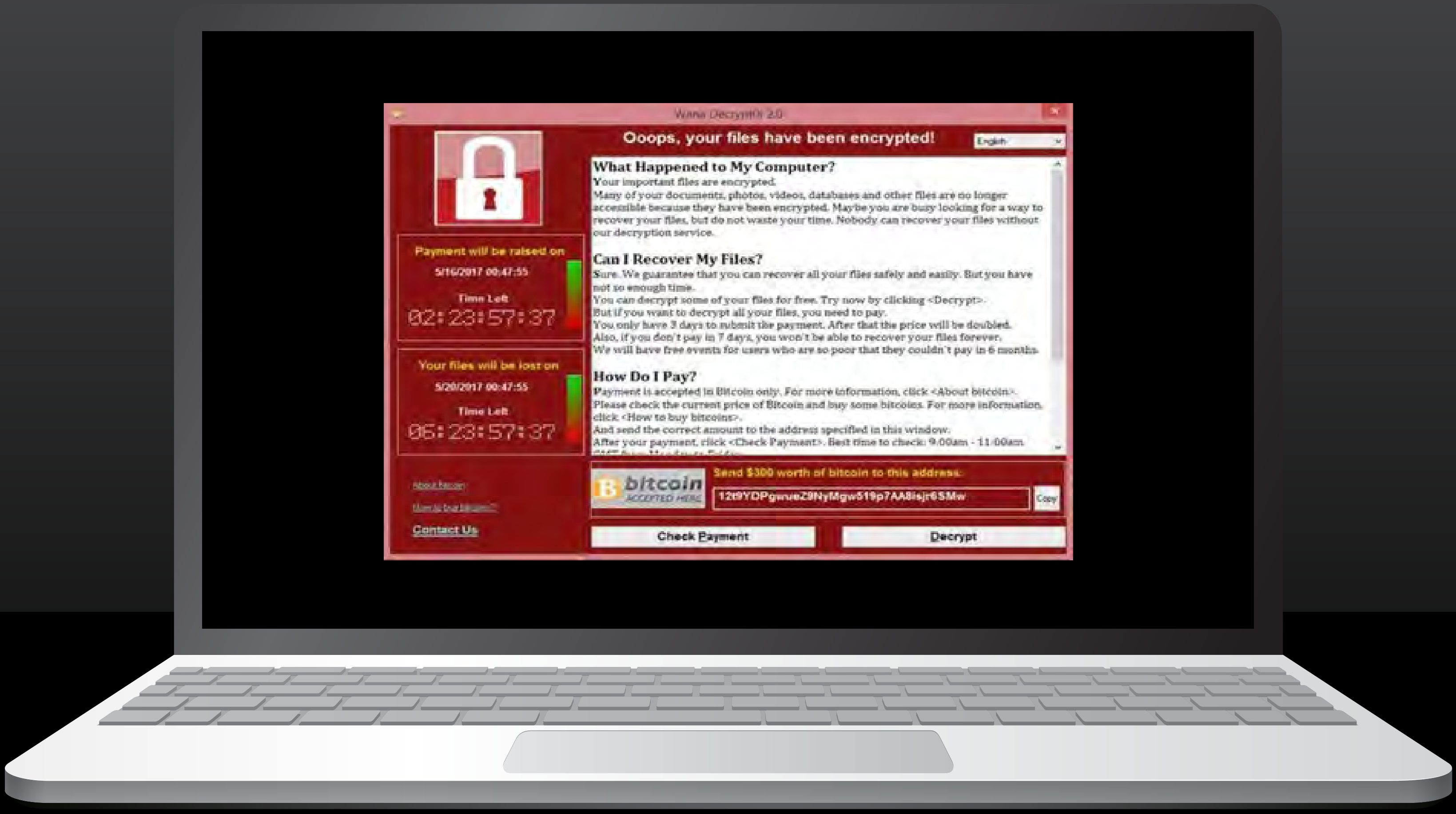
8 STEPS TO PREVENT RANSOMWARE

In recent years, ransomware has rocketed to the top of most feared attacks on an organization. Despite dozens of very high-profile ransomware outbreaks, organizations across the globe have continued to fall victim to ransomware. Some organizations refuse to pay the sometimes steep ransoms. Others capitulate to attackers' demands and pay the ransom. All of them suffer ongoing damage to their reputations. With no signs of this threat abating anytime soon, there are a number of key steps that organizations need to take in order to minimize the chances that ransomware will freeze them out of critical assets. Here is how to make your security team more effective at the job of preventing ransomware. After all, nobody wants to boot up their laptop and see this:



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

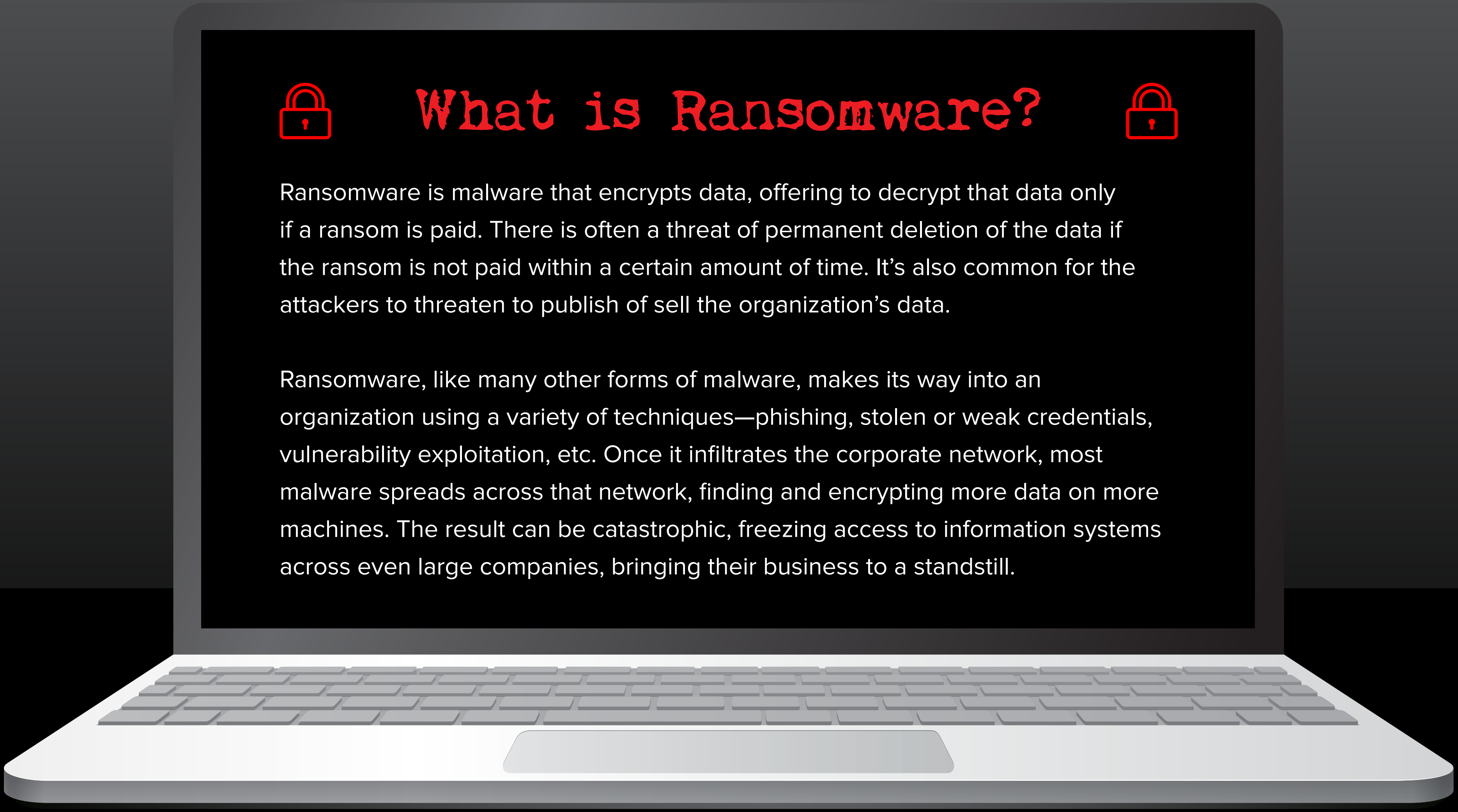
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



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.

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

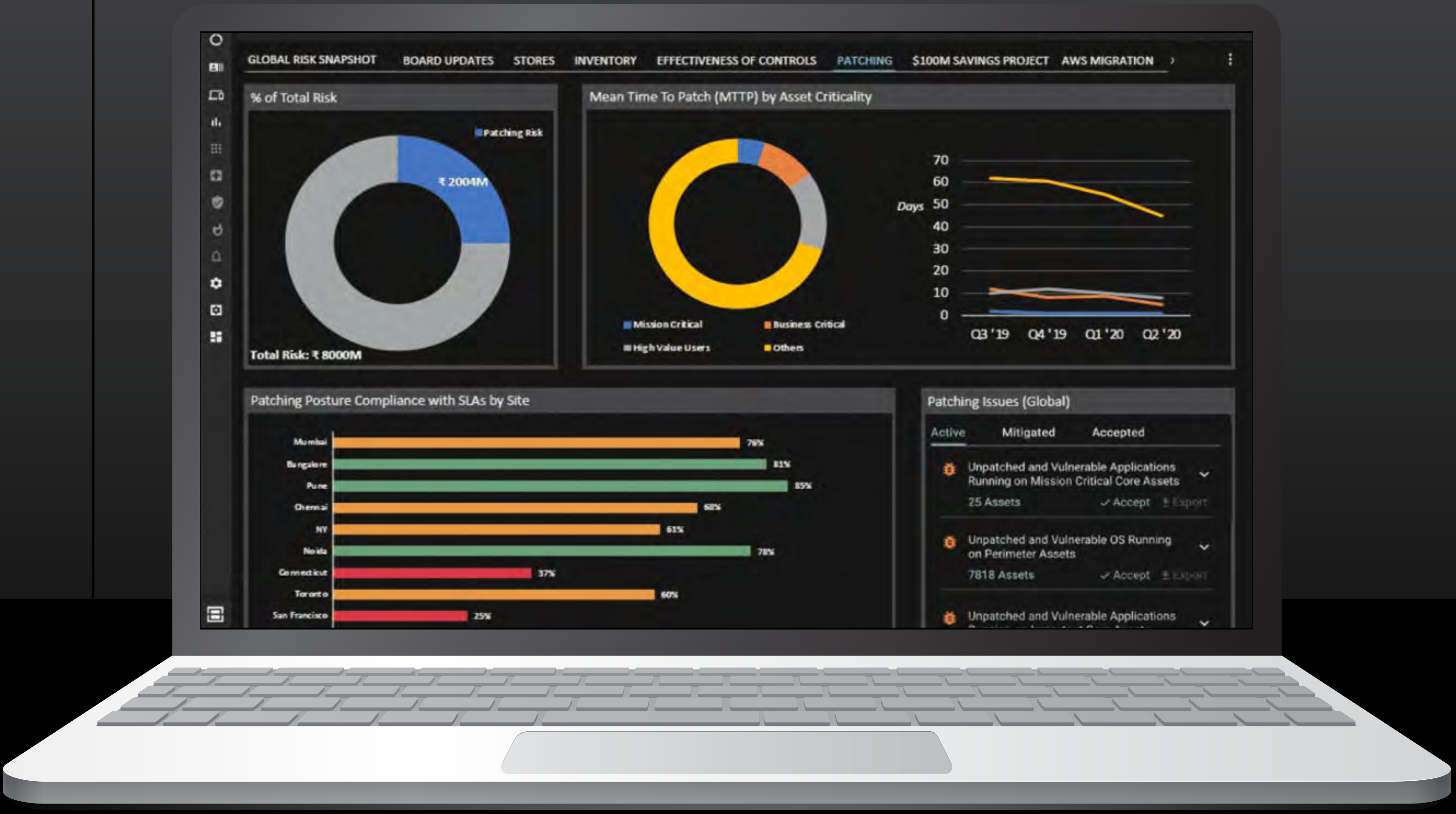
Unfortunately, there is no single silver bullet for preventing malware. As with many other forms of attacks, adversaries can exploit a single weakness anywhere to implant the malware and freeze users out of sensitive data. Here are 8 steps that your organization needs to take to help minimize the chances of malware infection.

1. **Patch** Your Enterprise Applications and Operating Systems
2. Update/Remove **Old and Obsolete Software**
3. Continuous Data **Backup** and **Restoration**
4. Disable **RDP** whenever it is possible
5. Maintain **Password** Hygine
6. **Anti-virus/Anti-Malware and Email Security Solution**
7. **Least Privilege and Network Segmentation** to control access
8. **Security Awareness Training** for all users

1. Patch Your Enterprise Applications and Operating Systems

The good news is that ransomware is like many other forms of malware is that it typically exploits known vulnerabilities. The bad news is that your patching program probably isn't as effective as you'd like it to be. Proper patching begins with an accurate inventory of all assets, including categorization and calculation of business criticality. From there, risk-based prioritization can ensure that the most important vulnerabilities are fixed first. Reporting on key metrics such as mean-time-to-patch (MTTP) can help you keep track of efforts and even introduce some gamification to pit one team against the next.

Here's a shot of a Balbix patching dashboard illustrating MTTP by asset criticality, patching compliance by site, and more.



Unpatched and Vulnerable Applications Running on Mission Critical Core Assets
25 Assets

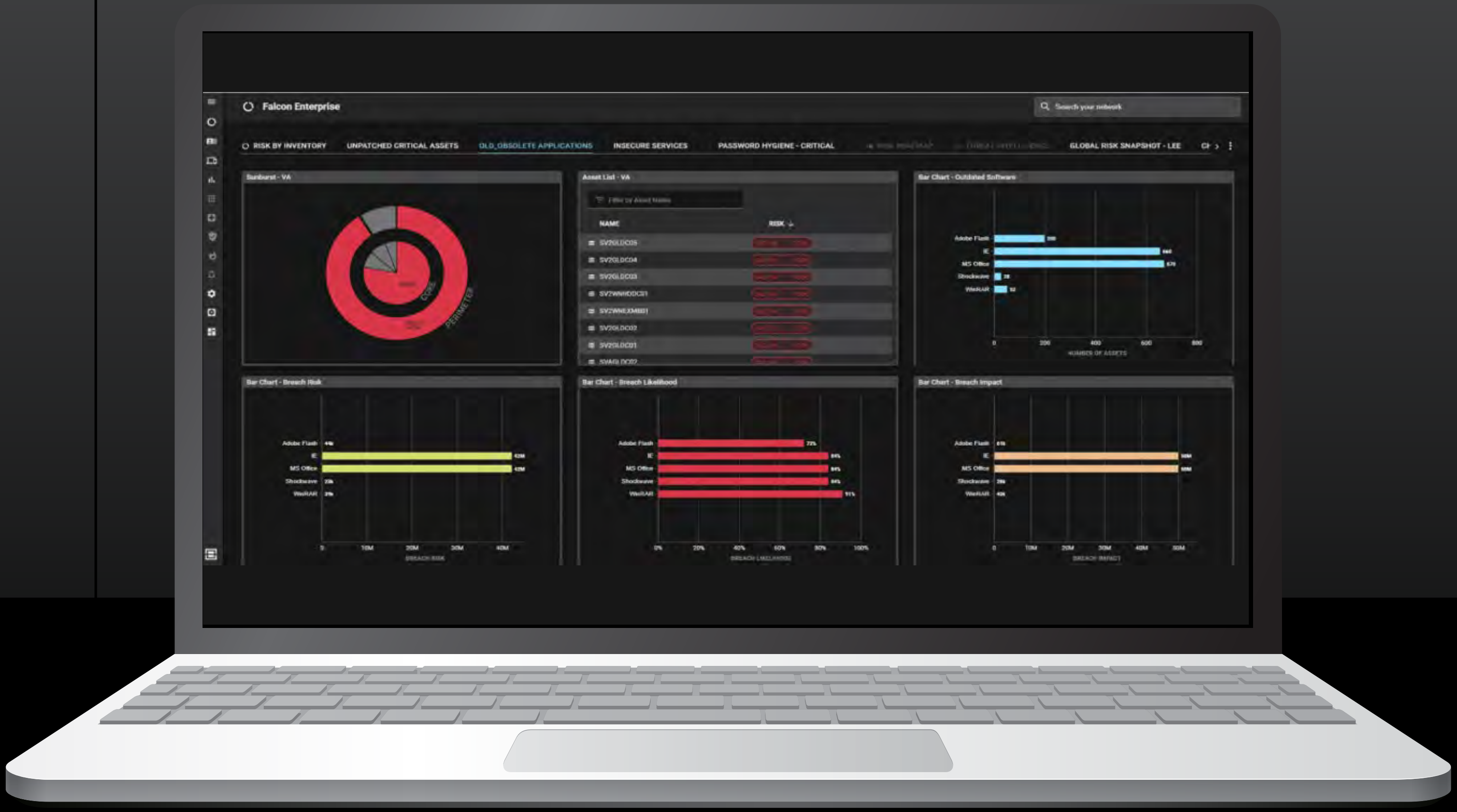
Unpatched and Vulnerable OS Running on Perimeter Assets
7818 Assets

Unpatched and Vulnerable Applications

2.
Update/Remove Old and Obsolete Software

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.

Fortunately, Balbix can help identify obsolete software so that you can remove it, or at the very least, have tough conversations with asset owners about upgrading or replacing the software.



NAME	RISK
SV20LDC05	[illegible]
SV20LDC04	[illegible]
SV20LDC03	[illegible]
SV2WNIDDC01	[illegible]
SV2WNEXMB01	[illegible]
SV20LDC02	[illegible]
SV20LDC01	[illegible]
SVAGLDC02	[illegible]

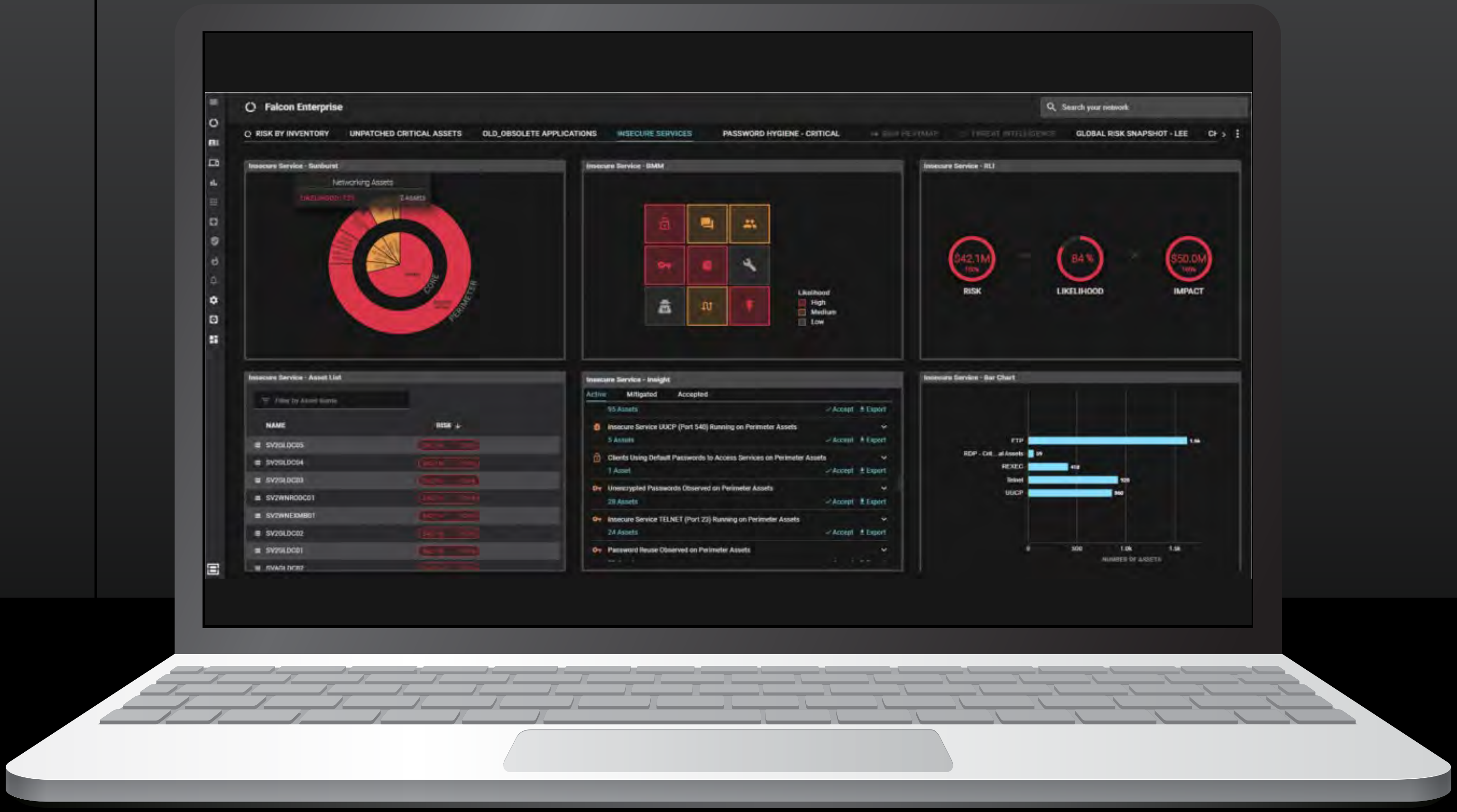
3. Continuous Data Backup and Restoration

If, despite your best efforts at prevention, ransomware were to hit your organization, ensuring that you have a strong backup and restoration process in place can ensure that you can restore data that has been encrypted, without paying the ransom. The perfect workaround! 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. 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.

As you might have guessed by now, Balbix can automate this entire process, ensuring that it doesn't become a burden on you, or anyone else in your organization:



Insecure Service - Insight

Active Mitigated Accepted

95 Assets ✓ Accept Export

Insecure Service UUCP (Port 540) Running on Perimeter Assets
5 Assets ✓ Accept Export

Clients Using Default Passwords to Access Services on Perimeter Assets
1 Asset ✓ Accept Export

Unencrypted Passwords Observed on Perimeter Assets
28 Assets ✓ Accept Export

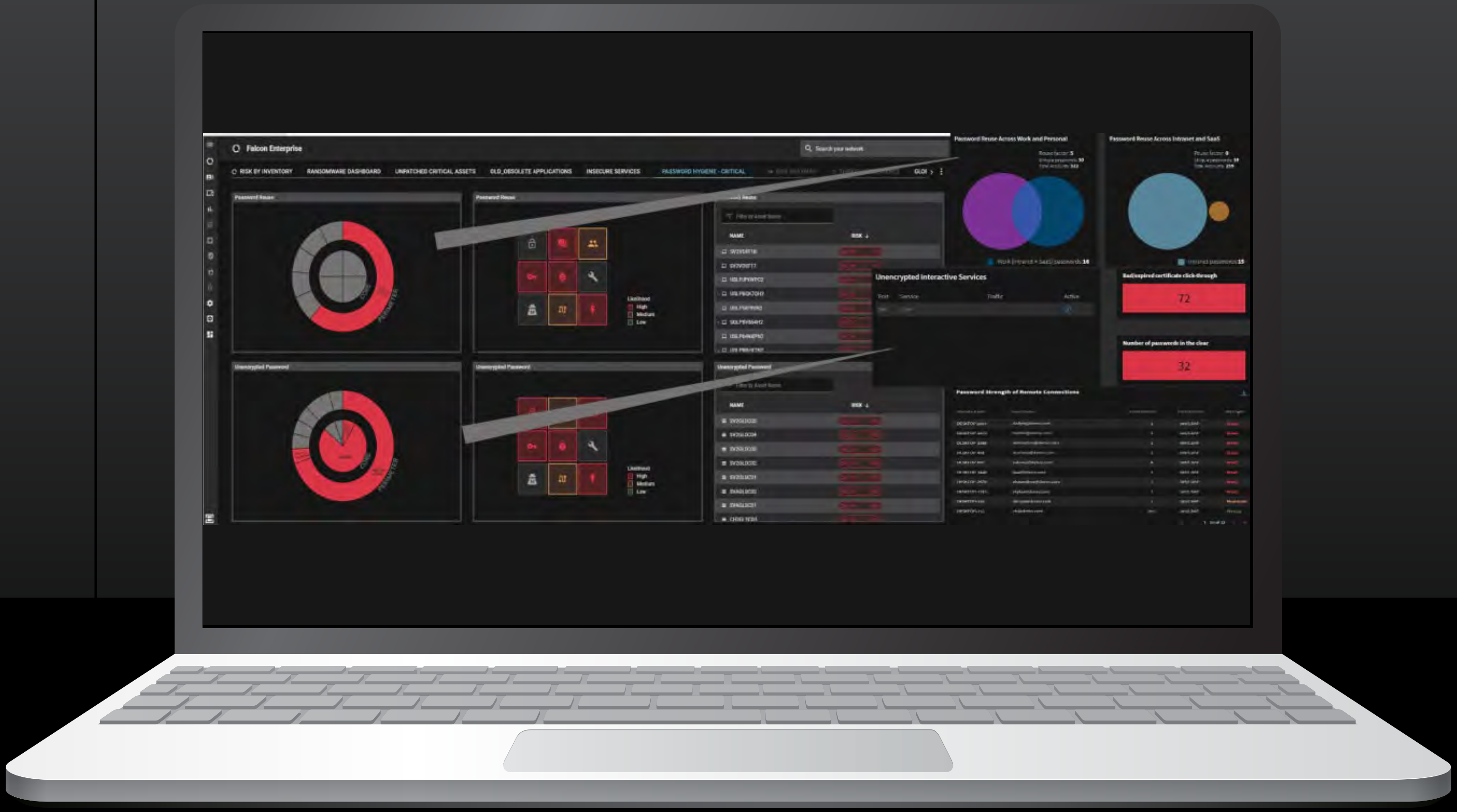
Insecure Service TELNET (Port 23) Running on Perimeter Assets
24 Assets ✓ Accept Export

Password Reuse Observed on Perimeter Assets

5. Maintain Password Hygiene

Amazingly, weak or stolen credentials are still the culprit behind 80% of enterprise breaches. And the list of password related challenges is long. Weak and default admin/system passwords. Password reuse between work and personal accounts. Unencrypted passwords. Lack of multifactor authentication. Accounts with no password or authentication. Poor password hygiene on privileged user machines.

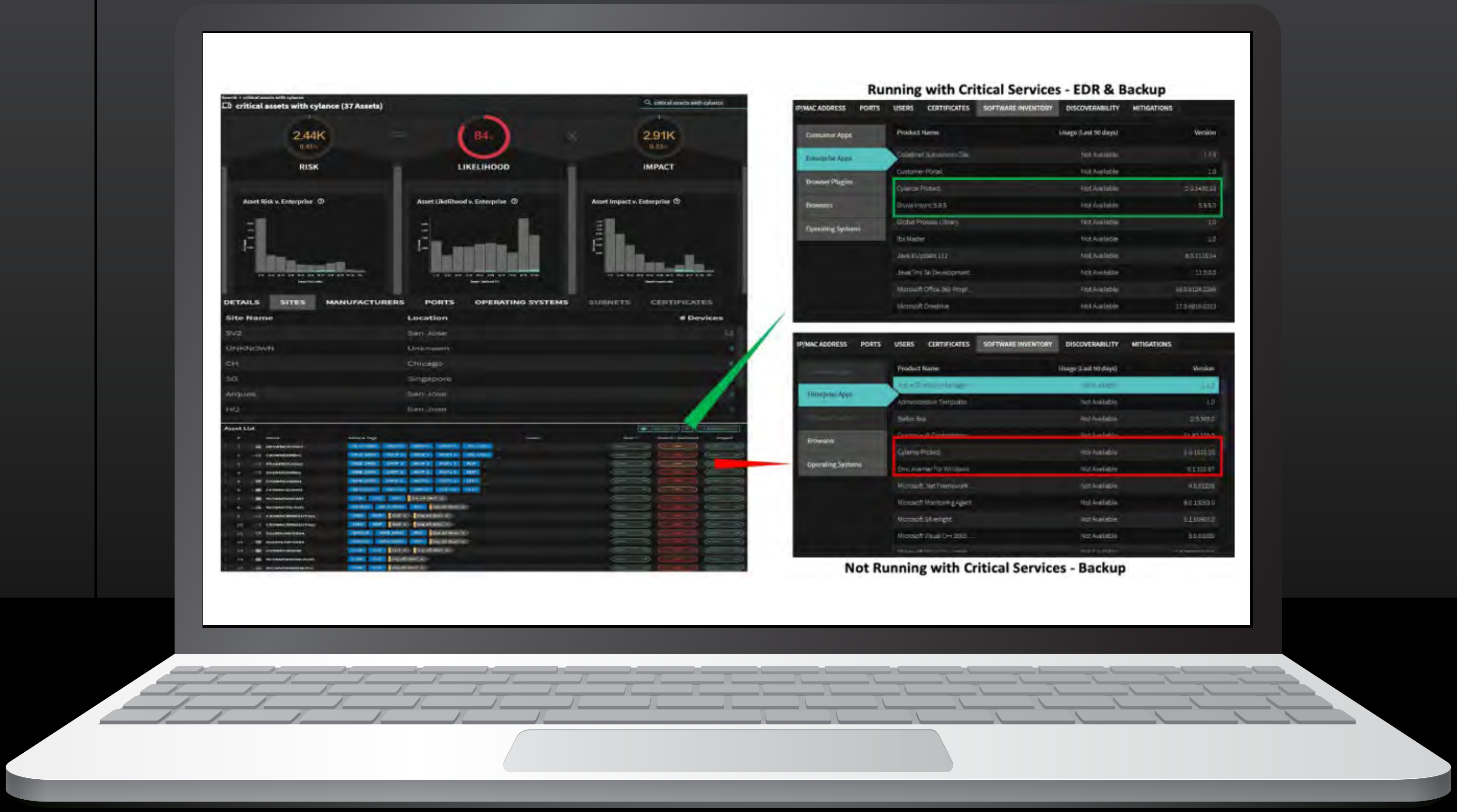
Find these issues. Eradicate them. Use Balbix.


Falcon Enterprise
Search your network
RISK BY INVENTORY
RANSOMWARE DASHBOARD
UNPATCHED CRITICAL ASSETS
OLD_OBSOLETE APPLICATIONS
INSECURE SERVICES
PASSWORD HYGIENE - CRITICAL
Password Reuse
Password Reuse
Likelihood
High
Medium
Low
NAME
RISK
Unencrypted Password
Unencrypted Password
Unencrypted Password
CORE
PERIMETER
Password Reuse Across Work and Personal
Password Reuse Across Intranet and SaaS
Unencrypted Interactive Services
Port
Service
Traffic
Active
Bad/expired certificate click-through
72
Number of passwords in the clear
32
Password Strength of Remote Connections

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.

Identifying assets not running these critical applications is quick and straightforward:.

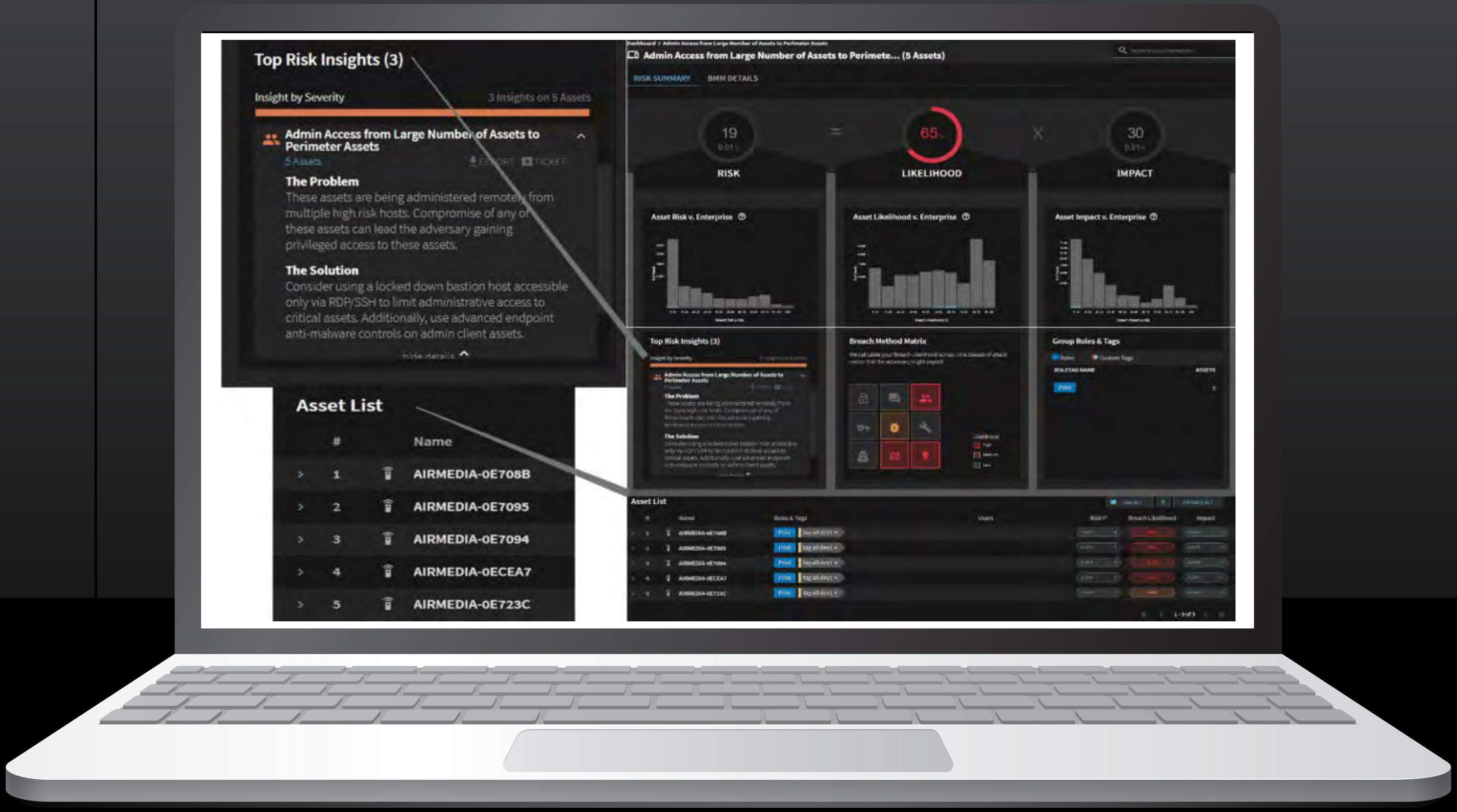


Running with Critical Services - EDR & Backup

Not Running with Critical Services - Backup

7. Control Access with Least Privilege and Email Segmentation

Too many privileges adds 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.



Top Risk Insights (3)

Insight by Severity — 3 Insights on 5 Assets

Admin Access from Large Number of Assets to Perimeter Assets
5 Assets

The Problem
These assets are being administered remotely from multiple high risk hosts. Compromise of any of these assets can lead the adversary gaining privileged access to these assets.

The Solution
Consider using a locked down bastion host accessible only via RDP/SSH to limit administrative access to critical assets. Additionally, use advanced endpoint anti-malware controls on admin client assets.

Asset List

#	Name
1	AIRMEDIA-0E708B
2	AIRMEDIA-0E7095
3	AIRMEDIA-0E7094
4	AIRMEDIA-0ECEA7
5	AIRMEDIA-0E723C

Admin Access from Large Number of Assets to Perimete... (5 Assets)

RISK 19 = LIKELIHOOD 65% X IMPACT 30

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. If any of the screenshots above seem like things that can help your organization, please don’t hesitate to reach out for a demo. One of my favorite parts of my job is demonstrating our new technology to people that have never seen it before.!

Request a demo today to learn more about these and other capabilities in the Balbix platform.

LEARN MORE

Balbix®