Trellix • aws

SOLUTION BRIEF

Trellix XDR Enhances Zero Trust Architecture with Amazon Web Services (AWS)

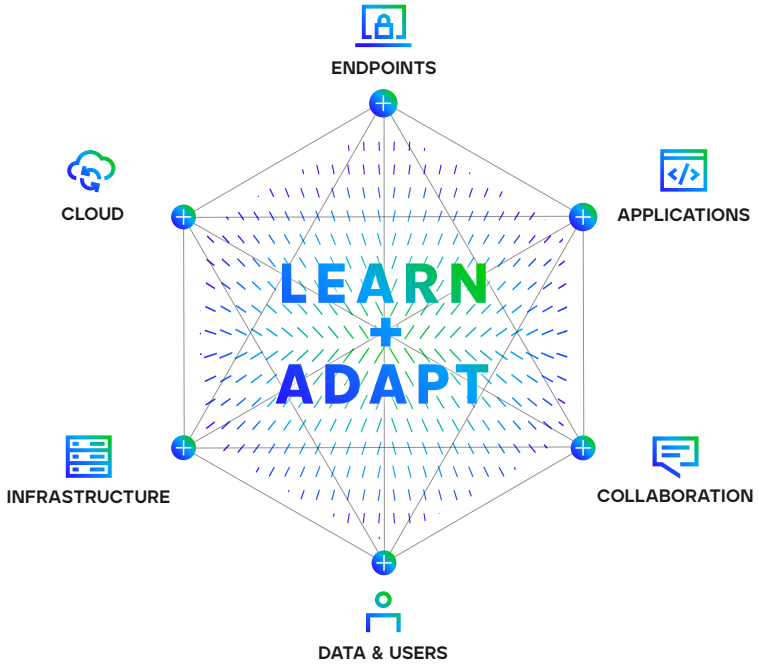
Trellix XDR: We Make Zero Trust Better

"Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources." This quote from NIST highlights that Zero Trust evolves based on the information, processes and tools that are available at any given time for an organization to make decisions on what work can get done. No implicit trust is granted to assets or user accounts based solely on their location, asset ownership or any other factors that organizations relied on historically. The focus is on enabling secure resources, services and workflows regardless of where those live, whenever a task is needed to be performed.

How does Zero Trust work with XDR (eXtended Detection and Response)? XDR improves and adds to a company's Zero Trust framework. Visibility and mitigation of security threats are as important as ever, but the challenge of seeing all potential attacks is heightened due to the decentralized, dynamic nature of Zero Trust deployments. Trellix makes Zero Trust architectures better by finding the risks in all your telemetry and sharing that with the tools/processes that help determine the authorization and access levels needed for business to perform their work securely. Trellix's flexible XDR platform connects all Trellix technologies and a broad ecosystem of over 800 vendor partners and tools to provide a seamless SecOps experience in one place.

Visibility into endpoint activity, email messages, network traffic, cloud security posture, data security and many other sources is crucial in Zero Trust since assets are no longer confined to Enterprise boundaries and ownership. Trellix Security Solutions analyze and protect your critical vectors, feeding it to Trellix Helix Security Platform, which offers advanced detection and correlation capabilities and automated responses to help protect your business.

LIVING SECURITY XDR ECOSYSTEM



Highlights:

- Visualize and analyze security threats regardless of where they occur
- Stop zero-day, phishing attacks, malware and advanced targeted attacks
- Easily scale deployments while lowering total cost of ownership
- Provide risk scoring of users, accounts and assets that change the way people and things perform business operations

How Trellix Security Solutions Protect Your Business	
Cloud Assets	Trellix Cloudvisory provides centralized control for managing multi-cloud environments with continuous & proactive compliance for multi-account, multi-cloud, environments. This includes all-around protection from cloud-native microservices for asset discovery, policy governance, control over cloud sprawl and infrastructure misconfiguration.
Network	Trellix Network Security is an advanced threat protection and breach and lateral movement detection solution with visibility and SaaS based alerting into the most sophisticated attacks, deployed via AMI's into VPCs.
Endpoints	Trellix Endpoint Security is a flexible, unified solution that protects devices and endpoints at the network edge, empowering your organization to address complex, distributed security issues utilizing analytics and machine learning.
Operations	Trellix Security Operations is an integrated approach to improving your cyberattack management and security posture through threat intelligence, endpoint policy management and our Sec Ops platform Trellix Helix that allows you to take control of security issues from incident to detection to response.
Data	Trellix Data Protection empowers you to discover, monitor, and protect sensitive data across your AWS and on-premise environments with centralize management and reporting. Additional capabilities include scanning S3 buckets for malicious content.
Email	Trellix Email Security identifies and mitigates advanced email threats—including ransomware, business email compromise (BEC), and phishing.

Figure 2: Trellix Helix Dashboard to highlight the top risks in a customer's ecosystem

This fulfills the promise of XDR, by allowing customers to identify and respond to threats faster, ensuring the latest risks are always being used to determine how a business should operate.

Want to learn more?

Start leveraging the speed and efficiency used between Trellix and AWS to respond to security issues today. Please reach out to AWS@Trellix.com to learn more or join our latest XDR workshop to get hands-on with Trellix today!

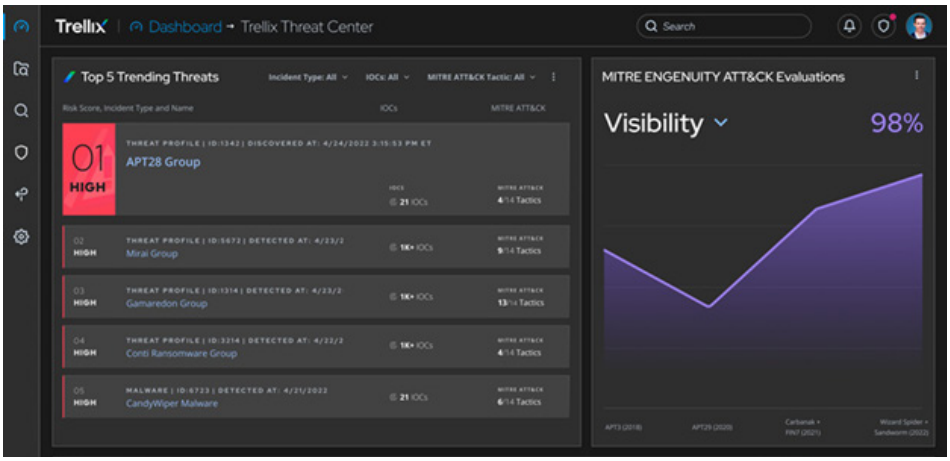
To see how Trellix and AWS work together, view our integrations and marketplace listings on the AWS Marketplace.

All of our solutions leverage AWS to scale to meet your business needs while fulfilling the shared capability model to protect your AWS resources. Security and compliance is a shared responsibility between AWS and you, the customer. This shared model can help you relieve the operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Our customers assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS provided security groups. By leveraging your AWS telemetry into Trellix Helix, we can ensure there are no misconfigurations and risks associated with your ownership of the shared responsibility model.

This telemetry is then used to identify risks of users and assets when combined with the rest of your visibility.

How Trellix Helix Enhances Your Zero-Trust Architecture

Customers can leverage Trellix Helix to gain visibility into the riskiest and most vulnerable users and assets in their environments. This is done by enriching your telemetry with threat intelligence and evaluating with behavior analysis and machine learning to prioritize those alerts that are most actionable. By evaluating a user/asset and the risks correlated across their endpoint, network, email, data and cloud actions, Trellix is able to rate how risky they are and that information is shared with downstream systems such as IAM providers to take the appropriate action the next time a user/asset performs a business action.



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.