ARCTIC WOLF

Reduce Your Attack Surface with Risk Assessment

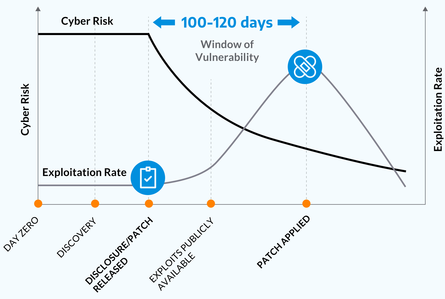
7.2 days

Average time for a hacker to exploit a vulnerability.[1]

120 days

Time to patch a vulnerability.[2]

Close the window of vulnerability by patching vulnerabilities regularly



You cannot measure what you cannot see.

What Is the Impact?

200,000

Computers with unpatched vulnerabilities affected by WannaCry ransomware.[3]

147 million

Equifax records stolen after attackers exploited unpatched vulnerability in Apache web server.[4]

1,000

Number of nuclear centrifuges incapacitated by Stuxnet virus through unpatched Windows.[5]

5 Steps to Effective Risk Management

1. Take asset inventory

2 in 3

Organizations lacking visibility into their networks.[6]

2. Scan assets for vulnerabilities

Organizations scanning their network only once per quarter.[7]

3. Prioritize vulnerabilities based on severity

Organizations finding it difficult to prioritize what to patch first.[8]

4. Report progress on risk mitigation

99.9%

Vulnerabilities unpatched one year after disclosure.[9]

5. Unified visibility across multiple risk vectors

1 in 5

In-house SOCs failing to achieve minimal monitoring capabilities.[10]

For more information about Arctic Wolf risk management solutions, visit arcticwolf.com/solutions/risk-management

Read the White Paper

Reduce Your Attack Surface with Continuous Risk Assessment

Download Now

Sources:

1. Gartner: Implement a Risk-Based Approach to Vulnerability Management, 2018
2. Kenna Security: Remediation Gap Report, 2018
3. WannaCry: Reuters, 2017
4. Equifax: Company SEC filing, 2017
5. Stuxnet: Institute for Science and National Security, 2010
6. SANS: SANS Analytics Intelligence Survey, 2014
7. Secunia: Secunia Vulnerability Review, 2015
8. ServiceNow: ServiceNow Report, 2017
9. Verizon: Data Breach Report, 2015
10. HP: Report on maturity of Cyber Defense Orgs, 2017

ARCTIC WOLF