Why automation is essential for cyber resilience

Digital transformation makes today’s businesses more productive and more vulnerable to cyberattacks. Security professionals know that breaches are inevitable. To be successful, companies must establish cyber-resilient endpoints. Where do you turn when legacy approaches fail? In a word: Automation.

Companies are at risk

75% of organizations assume they are likely to experience a breach within the next 1–3 years.\(^1\)

33% of cybersecurity professionals lack a response plan for a security breach.\(^2\)

A lot is at stake

$4.2M in average losses
Customer turnover, increased customer acquisition investments, reputation damage, and diminished goodwill all contribute.\(^3\)

$1M first 30 days
Companies that contain a breach in less than 30 days save $1M compared to those requiring more than 30 days.\(^4\)

266 days to respond
On average, it takes companies 197 days to identify an attack and 69 days to contain it.\(^5\)
Where traditional approaches fail

**Lack of visibility**
- 46% of cybersecurity professionals claim their cyber resilience is impeded by a lack of visibility into applications and data assets.

**Staffing shortages**
- 56% of organizations report having an inability to hire and retain skilled staff.
- There will be 3.5M unfilled cybersecurity positions by 2021.

**Expanding attack surface**
- Cloud adoption and device mobility have introduced distributed networks.
- 67% of enterprise infrastructure and software will be cloud-based by 2020.

Why automation is a must

Automated cybersecurity performs at the same speed and scale as attacks themselves, delivering a rapid, active response where endpoint recovery is achieved within minutes. This allows CISOs to strengthen cyber resilience and relieve pressure from staff and skills resource constraints.

**The right approach**
Most security professionals (54%) have invested in automated cybersecurity.

**Rapid response**
71% of security professionals state that automation improves response time for detection.

**Cyber resilience**
When CISOs adopt automated cybersecurity for threat detection, endpoint isolation, remediation, and data recovery, they can confidently advance business initiatives in the following ways:

- Deliver real-time reports to board members
- Maintain business operations
- Protect customer and company data
- Protect company reputation

87% of security professionals are required to discuss security response plans with their executives and boards at least once a year.
Protect your business

Cyber-resilient companies understand the value of their data and implement automated solutions to relieve resources and allow analysts to focus on revenue-generating initiatives.

Learn more about cyber resilience

Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware and exploits that escape detection by traditional antivirus solutions. Malwarebytes completely replaces antivirus with artificial intelligence-powered technology that stops cyberattacks before they can compromise home computers and business endpoints. Learn more at www.malwarebytes.com.

Copyright © 2019, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.

Citations

visit malwarebytes.com/business/solutions/enterprise

malwarebytes.com | corporate-sales@malwarebytes.com | 1.800.520.2796