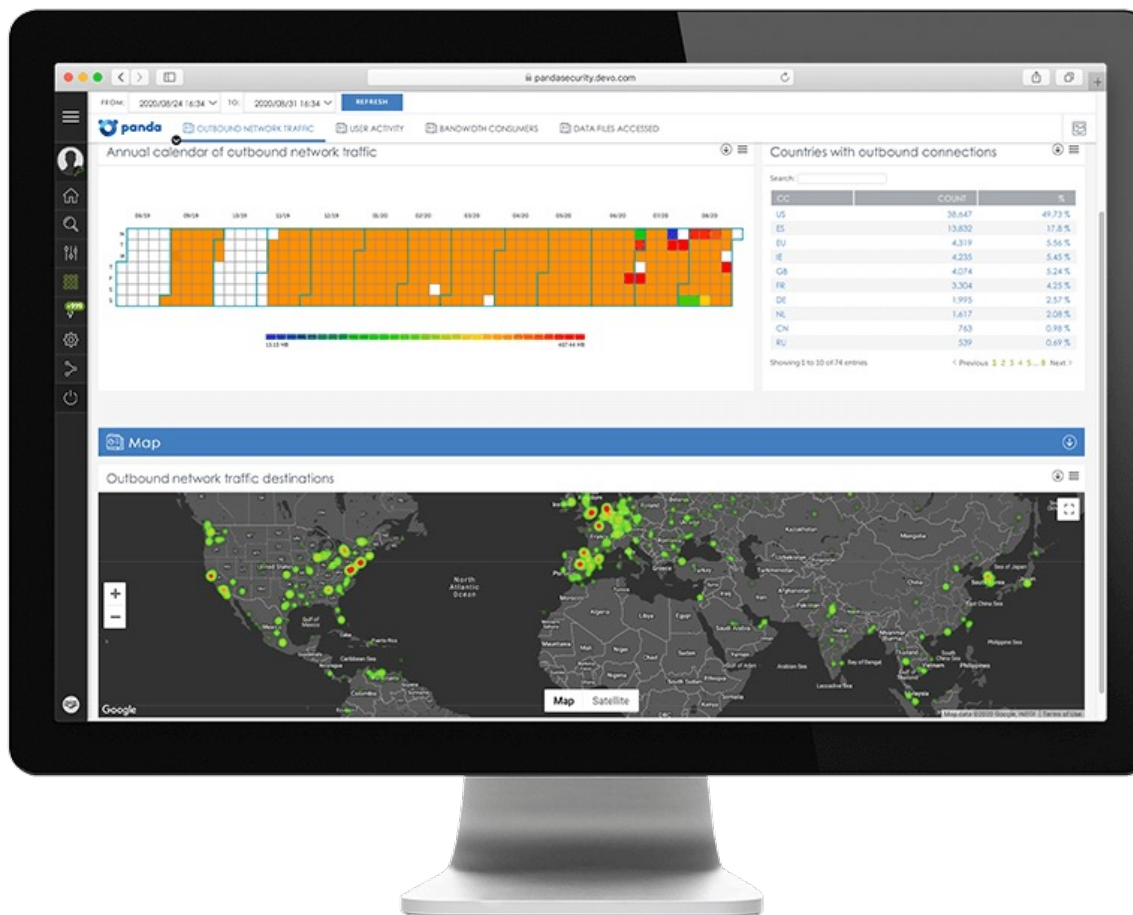
Panda Security is a leading provider of cloud-based security solutions with products available in more than 23 languages and millions of users located around the world. Panda Security was the first IT security company to harness the power of cloud computing with its Collective Intelligence technology. This innovative and proprietary security model can automatically analyse and classify thousands of new malware samples per day, guaranteeing corporate customers and home users the most effective protection against

internet threats with minimum impact on PC performance. With sales in more than 200 countries, Panda has 56 offices across the globe with headquarters in Spain (Madrid and Bilbao).





# Prepare, Prevent and Control for a Safe Environment



## Panda Adaptive Defense 360

Advanced Security to Stop Breaches  
Unified Endpoint Protection (EPP) and  
Endpoint Detection and Response (EDR)  
capabilities, with our unique Zero-Trust  
Application Service and Threat Hunting  
Service in one single solution, to  
effectively detect and classify 100% of  
processes running on all the endpoints  
within your organization. Cloud-  
delivered endpoint prevention,  
detection, containment and response  
technologies against advanced threat,  
zero-day malware, ransomware,  
phishing, in-memory exploits and

malware-less attacks. It also provides  
IDS, firewall, device control, email  
protection, URL & content filtering  
capabilities.

## Panda Fusion

Fusion combines our Systems  
Management and Endpoint Protection  
Plus solutions to protect, manage and  
support all of your corporate devices.  
Our Cloud-delivered solution allows a  
rapid deployment without needing  
maintenance or costly investments in  
server infrastructure.

## Panda Adaptive Defense

Intelligent Endpoint Detection and  
Response Intelligent EDR that  
automates the detection, classification  
and response to all the endpoint  
activity. Automatically detects  
suspicious behaviours to block and  
respond to breaches, malware and  
advanced threats. Its technology is  
based on the Zero-Trust Application  
Service, which provides full and  
accurate visibility on endpoints,  
applications and users and denies any  
suspicious execution.

## Panda Fusion 360

Fusion 360 combines our Systems  
Management and Adaptive Defense  
360 solutions to unify RMM with EPP  
and EDR capabilities. This holistic  
solution combines the best of two  
worlds to provide advanced endpoint  
security, centralized IT management,  
monitoring and remote support  
capabilities. Fusion 360 ensures the  
classification of 100% of the running  
processes on all your endpoints with  
our Zero-Trust and Threat Hunting  
services.

## Panda Endpoint Protection/Plus

This effective, Cloud-native security  
solution centrally manages the security  
of endpoints, both inside and outside  
the corporate network. Our Endpoint  
Protection (EPP) technologies prevent  
infections by utilizing our Collective  
Intelligence. It also analyses endpoint  
behaviours to detect and block both  
known and unknown malware,  
ransomware, trojans and phishing  
attacks, and our threat intelligence and  
machine-learning algorithms provide  
faster detection.



## Panda Advanced Reporting Tool

From Data to Actionable IT and Security Insights Advanced Reporting Tool stores and correlates information from endpoints on processes executed and other contextual information. It is then presented in a way to draw informed conclusions about corporate IT and security intelligence. Detailed visibility of every event run on your endpoints is represented to facilitate easy security decisions and fast reactions.

## Panda Patch Management

Patch Management is an easy-to-use solution for managing vulnerabilities in operating systems and third-party applications on Windows workstations and servers. It covers all the patch management processes including discovering, identifying, assessing, reporting, managing, deploying installations and remediating security risks.

## Panda Full Encryption

Panda Full Encryption is the first line of defence to protect your data in a simple and effective way. It is a full-volume encryption solution that strengthens security against unauthorized access

# Complete your endpoint solution with a wide range of addon modules

using established authentication mechanisms. Data encryption minimizes data exposure and provides an additional layer of security and control to your organization.

## Panda SIEM Feeder

SIEM Feeder provides a new source of critical and valuable information into your current SIEM tool. It collects and correlates all the processes run on endpoints, allowing organizations to turn massive volumes of data into useful information for decision making, and thus enriching the organization with the knowledge provided by Adaptive Defense.

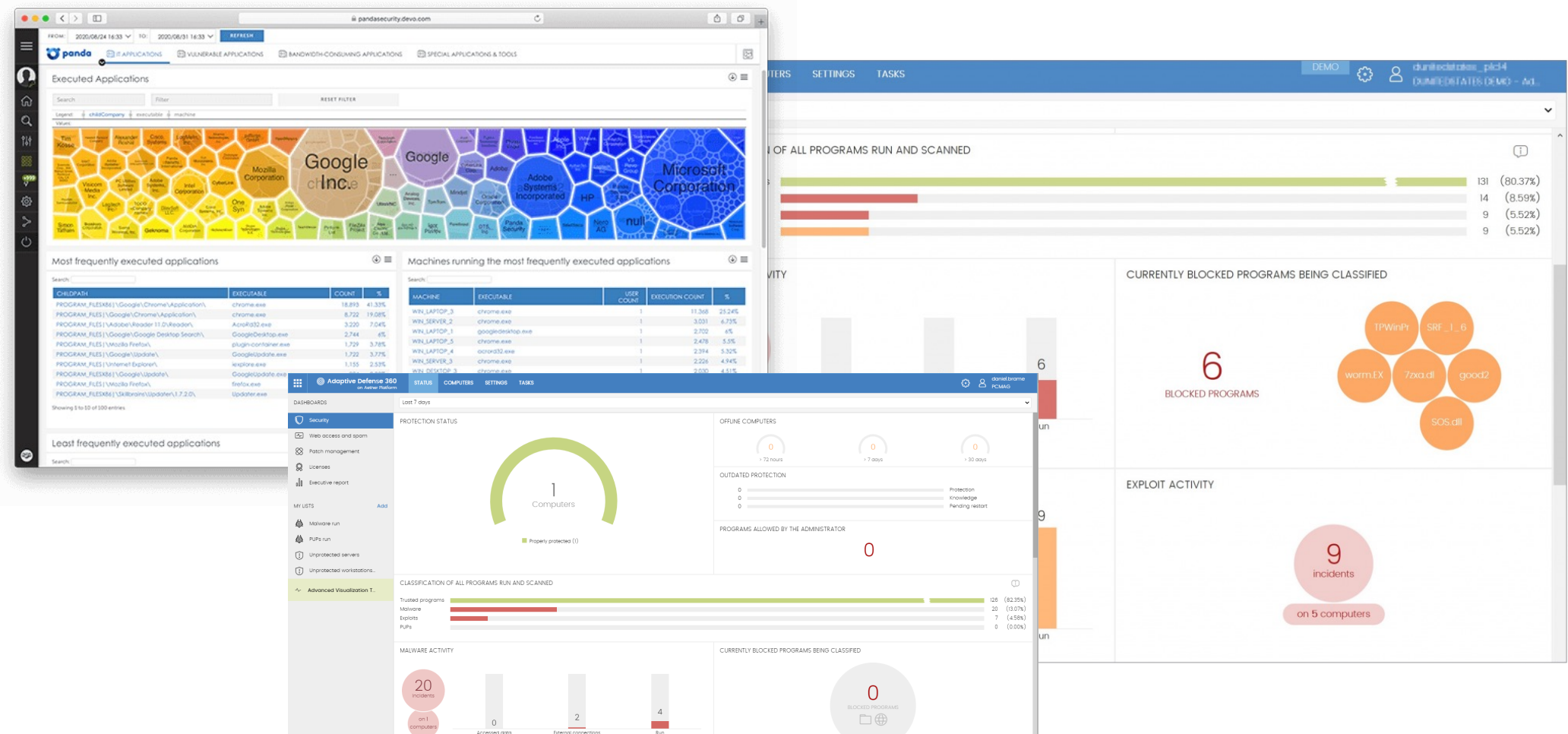
## Panda Email Protection

Block spam, malware, and phishing attacks. Email Protection is a Cloud-

based, multi-layer security solution designed to prevent unwanted emails that delivers immediate and effective protection and filtering technologies against phishing attacks, malware, and spam.

## Panda Systems Management (RMM)

Systems Management is the easy and affordable way to manage, monitor, maintain and support all your organization’s devices and IT systems, whether they are in the office or remote.







# The next Generation of Digital Protection

Cybersecurity tailored to your needs.

With Panda Security, a WatchGuard brand, you have the most advanced protection for your family and your business. Panda Dome offers maximum security against viruses, ransomware, and cyberespionage for Windows, Mac, Android and iOS.

**Panda Dome Advanced Essential +**  
Ransomware protection  
Parental Control

**Panda Dome Complete Advanced +**  
Clean-up: PC optimization  
Password Manager

**Panda Dome Premium Complete +**  
Update Manager  
Total Care: 24/7 technical support

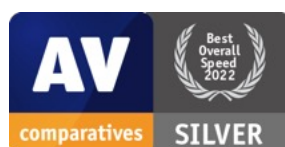
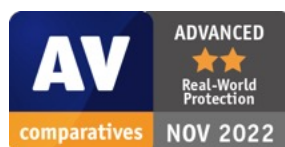
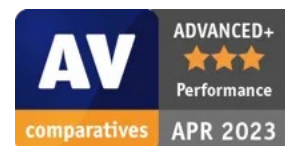
**Addons for Dome Products**  
Panda Clean-up  
Panda VPN  
Panda Family  
Panda Passwords

## Panda Dome

Our cybersecurity dome delivers the best protection moulded to your specific needs. Keep your computers, smartphones, tablets, and smartwatches safe.

## Panda Dome Essential

Antivirus with Firewall  
VPN with 150 MB/day limit  
Wi-Fi protection  
Secure online shopping





SecPoint stands at the forefront of security solutions, consistently outpacing competitors in its market. Our primary commitment is to deliver exceptional, innovative IT security solutions to businesses with unparalleled ease.

Furthermore, we've crafted the Penetrator vulnerability scanner to identify and address security vulnerabilities throughout networks. It not only scans for existing threats but also proactively alerts users about emerging vulnerabilities. Designed with accessibility in mind, its user-friendly interface caters to both technical experts and those with less technical proficiency.

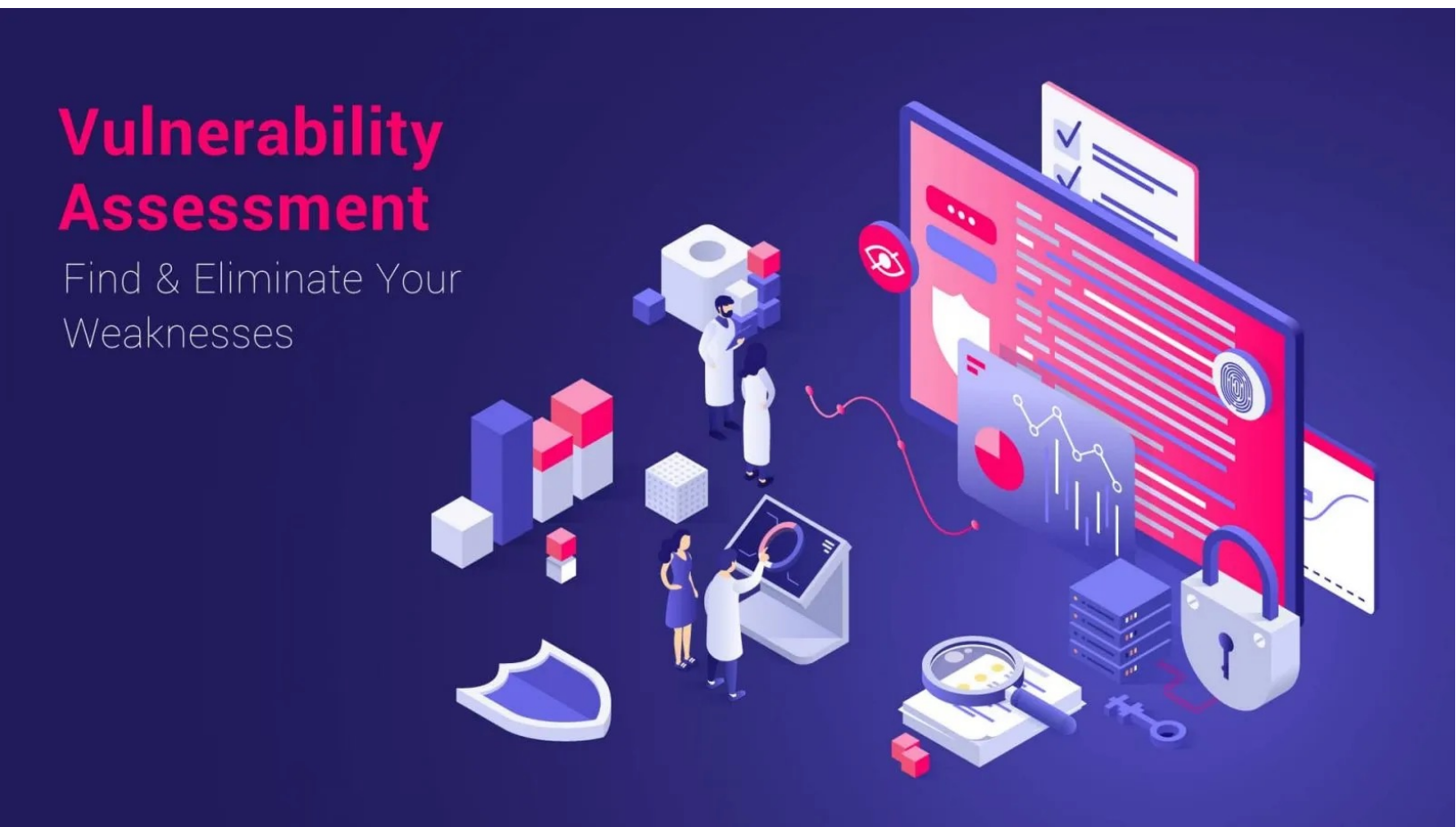
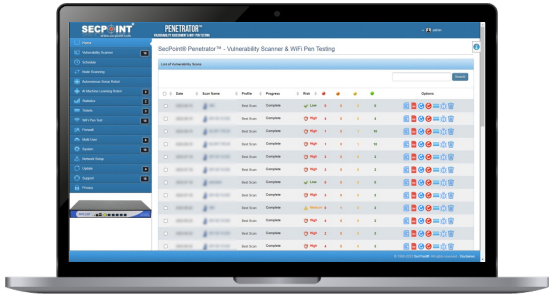
**SecPoint® Penetrator**

- Scan Local & Public IPs
- Virtual Software & 1U/SFF Appliance
- Lethal Attack Blind SQLi & RCE
- SQL Injection, XSS & Reflected
- Scans Websites, Web shops, Firewalls
- Data Leak Detection
- White labelling
- Logo Branding, Watermark, Name
- 19 Vulnerability Scan Profiles
- Over 122,000+ Vulnerability Checks I
- 1,400+ Web Shells Detection/ RCE

Vulnerability management is the key to any security strategy



- WiFi Penetration Testing
- Professional PDF & HTML Reporting
- Advanced AI with High Accuracy
- IoT & SCADA Vulnerability Scanning
- Automatic Scheduled Scanning
- Managed Service Provider (MSP)
- Reporting in 17 Languages



**Vulnerability Management**

The SecPoint® Penetrator stands as the pinnacle of vulnerability management and penetration testing platforms. Fully equipped and ready-to-use, this powerful security assessment solution is an essential asset for any network.

**Comprehensive Vulnerability Scanning**

Equipped with an expansive vulnerability database and advanced scanning techniques, the SecPoint® Penetrator ensures you always remain a step ahead of adept attackers. Users can select from 19 diverse vulnerability scanning profiles to best meet their needs. Though the IP License restricts only concurrent scanning, it's easily upgradable, marking the Penetrator as one of the most thorough vulnerability assessment solutions available today.

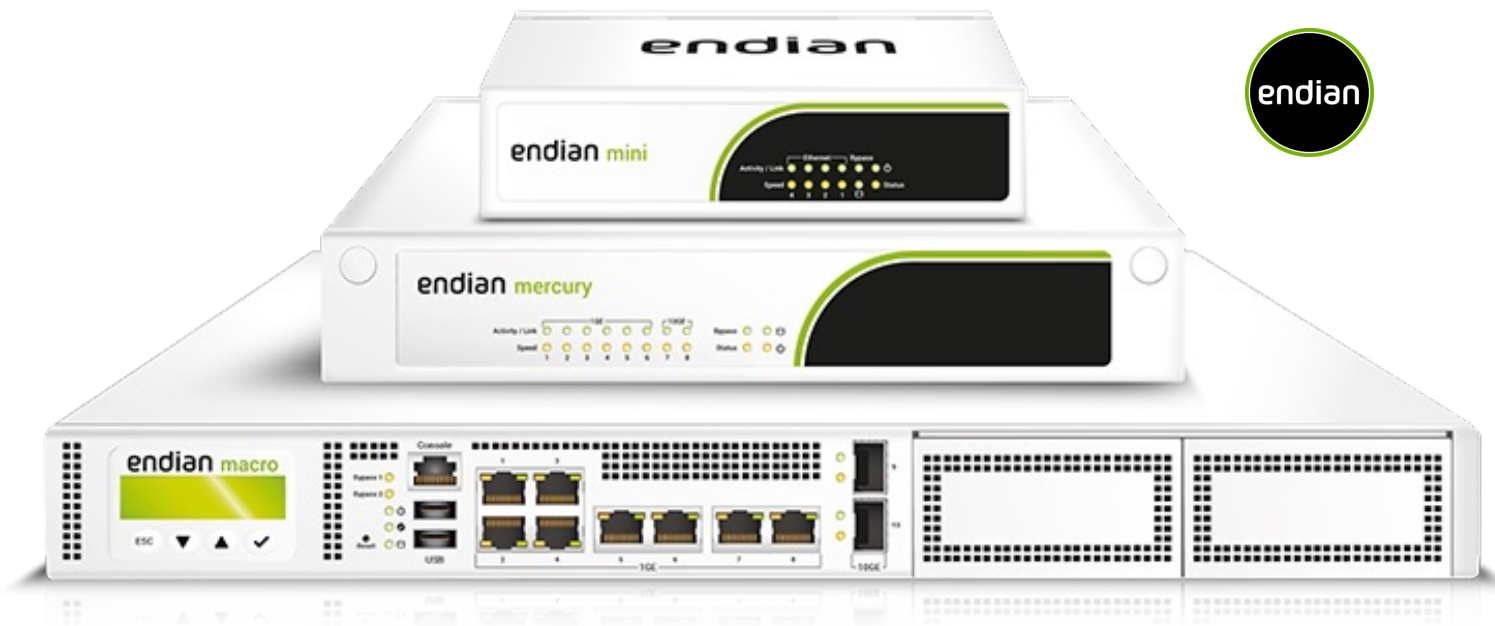
**Professional Skilled Support**

Unparalleled in the industry, we pride ourselves on our swift reply and response times to support queries. Our top-tier 24-hour support team is always at your service. Track your inquiries and stay updated with our Support Centre's ticket status feature.



# Secure everyThing

**Endian** is an emerging market leader in Industrial IoT security. We have a proven track record in delivering innovative security solutions and a strategic commitment to the needs of industrial customers. We provide integrated software and hardware solutions that maximize effective security. Endian Connect Platform for Industrial IoT helps customers protect their business with best-in-class security and minimal operating cost.



## Endian OS - Engine for a Secure Digital Transformation

### Endian UTM

A powerful solution for network security, providing organizations with the tools they need to protect their networks, enforce security policies, and optimize network performance.

### Zero Trust Architecture

In the new Zero Trust architecture, businesses trust less and verify everything so they can reduce their attack surface using fine-grained access, authorization and security policies. In addition, a Zero Trust environment ensures stronger and better compliance and audit efforts.

### Network Visibility and Monitoring

Before an organization can implement a Zero Trust model, they must identify and assess every single device on their network.

### Microsegmentation

As part of the Zero Trust architecture, creating smaller and more targeted network zones increases security while reducing risk exposure. By utilizing powerful security policies to enforce zone boundaries organizations can ensure only approved network communications.

### Edge Computing

The concept of edge computing simply means utilizing computing resources at the edge of the network (instead of the central network or datacentre). By leveraging Docker and container technology, organizations can leverage micro services and applications to replace or extend edge network capabilities.

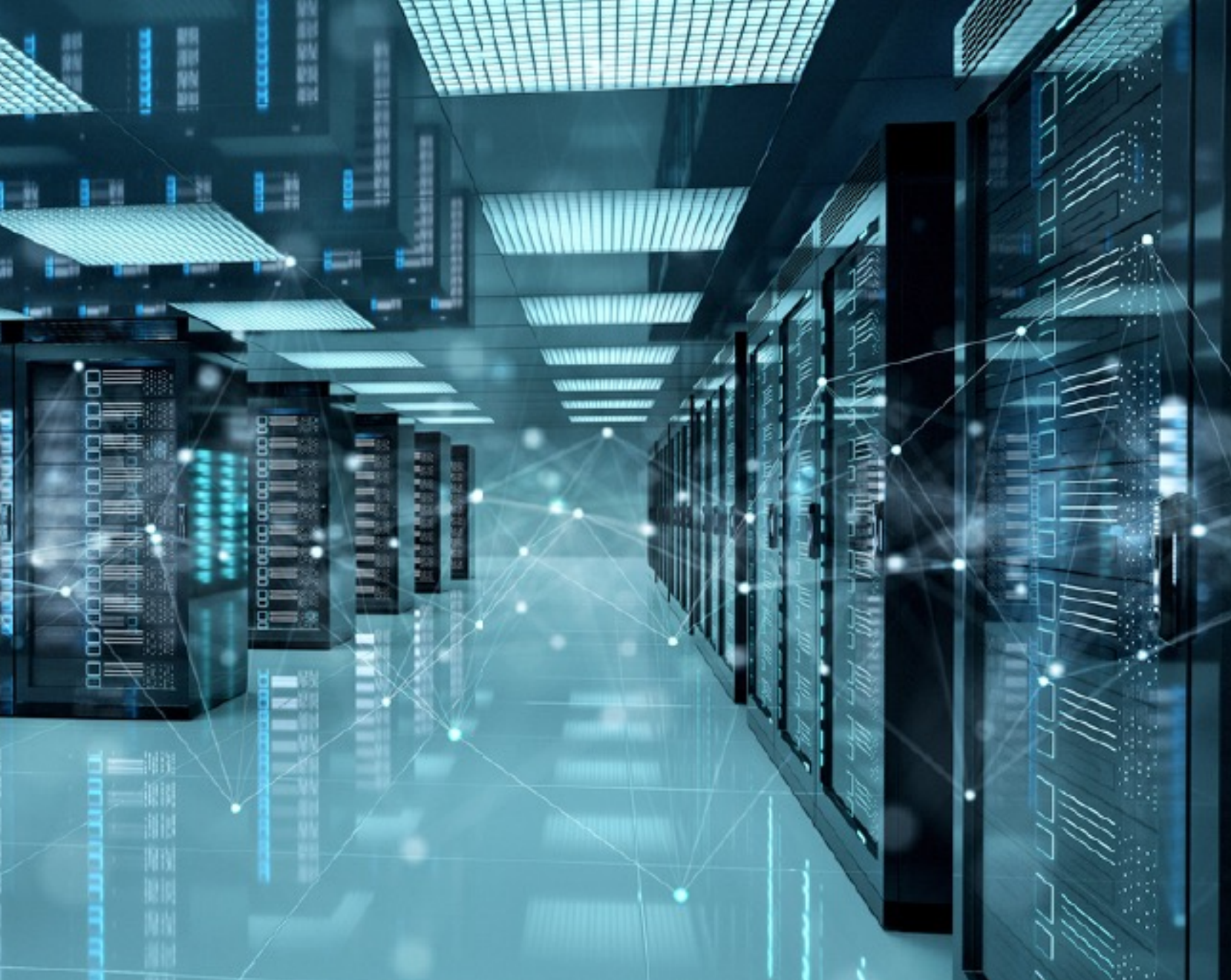
### Threat Management

For approved network communications, a business must go deeper to ensure they are safe and secure. The threat management toolset helps to detect and stop advanced threats and malware from infiltrating business networks. Using deep-packet intrusion detection and prevention to identify and enforce security policies.

### Secure Web and Mail Communication

To ensure businesses continuity and resilience, organizations must take steps to enforce strong network policies that maximize productivity while reducing disruption. This includes the protection of major internal communications channels like web browsing and email.





# Powerful Backup and Recovery for your Data – Wherever it Resides

## NAKIVO Backup & Replication

NAKIVO's range of supported platforms covers virtual, cloud, physical, SaaS and NAS. NAKIVO Backup & Replication, delivers reliable backup, replication, disaster recovery and infrastructure monitoring all from a single web-based interface.

**Virtual:** Backup, replication and Site Recovery for VMware vSphere, Microsoft Hyper-V and Nutanix AHV environments

**Cloud:** Backup, replication and Site Recovery for Amazon EC2

**Physical:** Backup, instant granular recovery and instant P2V recovery for Windows and Linux physical servers and workstations

**Network shares:** Backup and recovery for files and folders stored on NAS devices and Windows/Linux network shares over CIFS/NFS

**SaaS:** Backup for Microsoft 365 data in Microsoft Teams, Exchange Online, OneDrive for Business and SharePoint Online

**DB:** Backup for Oracle Database via RMAN

**IT Monitoring:** VM performance and health tracking functionality to help you proactively address issues and prevent bottlenecks.

## Why Choose NAKIVO

Customers choose NAKIVO Backup & Replication for the advanced feature set, superior performance and highly-rated technical support team.

Trusted by organizations with strict cybersecurity standards

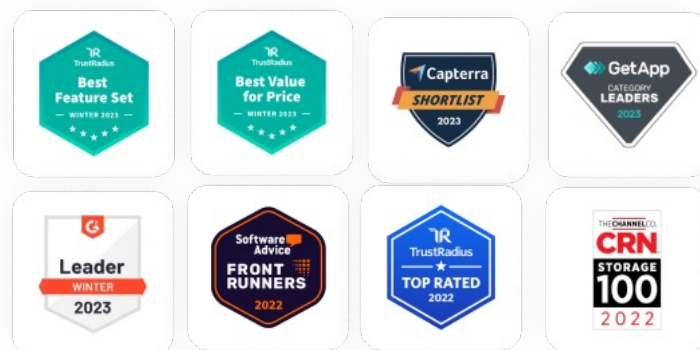
One platform for all data protection needs

Fraction of the cost of competitors

Founded in 2012, **NAKIVO** delivers an affordable and reliable backup and recovery solution that meets the data protection needs and requirements of SMBs and enterprises in every industry.

Over the years, customers and partners have trusted us with their data, and this has translated into double-digit growth, quarter over quarter. We continue to deliver on that trust with frequent releases, new solutions and

expanded functionality to meet emerging data protection challenges and threats.





# Zero-Trust file protection

## Glasswall is keeping organizations safe

With offices in both the US and UK, Glasswall keeps governments and commercial organizations around the world secure from advanced threats such as malware, phishing, and zero-day attacks.

## File security for today and tomorrow

Unlike detection-based solutions, our zero-trust CDR (Content Disarm and Reconstruction) technologies ensure that organizations are protected against both known and zero-day (new) threats. Our clients can rely on Glasswall to provide the highest level of protection, both for now and in the years to come. Glasswall has already started to develop tomorrow's protection solutions – we have a number of patents that will allow us to evolve our industry-leading protection capabilities, keeping us one step ahead.

## Zero-trust file protection with Glasswall CDR

A sharp increase in the number of individuals working remotely has supercharged the scale of digital information sharing. This presents an opportunity for cyber criminals to manipulate file vulnerabilities and embed malware with devastating effect.

There are a number of solutions designed to keep organizations safe against file-based threats – however, most share one common issue – a reliance on detection.

## What is zero-trust file protection?

Glasswall's zero-trust file protection is different. Instead of looking for malicious content, our advanced CDR (Content Disarm and Reconstruction) process treats all files as untrusted, validating, rebuilding and cleaning each one against their manufacturer's 'known-good' specification.

Only safe, clean, and fully functioning files enter and leave an organization, allowing users to access them with full confidence.

## Existing Security Solutions fall short

### Take a zero-trust approach to files

With Glasswall CDR, only safe, clean and fully functioning files enter and leave an organization, allowing users to access them with full confidence.

## No more security trade off – just safe, usable files at speed

Security teams need no longer choose between complete file security or speed and usability. Unlike other CDR vendors who flatten files, Glasswall CDR provides rapid zero-trust file protection that maintains original document usability. There is no dependence on antivirus databases to provide knowledge of a new threat, and security teams no longer deal with disruptions from quarantining files or false positives.





# Innovation Beyond Networks



Since founded in 2003, **Ruijie** has been building in-depth scenario-oriented application experience through solution design and innovation in the industry, thus assisting the upgrade into the digitalization of all industries. Ruijie dedicates in the R&D, design, and sale of network devices, network security products, and cloud desktop solutions.

**Reyee** is a brand from enterprise manufacturer Ruijie. Reyee products are designed for small to medium business (SMB) and small office home office (SOHO) markets which are cost-effective without compromising on features. Products include wireless routers, access points and network switches with PoE options. All managed devices are compatible with Ruijie Cloud which allows users to configure and maintain Reyee network devices via the cloud for free.

**Ruijie Networks** excels in delivering cutting-edge network solutions tailored for the electronics, automotive, pharmaceuticals, and steel manufacturing industries. Our comprehensive network services cater to diverse applications including mobile office, safety production, intelligent warehousing, and logistics. We are committed to empowering the digital revolution toward intelligent manufacturing.

Ruijie Networks achieves a compound annual growth rate of over 60% in the manufacturing industry market. We proudly serve tens of thousands of enterprise customers, including over 300 top-500 Chinese enterprises.

## Intelligent Manufacturing

The industrial Internet enables enterprises to automate and streamline their production processes, improving efficiency and product quality. Intelligent manufacturing will become the mainstream mode of future industrial production, offering enterprises a significant competitive edge.



**Zimperium, Inc.** is a global leader in mobile device and app security, offering real-time, on-device protection against both known and unknown threats on Android, iOS and Chromebook endpoints. The company was founded under the premise that the then current state of mobile security was insufficient to solve the growing mobile security problem. At the time, most mobile security was a port from traditional endpoint security technologies.

Zimperium recognized mobile devices had unique characteristics needing a completely new approach. The team set to work to reimagine how to protect mobile devices and developed the award winning, patented z9 machine learning-based engine. z9 protects mobile devices from device, network, phishing and application attacks. And as first envisioned, z9 has detected 100% of zero-day mobile exploits in the wild without requiring an update or suffering from the delays and limitations of cloud-based detection—something no other mobile security provider can claim.



## Your data is mobile. Is your security?

**Zimperium Mobile Threat Defense (MTD)** – formerly known as zIPS – is a privacy-first application that provides comprehensive mobile security for enterprises. It is designed to protect corporate-owned and/or BYO (bring-your-own) devices from advanced persistent threats across four categories: device, network, phishing, and app attacks.

As the mobile attack surface continues to expand and evolve, so does Zimperium's machine learning-based engine. Zimperium MTD detects known and unknown threats by analyzing the behavior of a mobile device and can accurately identify mobile system deviations, applications that behave as malware, anomalous network traffic, and advanced phishing attacks. Further, the machine learning is delivered on-device, securing it even if the endpoint is not connected to the network.

### Privacy-Focused, Enterprise Mobile Security

With a privacy-by-design approach, Zimperium MTD provides users with a transparent experience by delivering customizable user settings and insight into what data is collected and used for threat intelligence. Because Zimperium MTD's detection is done on-device, private information is never sent to the cloud.

### Scalable Enterprise Mobile Security

Zimperium MTD can be used as a stand-alone tool or integrated with a MDM/EMM for managed devices. When integrated with a MDM/EMM, Zimperium MTD sends alerts about detected threats to the MDM/EMM, and the MDM/EMM remediates the risk based on predefined rules. Zimperium MTD works seamlessly with leading MDM/EMM solutions and is the only mobile threat defense solution that can simultaneously integrate with multiple MDMs/EMMs, which is particularly helpful when transitioning solutions. Zimperium MTD can also be used for unmanaged devices with mobile application

management (MAM). With MAM-enabled apps, when a user launches a work application, such as Microsoft O365, on a mobile device, the application only permits access when mobile threat defense is running on the device.





## Cyprus HQ

15, Aglantzia, 1st floor, 2108 Nicosia, Cyprus  
Tel: +357 22 441514

## Greece

34 Amfitheas Ave, 1st floor, 17564 Palaio Faliro, Greece  
Tel: +30 215215 4480

## Balkans

1 Rudo, 1000 Belgrade, Serbia  
Tel: +38 64 311 25 85

