ROADMAP TO PREVENT RANSOMWARE

What is Ransomware?

Ransomware is malware that encrypts data, offering to decrypt that data only if a ransom is paid. There is often a threat of permanent deletion of the data if the ransom is not paid within a certain amount of time. It's also common for the attackers to threaten to publish of sell the organization's data

DANGER

Ransomware, like many other forms of malware, makes its way into an organization using a variety of techniques—phishing, stolen or weak credentials, vulnerability exploitation, etc. Once it infiltrates the corporate network, most malware spreads across that network, finding and encrypting more data on more machines. The result can be catastrophic, freezing access to information systems across even large companies, bringing their business to a standstill.

8 Steps to Prevent Malware

1 Patch Your Enterprise Applications and Operating Systems

Ransomware and all malware typically exploit known vulnerabilities. An effective patching program which begins with an accurate inventory of all assets, including categorization and calculation of business criticality is needed. From there, risk-based prioritization can ensure that the most important vulnerabilities are fixed first.

2 Update/Remove Old and Obsolete Softwares

37% of IT budgets are wasted on unused software, so removing that software can help with significant cost savings. Regardless, old or obsolete software is a danger because vendors stop issuing security updates

3 Continuous Data Backup and Restoration

Having a strong backup and restoration process in place can ensure that you can restore data that has been encrypted, without paying the ransom. Just make sure that the machines on which the backups are stored are completely isolated from network segments where malware might spread

4 Disable Vulnerable Services Like RDP Whenever Possible

There are a lot of important network services in a typical enterprise network—Telnet, RDP, FTP, etc. These same services can also represent a way to infiltrate your network, so they need to be carefully controlled. Start by identifying critical assets running these services and analyze whether there is a true business need for the service, as well as whether the appropriate compensating controls are in place.

5 Maintain Password Hygiene

Ransomware and all malware typically exploit known vulnerabilities. An effective patching program which begins with an accurate inventory of all assets, including categorization and calculation of business criticality is needed. From there, risk-based prioritization can ensure that the most important vulnerabilities are fixed first.

6 Employ Anti-virus and Email Security

Employing these basic services sounds, well, basic. That said, not all such compensating controls are created equally. It can be just as important to identify effectiveness of your controls as it can be to have them in place to begin with. That means ensuring that they are up-to-date and patched, as well as ensuring that you have the best tools for the job in place.

7 Control Access with Least Privilege and Email Segmentation

Too many privileges add up to too much risk. It's important to identify assets, especially critical machines, where users have more privileges than are necessary for their roles. As with disabling risky network services, risk owner assignment can help ensure that these decisions are being made by the people closest to the area of the business where the assets are used.

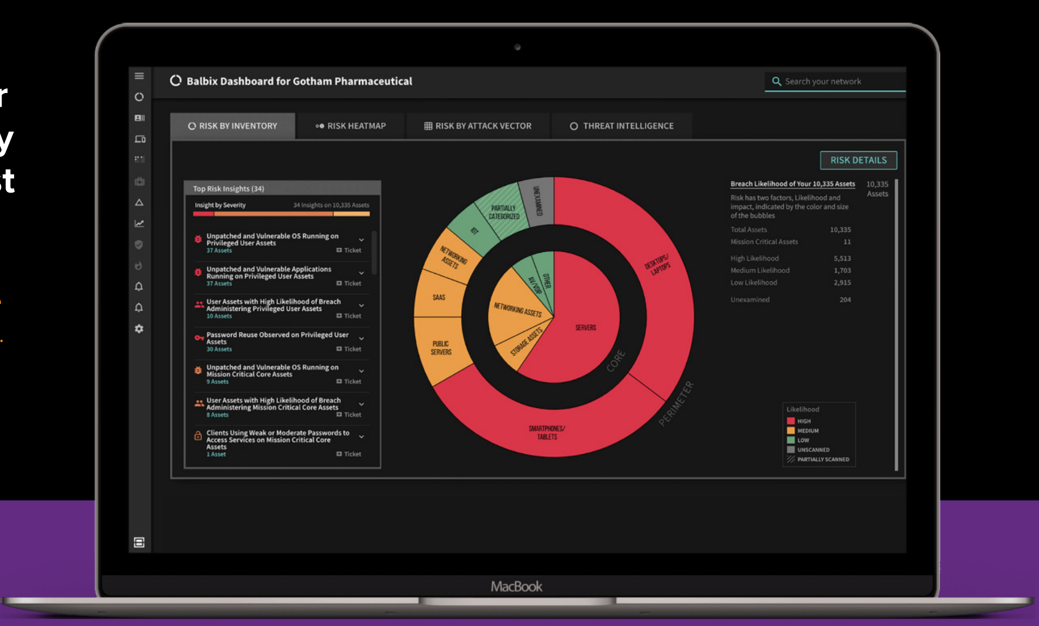
8 Train All Users on Security Awareness

Of course, much of this could be avoided if all users were 100% aware and 100% compliant on appropriate security measures to avoid things like phishing or downloads of malware. Preventing ransomware is a team effort and ensuring that your "team" of end users is appropriately trained and aware is as important as anything else on this list.

Balbix helps to continuously assess your enterprise's cybersecurity posture to protect against ransomware attacks.

Request a demo today to learn more the capabilities in the Balbix platform.

LEARN MORE



Balbix Dashboard for Gotham Pharmaceutical

Search your network

RISK BY INVENTORY | RISK HEATMAP | RISK BY ATTACK VECTOR | THREAT INTELLIGENCE

RISK DETAILS

Top Risk Insights (34)

Insight by Severity — 34 Insights on 10,335 Assets

- Unpatched and Vulnerable OS Running on Privileged User Assets — 37 Assets — Ticket
- Unpatched and Vulnerable Applications Running on Privileged User Assets — 37 Assets — Ticket
- User Assets with High Likelihood of Breach Administering Privileged User Assets — 10 Assets — Ticket
- Password Reuse Observed on Privileged User Assets — 30 Assets — Ticket
- Unpatched and Vulnerable OS Running on Mission Critical Core Assets — 9 Assets — Ticket
- User Assets with High Likelihood of Breach Administering Mission Critical Core Assets — 8 Assets — Ticket
- Clients Using Weak or Moderate Passwords to Access Services on Mission Critical Core Assets — 1 Asset — Ticket

Breach Likelihood of Your 10,335 Assets — 10,335 Assets

Risk has two factors, Likelihood and impact, indicated by the color and size of the bubbles

Total Assets	10,335
Mission Critical Assets	11
High Likelihood	5,513
Medium Likelihood	1,703
Low Likelihood	2,915
Unexamined	204

Likelihood

- 🟥 HIGH
- 🟧 MEDIUM
- 🟩 LOW
- ■ UNSCANNED
- ▨ PARTIALLY SCANNED

Balbix