Trellix

SOLUTION BRIEF

Trellix Network Detection and Response

Steer clear of costly cyberbreaches and other evolving threats

In an ideal world, you wouldn't have to think twice about your network security. You could operate with complete confidence, knowing your entire infrastructure is safe and sound.

But cyberbreaches are an unfortunate reality for organizations both big and small. And as threats grow more sophisticated and complex, businesses are forced to deal with their many adverse impacts—from system downtime and financial penalties to reputational loss.

270
In 2021, the average company experienced 270 cyberattacks.[1]

53%
Up to 53% of all attacks can lead to cyberbreaches.[2]

$4.24 million
The average total cost of a single data breach is upwards of $4 million.[3]

Five must-haves for advanced cyberbreach protection

For your organization to protect its infrastructure and rise above cyberbreaches and other dynamic attacks, you need a living, learning network security solution—one that empowers you to:

1. Detect and prevent threats other products miss
2. Proactively respond to and quickly contain incidents
3. Quantify incident impact and improve response quality
4. Adapt to the constantly evolving threat landscape
5. Scale as your business changes and grows

1. State of Cybersecurity Resilience, Accenture, 2021
2. State of Cybersecurity Resilience, Accenture, 2021
3. Cost of a Data Breach Report, Ponemon Institute, 2021

Harness the power of Network Detection and Response

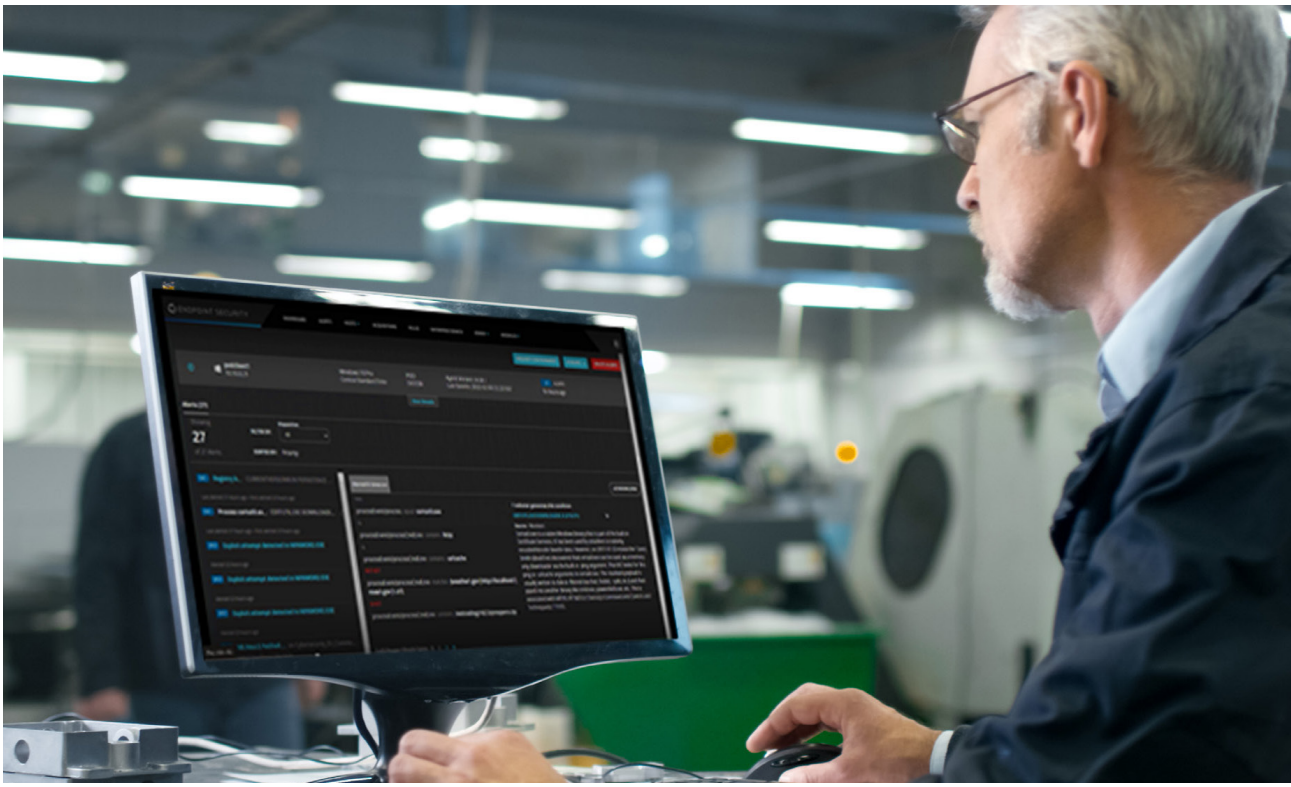
Welcome to the new normal in cybersecurity—where every organization must go beyond mere prevention. Today's businesses require the ability to monitor their environments in real time and address incidents the moment they arise.

Enter Trellix Network Detection and Response (NDR).

NDR uses behavioral techniques like machine learning and advanced analytics to detect network anomalies and analyze raw traffic and flow records to establish baseline network behavior patterns. It allows your team to examine traffic as it crosses the perimeter (north/south) and moves laterally throughout your network (east/west). It also enables you to take advantage of response capabilities to remediate the threat of suspicious network traffic.

It's time to shore up your defenses. To put an end to costly cyberbreaches. To gain greater peace of mind knowing your organization and its people are protected against advanced, targeted, and other evasive attacks.

It's time for Trellix Network Detection and Response.



Trust Trellix to protect your network

The Trellix Network Detection and Response solution gives you everything you need to ensure the ongoing safety of your hybrid networks, data centers, and servers.

Our living security solutions provide your organization with the ability to:

Detect the undetectable

Gain improved visibility into all network traffic. Locate zero-day, ransomware, and other attacks hiding in your hybrid network infrastructure. Correlate events across multiple security vectors—including email, endpoint, and more—for end-to-end protection.

Reduce mean time to detect and respond

Harness the power of AI, machine learning, and correlation engines to monitor attacks around the clock. Give your SecOps staff the contextual intelligence and concrete evidence they need to quickly and accurately resolve incidents. Automate alert-response workflows to speed time to resolution.

Improve process and employee efficiencies

Empower your security analysts by reducing alert volume and alleviating alert fatigue. Prioritize alerts and free up your staff so they can focus their efforts on the threats that matter most. Take advantage of automated response capabilities to minimize manual errors and maximize employee productivity.

Introducing the Trellix Network Detection and Response

Industry accolades

First Prize:
NAVWAR AI ATAC

2022 Gold Winner:
Network Detection and Response, Cyber Security Global Excellence

Certified Secure Distinction Award:
Next-Generation IPS, Miercom

Whether you need to inspect network traffic, block advanced threats, or streamline attack investigations, Trellix has you covered.

Trellix Network Security

Automatically spot suspicious network behavior and prevent attacks that elude traditional signature- and policy-based security. Combining multiple AI, machine learning, and correlation engines, Trellix Network Security allows you to detect and respond to advanced threats and lateral movements in a matter of minutes.

Trellix Intrusion Prevention System

No matter where intruders are hiding, Trellix Intrusion Prevention System can help you find them—and keep them out for good. With advanced threat prevention capabilities, you can continuously monitor your network for malicious activity and block intrusions the moment you identify them.

Trellix Network Forensics

Get to the bottom of the threats impacting your organization. Trellix Network Forensics enables you to better quantify the impact of an attack and improve the quality of your response. Plus, you can visualize events before, during, and after an attack to keep incidents from happening again and again.

Take your network security to the next level

The safety and well-being of your network is crucial to your company's success. It's the key to keeping your employees productive and your customers satisfied.

With innovative network protection delivered on-premises or in the cloud, you can always stay one step ahead of constantly evolving attacks. So steer clear of cyberbreaches and the consequences they bring—from fines to frustrations to headlines—with Trellix Network Security.

Why choose Trellix Network Detection and Response: Solution benefits at a glance

Detect and prevent threats other products miss

Capability	Benefit
Signatureless threat detection	Detects multiflow, multistage, zero-day, polymorphic, ransomware, and other evasive attacks
Real-time and retroactive detection	Monitors known and unknown threats in real time and enables back-in-time threat detection
Multivector correlation	Automates validation and blocks attacks across email, endpoint, and other security vectors
Lateral movement detection	Detects formerly undetectable suspicious network traffic within the network
DoS and DDoS prevention	Prevents malicious traffic from reaching your network, while allowing legitimate traffic to get through
Inbound/outbound SSL decryption	Detects malware and other advanced threats in inbound and outbound encrypted traffic
MultiOS, multifile, and multiapp support	Supports heterogeneous endpoint environments for a wide range of applications
Hardened hypervisor	Provides evasion proofing

Proactively respond to and quickly contain incidents

Capability	Benefit
Real-time inline blocking	Stops attacks instantly
Advanced intrusion prevention	Performs deep inspection of network traffic to detect and protect against malware callbacks and other advanced threats
Integrated security workflows	Pivots from detection to investigation and response
High availability	Provides resilient defense
Signature-based IPS detection with noise reduction	Automates and accelerates alert noise triaging to eliminate manual overhead
Riskware detection and categorization	Categorizes critical and non-critical malware to prioritize response resources
Actionable contextual intelligence	Accelerates advanced threat containment by providing in-depth information about the attack and attacker

Quantify incident impact and improve response quality

Capability	Benefit
Rich context	Reviews specific network packets, connections, and sessions before, during, and after an attack
Retrospective threat hunting	Integrates threat intelligence for back-in-time IOC threat analysis and provides automatic alerts to IOCs present in your network days or weeks earlier
Breach impact reduction	Accelerates forensics process with a single workbench with immediate one-click pivot to session data from alerts

Adapt to the constantly evolving threat landscape

Capability	Benefit
Real-time threat intelligence sharing	Enables the global sharing of real evidence to immediately block previously unknown attacks and accelerate response
Custom and third-party threat intelligence	Ingests Trellix intelligence and third-party indicators into our engines for better threat insights
Strategic threat intelligence	Permits proactive assessments of changes in the threat landscape to strengthen security posture

Scale as your business changes and grows

Capability	Benefit
Supported bandwidths	50 Mbps–14 Gbps Up to 100 Gbps (IPS) Up to 20 Gbps (Forensics)
Supported scale	Single site to thousands of sites for distributed deployments
Supported deployments	Physical, virtual, and cloud

Trellix
6000 Headquarters Drive
Plano, TX 75024
www.trellix.com

To schedule a demo, visit trellix.com

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.