Trellix

EBOOK

Be a Security Superhero with Trellix Helix Detect

Understand how to face the increasing threats faced by small and medium sized businesses

aws PARTNER

- Public Sector
- AWS Marketplace Seller
- Authority to Operate
- Security Software Competency

Protect your company, regardless of size, from unauthorized users

There was a time when cyber threats like ransomware were something only large, global enterprises and organizations needed to understand and respond. These big organizations had the intellectual property and financial resources that were enticing threat actors.

But that's changing.

Threats are moving down-market as smaller companies do not have the security tools of larger companies, which makes them vulnerable. Meanwhile, ransomware as a service and cryptocurrency for facilitating payment has made the attacker's job effortless.

As a result of these threats, smaller-sized businesses need to modernize their security operations. But without the budget for enterprise-grade solutions or in-house skills, they seek a holistic, foundational approach that provides comprehensive cybersecurity without an expensive price tag.

In this eBook, discover how even a lean security team can handle the most complicated of incidents.

Legacy systems are unable to handle threat volume

No matter the company size, protecting against online threats is a struggle that keeps getting tougher as both tools and attack methods evolve. The challenge is put into perspective when you look at the numbers.

One study found that 35 percent of security analysts ignore alerts when the queue gets too full.[1] And another survey discovered that 70 percent of IT security stakeholders report more than double the volume of security alerts in the past five years.[2]

Many companies suffer from lack of visibility across different threat vectors. Using legacy security and information event management (SIEM), they can centralize security operations. However, legacy SIEM don't have the scale and data to connect the dots. This can result in more alerts than customers can reasonably keep up with—and missing the ones that matter.

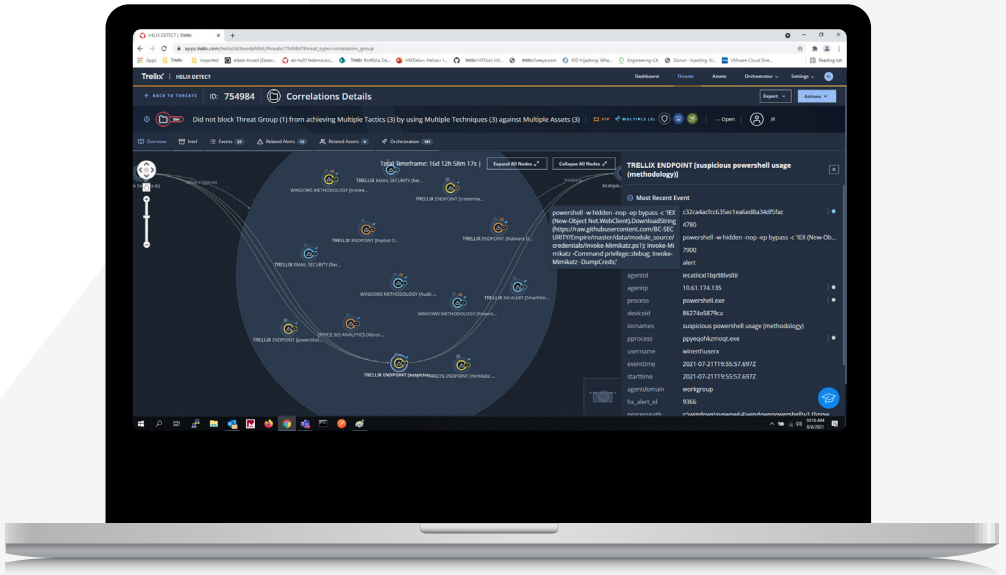
There are risks and negative consequences of a poorly managed or inefficient security operations center (SOC). That can lead to missing critical alerts, wasting time and resources configuring disparate tools, and slow response times due to lack of analyst competency or situational awareness as well as the inability to prioritize threats.

1. IDC, The Voice of the Analysts, January 2021
2. Dimensional Research, 2020 State of SecOps and Automation, Dimensional Research, 2020

How do you know if you're a target?

These days, anyone can be a target as every organization faces security risks. Ransomware attacks are rising exponentially and, for example, the SolarWinds breach impacted thousands of companies.

An important component of any security strategy is reducing dwell time, or the time between when an attack begins and when it is discovered. Trellix recommends the following three steps to reduce dwell time:



1. **The first step** is to gain visibility into what's happening across your company while having all your data connected in one place. You don't want to be spending hours each day collecting data and writing scripts to compare different data feeds. Trellix Helix works instantly with over 600 different data sources, affording greater visibility across your ecosystem.

2. **The second step** is making sure you are responding to the top threats. Trellix's advanced detection sees 1,000 malicious attacks every minute. When coupled with advanced artificial intelligence (AI) that spots risky users and behaviors, it can help surface the most important threats across your organization.

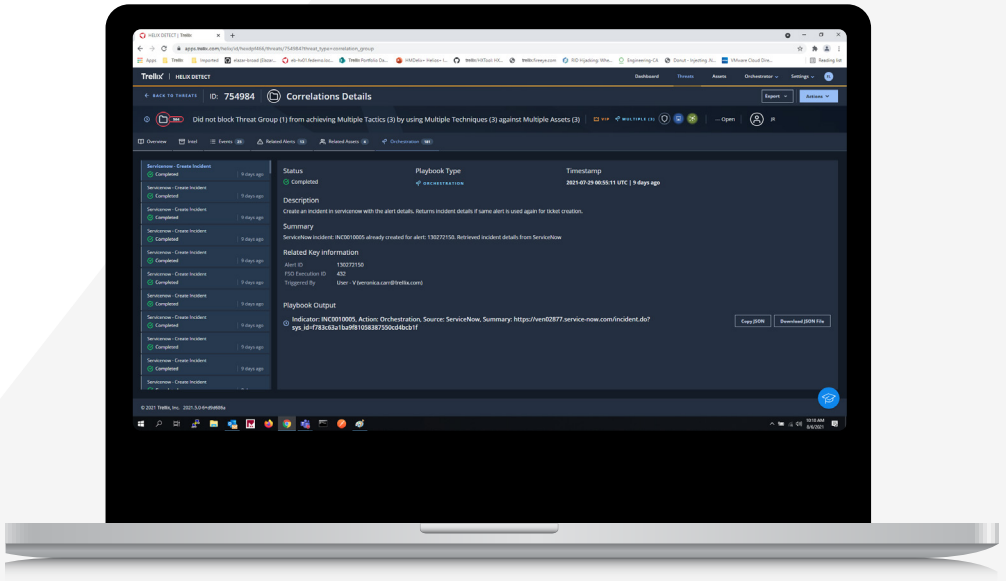
3. **The final step** is responding to incidents as quickly as possible. Trellix Helix provides frontline expertise on dealing with almost any incident and walks you through what to investigate. This, on top of Trellix's automated orchestration features, helps accelerate your response time and improve the efficiency of your security team.

Where to start your journey to be a SecOps superhero

How do you corral improvements across your security operations (SecOps) in a way that bolsters team performance and processes to make a significant reduction in your cyber threat exposure?

And given all those considerations, how do you accomplish it when resources and budgets are tight?

You need a superhero.



Trellix Helix, a tool used by many Fortune 500 companies, is now available to small-business customers to take the first step on their security journey.

Trellix Helix is a SaaS security operations platform that gives you more control over incidents, from detection to response. Trellix Helix integrates disparate security tools and augments them with next-generation SIEM, orchestration, and threat intelligence capabilities to capture the untapped potential of your security investments.

Helix Detect is a new extended detection and response (XDR) SaaS edition of Trellix Helix tailored for those that want superior detection and response—and still benefit from low overhead.

Helix Detect is designed to improve your analyst and SOC efficiency by correlating disparate events from multiple tools into actionable investigations. Helix Detect works smoothly with your third-party security solutions while using security analytics and automation to prioritize investigations to accelerate incident detection and response.

Be a Security Superhero with Trellix Helix Detect

Consolidate your security data and infrastructure

With an interface showing immediate situational awareness, Helix Detect brings together existing security data and infrastructure and detects security incidents by merging data from multiple tools.

That equips your team with the contextual threat intelligence they need to make informed, efficient, and—superhero!—decisions.

Helix Detect minimizes the impact of incidents by accelerating response with security orchestration and workflow automation informed by frontline experience.

You have the option to integrate over 600 Trellix and non-Trellix security tools as well as overlay contextual threat intelligence and behavioral analytics.

Put Trellix and AWS on your SOC team

Trellix and Amazon Web Services (AWS) have come together to expand security capabilities on the cloud and uncover cloud-specific threats.

Here's how Helix Detect helps security professionals find anomalies across AWS:

AWS Network Firewall allows mutual customers to deploy network security via firewall rules across their Amazon Virtual Private Cloud (Amazon VPC). Trellix Helix Detect provides visibility into the traffic, those requests that were allowed or blocked, and enriches with threat intelligence to help prioritize alerts.

AWS Security Hub is a comprehensive view of security alerts and security posture across AWS accounts. Combined with Helix Detect, this provides a holistic view of all third-party tools and alerts, allowing the customer to focus on top security incidents first.

Amazon Guard Duty continuously monitors for malicious activity and unauthorized behavior in AWS accounts, workloads, and data stored in Amazon Simple Storage Service (Amazon S3). Combined with Trellix Helix Detect, teams can respond faster with threat intelligence and prioritized alerts.

Amazon Inspector is an automated vulnerability management service that helps improve the security and compliance of workloads deployed on AWS. Amazon Inspector automatically assesses workloads for exposure, vulnerabilities, and deviations from best practices.

Amazon CloudWatch lets you monitor and capture data and actionable insights about applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. Trellix Helix Detect uses this to understand if operational issues in cloud applications are related to security incidents.

AWS CloudTrail automatically records and stores event logs for actions made within an AWS account. With Trellix Helix Detect, this provides a convenient way to search through log data, identify out-of-compliance events, and accelerate security incident investigations.

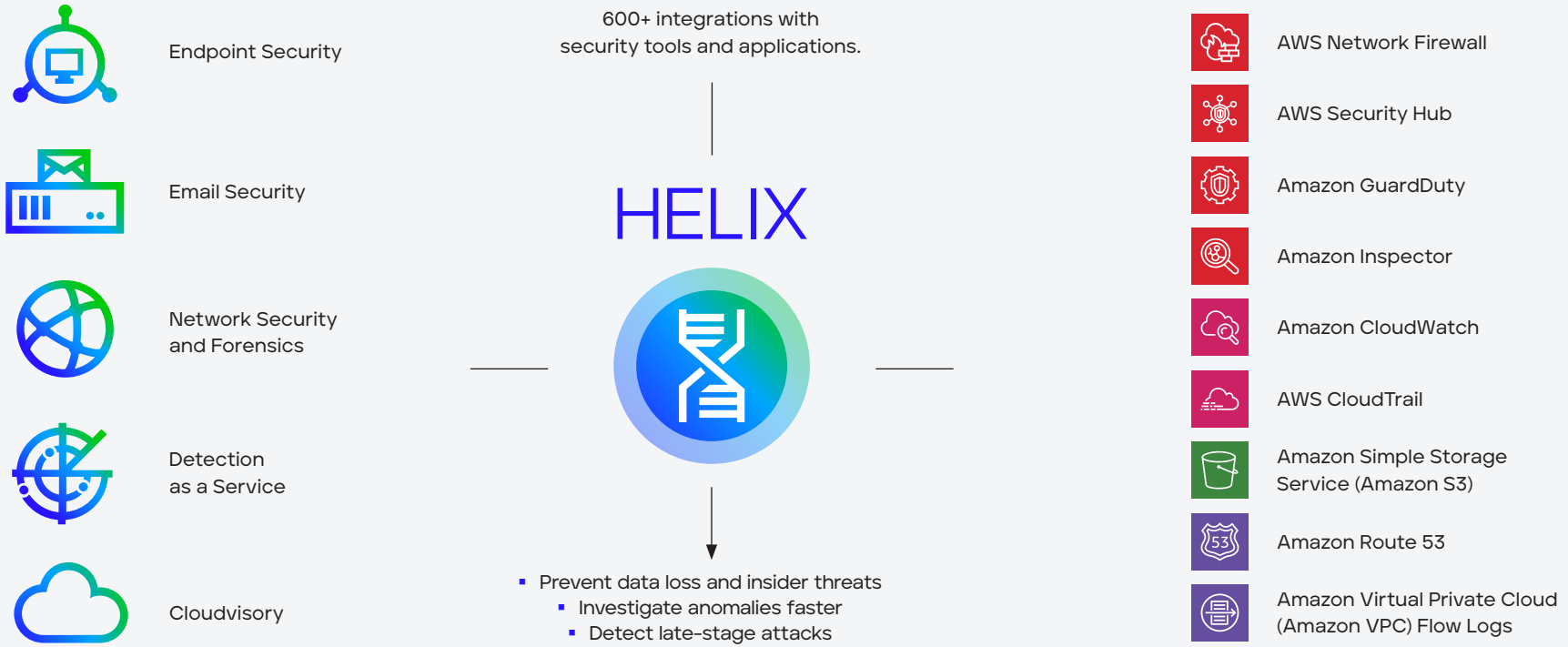
Amazon Simple Storage Service (Amazon S3) is an object storage service that offers scalability, data availability, security, and performance. Combined with Trellix Helix Detect, logs from anywhere can be stored and quickly ingested. Integrations can happen in minutes and customers can start responding to security incidents faster.

Amazon Route 53 captures DNS Firewall information to corollate user requests to infrastructure running in AWS. Trellix Helix can use this information to evaluate the source of these requests and provide risky asset scores when malicious activity is suspected.

Amazon Virtual Private Cloud (Amazon VPC) Flow Logs capture information about the IP traffic going to and from network interfaces in an Amazon VPC. Trellix Helix Detect can alert you to malicious traffic and help with threat hunting.

Trellix Helix Detect

features in-depth dashboard visibility across all AWS metrics and leverages Trellix's deep expertise to highlight risks and mitigate them. This visibility into AWS Cloud usage and data better positions your team to carry out streamlined and strengthened security practices.



Be a Security Superhero with Trellix Helix Detect

Ready to be a security superhero?

Gaining complete visibility into your company's threats and vulnerabilities takes a comprehensive approach. With Helix Detect, you can empower your team with the foundation needed to protect your workloads and data from malicious activity and unauthorized behavior in your AWS accounts.

Trellix solutions are engineered to grow with your organization—they can be reconfigured, added, or upgraded without disrupting organizational operations.

Contact Trellix today to view a demo and find out how you can get started in just a few hours.

Get started with Trellix Helix Detect
Email us for next steps

aws PARTNER
- Public Sector
- AWS Marketplace Seller
- Authority to Operate
- Security Software Competency

Trellix

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity. 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's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.

072022-18