Resecurity

Endpoint Protection

Advanced Threat Detection and Monitoring

The Challenge

The revolutionary changes in technology has led to an increased attack surface for businesses adopting the myriad of advantages across mobile, traditional internet web applications and cloud-based hosting. While the vast level of improved technology has its benefits, it also adds increased risk of threats and vulnerabilities.

In 2020, 86% of security breaches are financially motivated, making endpoint vulnerabilities an attractive opportunity for attackers.

The challenge for the enterprise is to continually defend against advanced attacks designed to find and exploit unknown vulnerabilities.

`

It only takes minutes for an attacker to exfiltrate data after a compromise, which makes it more important than ever to implement effective cyber-defenses on all endpoints to quickly detect, eradicate and alert administrators.

The EPP Solution

Resecurity offers an intelligence-based endpoint protection platform that detects the most complex advanced threats in the wild and stops them from becoming a critical data breach.

Our endpoint protection management system is fully scalable and flexible to work with any network environment and performs real-time threat intelligence for all mobile, web, and cloud endpoint attack surfaces. We provide solutions to help the enterprise maintain maximum visibility across all endpoints and enforce security against advanced threats targeting your organization.

EPP Benefits

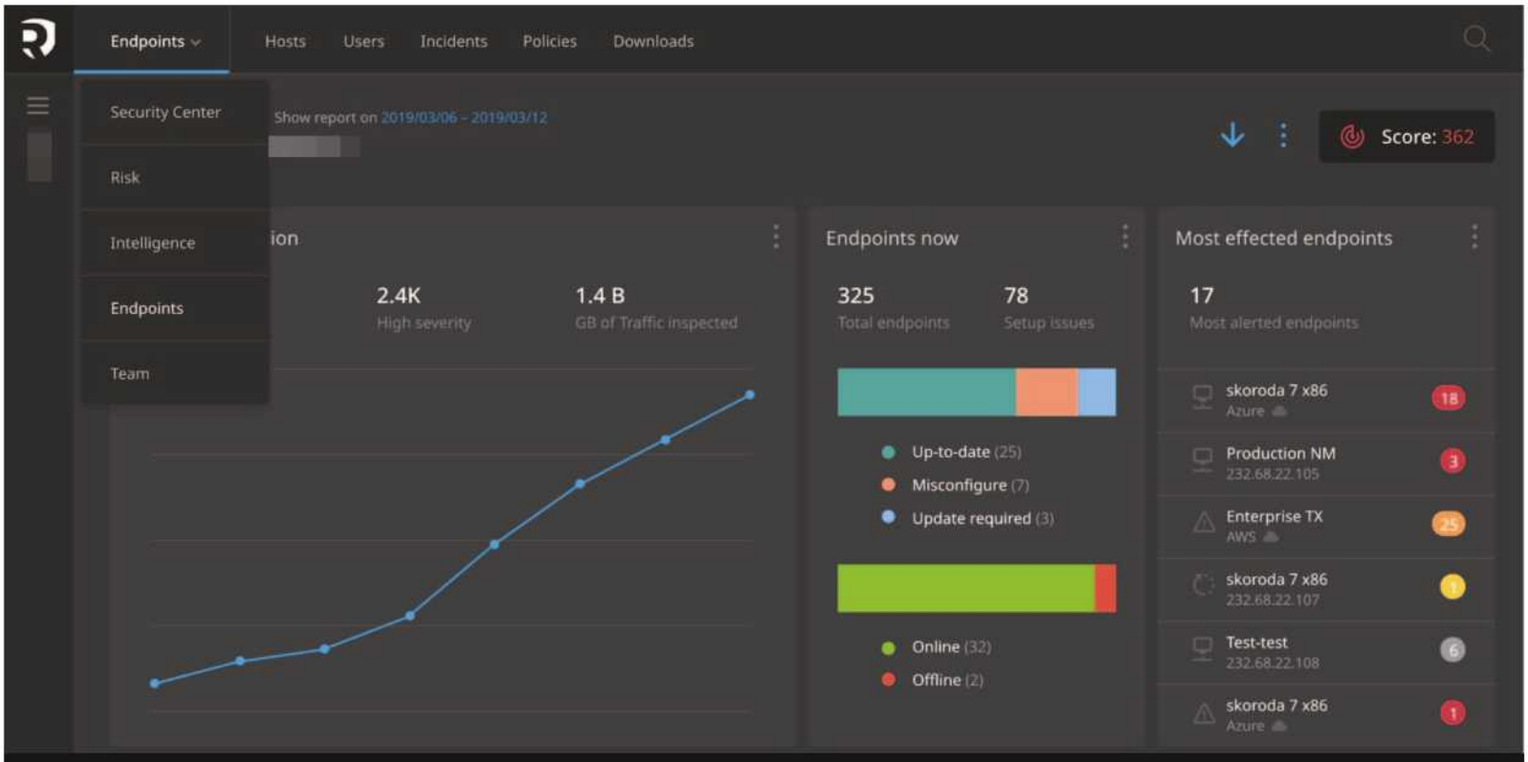
- Prevent targeted malware, ransomware, phishing, and other attacks against all endpoints and devices.
- Detect unknown advanced threats including stealth attacks.
- Leverage artificial intelligence to automatically stop complex cyber attacks.
- Generate analysis reports that provide actionable strategic feedback.
- Simplify management of your cyber defenses while providing a full 360-degree overview of endpoint activity.
- Stop ransomware, malware, zero-day vulnerabilities, and millions of other threats targeting your organization.

Key Features

- Early detection and warnings from a fully configurable central managemen console.
- Easy to use controls to manage every accessible endpoint.
- Incident analysis that provides actionableremediation advice.
- Centralized interface for full visibility of all cyber security events.
- Automatic analysis with built-in incident reports.
- Full cryptographically secure encryption to protect data.

Centralized Security Management

Simplify the way administrators and IT staff manage and oversee endpoint security. Administrators can access their management console from the operating system and device of their choice.



Ransomware and Malware Protection

Stop the most malicious attacks that could destroy data and cost the organization millions in disaster recovery, investigations, remediation and legal fees. Quarantine suspicious files and email attachments to stop attacks at the start.

Real-Time Monitoring and Alerts

Understand what is happening on all endpoints using real-time reports and threat alerts. Detailed alerts and notifications provide a comprehensive overview of all endpoint and device statuses and detect suspicious activity.

Configuration Interface for Devices and Profiles

Configure profiles and devices using cyber security templates that help administrators properly define authentication and authorization. Apply policies across profiles for least privilege authorization protecting digital assets.

Intuitive Installation and Deployment

Deploy cyber security features across the environment with intuitive installation controls. Flexible configurations help administrators deploy the right solution that follows the organization's unique environment requirements.

Automated Patch Management

Ensure your operating systems and applications are up-to-date with the latest patches. Find unpatched vulnerable software before attackers and update it securely from a central controller.

Email Protection and Phishing Defenses

Prevent email-based phishing and social engineering attacks. Quarantine suspicious messages that contain malicious links or file attachments.

Resecurity www.resecurity.com info@resecurity.com (800) 781-5698 445 S. Figueroa Street, 31st Floor, Los Angeles CA 90071, USA.