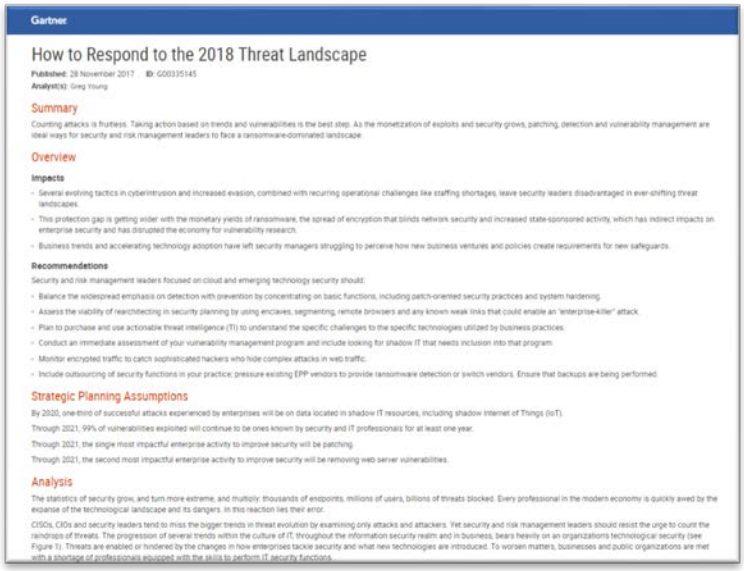
vmware®

REALIZE WHAT'S POSSIBLE.™

Analyst Report: Gartner

How to Respond to the 2018 Threat Landscape

Ransomware has opened a new era for security and risk management leaders. You know you must be proactive rather than reactive. But how? Gartner research has analyzed the latest trends and found that the evolving tactics in cyberintrusion coupled with decreased budgets and staffing for IT have put you at a disadvantage. Gartner has developed a set of recommendations for those focused on cloud and emerging technology to help you navigate this current threat landscape.



Gartner

How to Respond to the 2018 Threat Landscape

Published: 28 November 2017 ID: G00335145

Analyst(s): Greg Young

Summary

Counting attacks is fruitless. Taking action based on trends and vulnerabilities is the best step. As the monetization of exploits and security grows, patching, detection and vulnerability management are ideal ways for security and risk management leaders to face a ransomware-dominated landscape.

Overview

Impacts

- Several evolving tactics in cyberintrusion and increased evasion, combined with recurring operational challenges like staffing shortages, leave security leaders disadvantaged in ever-shifting threat landscapes.
- This protection gap is getting wider with the monetary yields of ransomware, the spread of encryption that blinds network security and increased state-sponsored activity, which has indirect impacts on enterprise security and has disrupted the economy for vulnerability research.
- Business trends and accelerating technology adoption have left security managers struggling to perceive how new business ventures and policies create requirements for new safeguards.

Recommendations

Security and risk management leaders focused on cloud and emerging technology security should:

- Balance the widespread emphasis on detection with prevention by concentrating on basic functions, including patch-oriented security practices and system hardening.
- Assess the viability of rearchitecting in security planning by using enclaves, segmenting, remote browsers and any known weak links that could enable an "enterprise-killer" attack.
- Plan to purchase and use actionable threat intelligence (TI) to understand the specific challenges to the specific technologies utilized by business practices.
- Conduct an immediate assessment of your vulnerability management program and include looking for shadow IT that needs inclusion into that program.
- Monitor encrypted traffic to catch sophisticated hackers who hide complex attacks in web traffic.
- Include outsourcing of security functions in your practice; pressure existing EPP vendors to provide ransomware detection or switch vendors. Ensure that backups are being performed.

Strategic Planning Assumptions

By 2020, one-third of successful attacks experienced by enterprises will be on data located in shadow IT resources, including shadow Internet of Things (IoT).

Through 2021, 99% of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.

Through 2021, the single most impactful enterprise activity to improve security will be patching.

Through 2021, the second most impactful enterprise activity to improve security will be removing web server vulnerabilities.

Analysis

The statistics of security grow, and turn more extreme, and multiply: thousands of endpoints, millions of users, billions of threats blocked. Every professional in the modern economy is quickly awed by the expanse of the technological landscape and its dangers. In this reaction lies their error.

CISOs, CIOs and security leaders tend to miss the bigger trends in threat evolution by examining only attacks and attackers. Yet security and risk management leaders should resist the urge to count the raindrops of threats. The progression of several trends within the culture of IT, throughout the information security realm and in business, bears heavily on an organizations technological security (see Figure 1). Threats are enabled or hindered by the changes in how enterprises tackle security and what new technologies are introduced. To worsen matters, businesses and public organizations are met with a shortage of professionals equipped with the skills to perform IT security functions.

Access the Report Today