How to Keep Systems Patched

One of the main jobs of a vulnerability management team is to keep all systems patched to safeguard your enterprise network and data.

KNOW

Get an inventory of your assets to know what systems you have

ASSESS

Understand which assets have vulnerabilities and need patching

PRIORITIZE

Know the priority order in which assets should be fixed based on risk to business

REPORT

Understand how to report on your organization's patching posture

5 Key Steps to Follow

#1

Identify Vulnerable Systems

- Scan all types of assets including non-traditional assets like BYOD, IoT, mobile and cloud.
- Maintain continuous, real-time inventory

#2

Use Modern Vulnerability Tools

- Use risk-based vulnerability management tools to monitor for all weaknesses, not just CVEs
- Automatically target scans to subnets, hosts, and other parts of the network

Do You Know:

- Which systems must be patched right away vs. those which can wait?
- Which assets are critical or more important than others?
- Which CVEs are actively being exploited?
- Which assets have more exposure based on usage patterns, where they exist in the network and whether they are core or internet facing?
- Whether your security controls work well enough to mitigate risk from vulnerabilities on unpatched assets?

#3

Prioritize Vulnerabilities

- Prioritize vulnerabilities based on severity, threat, business criticality, exposure and the impact of security controls.
- Get action items, and assign risk owners based on business priorities
- Set up target mean-time-to-patch SLAs for all kinds of vulnerabilities

#4

Know When to Act or Not to Act

- Understand which systems can't be patched right away or at all
- Identify risk reduction impact by using an appropriate security controls
- Receive timely notifications when emergency patches for vulnerable systems are released
- Use SLAs to create tickets and drive patching workflows

#5

Report on Your Patching Posture

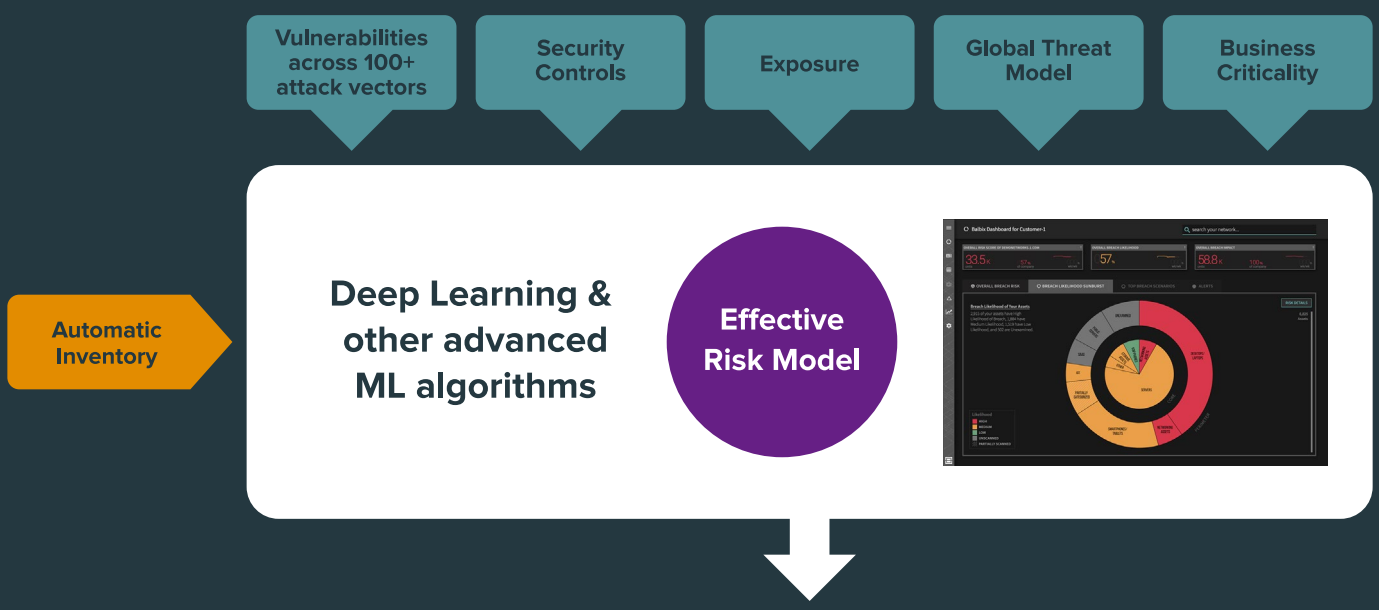
- Generate data on your patching coverage
- Report on your mean-time-to-patch and mean exposure time
- Use heatmaps that show significant areas of concern

Keeping Systems Patched with Balbix

Automatically discover and categorize assets and continuously monitor them across 100+ attack vectors.

Get top risk insights and action items in priority order taking into account 5 factors.

Report on MTTP and MET and keep track of your patching posture.



Balbix®