CYREN BY DATA443™

Risk-Based Decision-Making Using Threat Intelligence

Solution Brief

Business Challenge

Organizations spend millions of dollars annually to protect themselves against new cyber threats. But opportunistic attackers have continued to evolve their tactics and have managed to stay one step ahead of organizational defenses. This lack of visibility into new, evolving attacks has led to an increased occurrence of security incidents and breaches. These increased attacks have caused CISOs to scramble and come up with ad-hoc strategies to effectively balance enterprise security and business productivity. The lack of quality intelligence preventing rapid threat identification and response has become a major headache for CISOs.

Solution Benefits

- Understand the evolving threat landscape and its impact
- Reduce organizational risk through data-based decision making
- Optimized response for email-borne threats, maximizing returns

Challenges Solved by Threat Intelligence

Impact of Evolving Threats on Organizational Security - Constantly evolving security threats means security teams have to sort through massive amounts of seemingly unrelated threat data and understand which threats are connected and can impact their organization. This can lead to missed detections and increased organizational vulnerability. Context can help teams identify and prioritize threats that matter the most. Without this context, security executives cannot make accurate decisions to address organizational vulnerabilities and evolve their security posture against emerging threats.

Managing Organizational Risk and Business Productivity - Security executives constantly walk the tightrope between organizational risk and business productivity. With the threat landscape constantly changing, investing in the right security tools while ensuring minimal impact on business processes is objectively challenging. Making security investment decisions without the right threat data can potentially backfire on the executive and cause brand and monetary damage to the organization.

Ensuring Effective Threat Response - Security teams are constantly playing a cat-and-mouse game with rapidly changing attacker techniques. Existing security investments can effectively block known threats and existing attack vectors. But protecting the organization against new, evolving threats requires real-time visibility into targeted attacks and campaigns as they emerge and develop. Lack of this visibility can slow down threat detection and response leaving the organization vulnerable to attacks. Security executives are responsible for empowering their teams with the right tools and credible sources of intelligence to help achieve this objective.

25B	1.3B	300M
Security Transactions Daily	Users Protected	Threats Blocked Daily

CYREN BY DATA443™

Risk-Based Decision-Making Using Threat Intelligence

Solution Brief

Cyren Threat InDepth is contextualized, correlated threat intelligence that allows security teams and security executives to gain a comprehensive and multi-dimensional view of evolving email-borne threats and make meaningful decisions to combat them. This high-fidelity, actionable intelligence is gathered by analyzing, processing, and correlating billions of daily transactions across email content, suspicious files, and web traffic to provide unique, timely insights. Threat InDepth is available to enterprises as – Phishing & Fraud URL Intelligence, Malware URL Intelligence, Malware File Intelligence, and IP Reputation Intelligence. Threat InDepth assists security executives in making smart and effective business decisions that protect their enterprise while ensuring maximum
business productivity.

Threat InDepth Benefits

1. Contextual Insights that Evolve Organizational Security: Quality threat Intelligence provides security teams with the context needed to understand what, where, and how of the threat allowing them to rapidly identify and prioritize evolving threats. This prevents them from being blindsided while providing a more comprehensive view of the evolving threat landscape. Threat InDepth provides timely, contextual, and actionable intelligence that improves threat prioritization and decision-making allowing executives to understand the impact of emerging threats and evolve their security posture to address them.

2. Balancing Organizational Risk through Data-Based Decision Making: Contextual threat intelligence provides executives with a means of measuring organizational risk in near real-time. These insights lead to them making better business decisions that can minimize their organizational risk while ensuring business productivity. By providing quality, contextualized, and timely threat data, Threat InDepth allows security executives to understand the constantly changing organizational risk and make appropriate business decisions to minimize risk.

3. Optimize Threat Response and Maximize Security Investment ROI: Contextual insights and timely threat visibility help security teams and decision makers stay on top of the latest attack trends. Security investments can leverage this information to effectively detect and respond to evolving threats. Threat InDepth provides CISOs with unmatched threat visibility and context, allowing them to rapidly prioritize threat response against existing and evolving threats. This high-fidelity intelligence supercharges existing security investments and empowers CISOs to define and optimize proactive response against a fast-changing threat landscape.

IP Reputation Intelligence

Phishing & Fraud URL Intelligence

Malware URL Intelligence

Malware File Intelligence