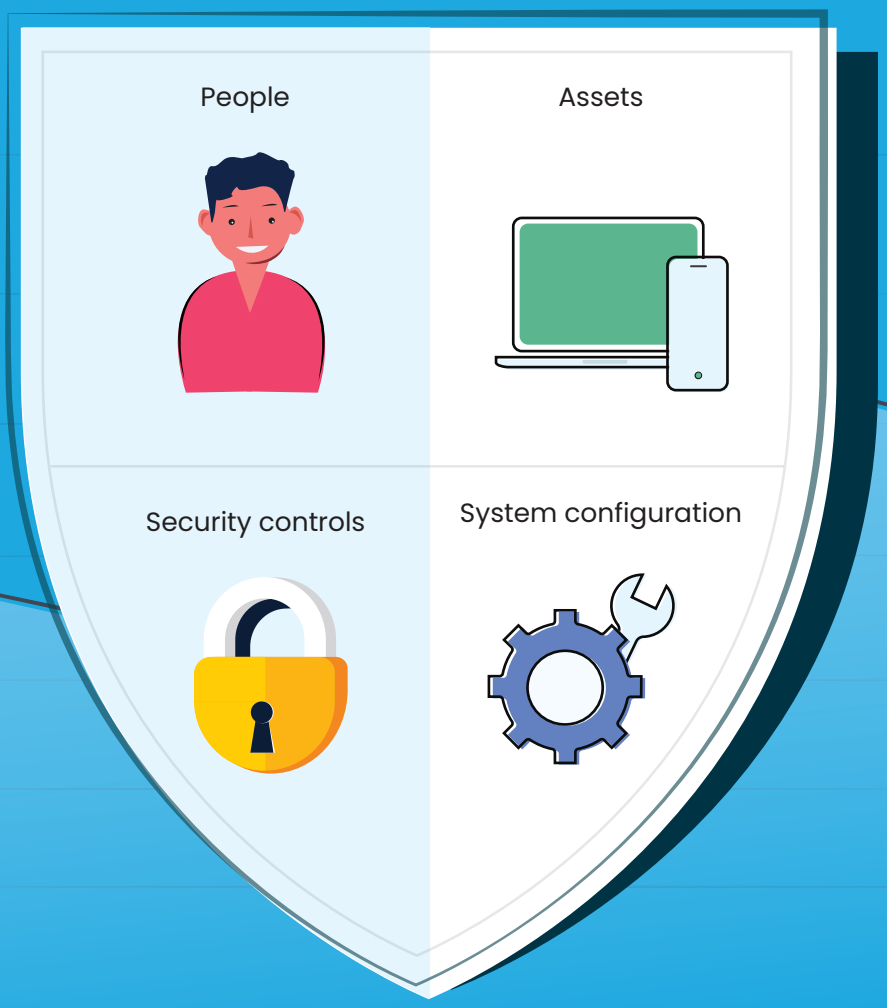
Leverage analytics to track the **4 essential pillars of IT security**



ManageEngine Analytics Plus

Leverage analytics to track the 4 essential pillars of IT security

Enterprise security is an uphill battle. For one, you're dealing with an ever-changing and ever-expanding security landscape, and two, you're fending off several internal and external threats all at once. In simpler terms, you need to win every day, whereas the bad guys need to win just once. This e-book provides a few useful suggestions that can help you strengthen your organization's data security.

Table of contents

Introduction

Gartner[1] hints that information security spend is at

$123 billion

Despite enterprises shelling out billions for IT security, 100 percent security is still an elusive dream for most of them. The reason is that traditional security measures no longer cut it. For instance, firewalls and spyware are no longer sufficient to ensure complete data security because they operate under the belief that an organization's IT department has complete visibility into its endpoints—desktops, laptops, handheld devices, etc. However, that is no longer the case. The explosion of endpoint usage due to a hybrid work culture, along with indiscriminate user behavior stemming from both benign and malicious intent, has made it difficult for IT departments to secure enterprise data.

Looking at the current security landscape, a report on **endpoint security trends**[2] suggests that 70 percent of all security threats originate from endpoints, with 35 percent of those threats arising from existing vulnerabilities. Here's some food for thought: In 2019, organizations around the world witnessed an astounding 80,000 cyberattacks per day; that's over 30 million attacks per year.

With operational challenges adding layers of complexity in ensuring data security, and the current threat landscape posing an alarming range of threats, complete visibility into endpoints is the only solution that can help IT departments secure their organization from internal and external threats. Because the IT landscape is too vast, we've made it simpler by splitting the entire IT landscape into four easily-trackable components—people, assets, security controls, and system configurations. Secure these four pillars, and you can easily ensure 100 percent data security for your organization.

Chapter 1: People

Security breaches are a costly affair for any organization, particularly when they come from insiders. Here are some stats:

The **average cost**[3] of a generic security breach is

$3.6 million

while the cost of an insider security breach is an astounding

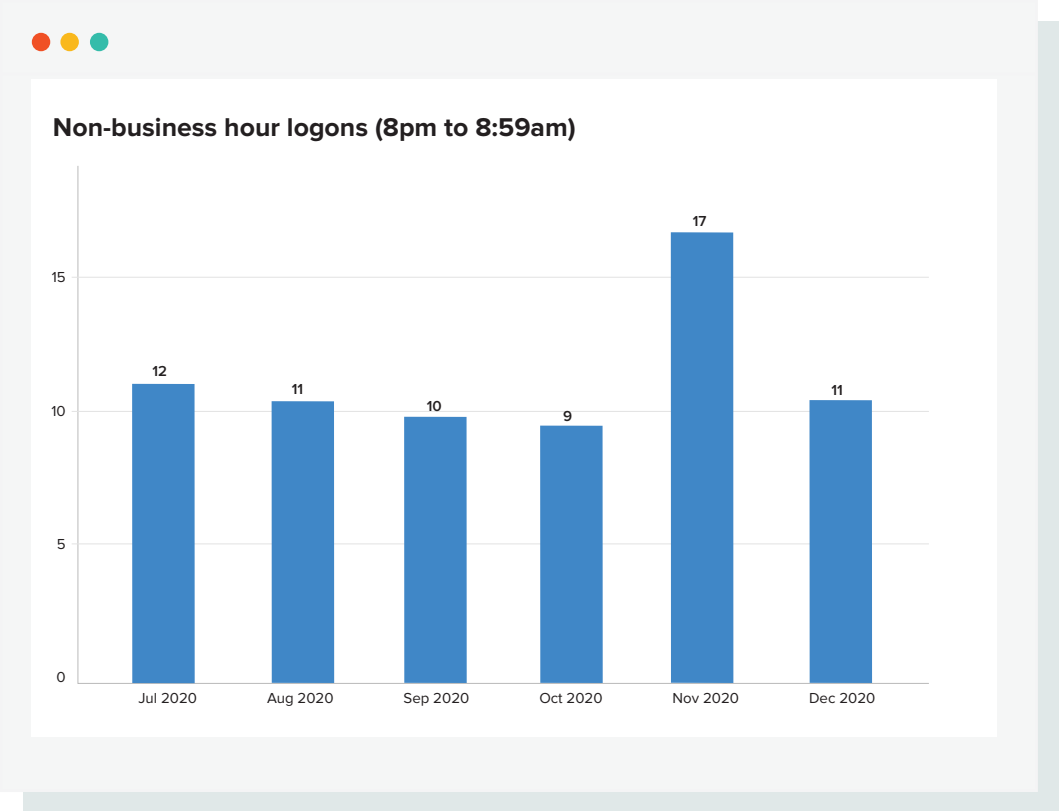
$11.5 million

That's almost three times the average cost of a generic security threat, proving that data loss due to insider threats is far more expensive to organizations compared to outsider-executed security threats. This is because insiders already have firsthand knowledge of where and how you store your valuable data, and have full access to it. Whether insider threats are attributed to negligence or malicious intent, from an organization's standpoint it's advisable to take the obvious protection and prevention steps, and put forth the strongest security stance.

To secure your data from insiders, start with these three steps:

1. Analyze user behavior

An effective way to combat insider security threat is to begin baselining normal user behavior to identify outliers in logon hours, logon duration, network traffic, systems accessed, etc. Interestingly enough, this is also one of the easiest and most obvious ways you can catch malicious activities in your networks. For example, a regular nine-to-fiver logging on to your systems remotely at 2am on a Sunday is a serious red flag in user behavior.



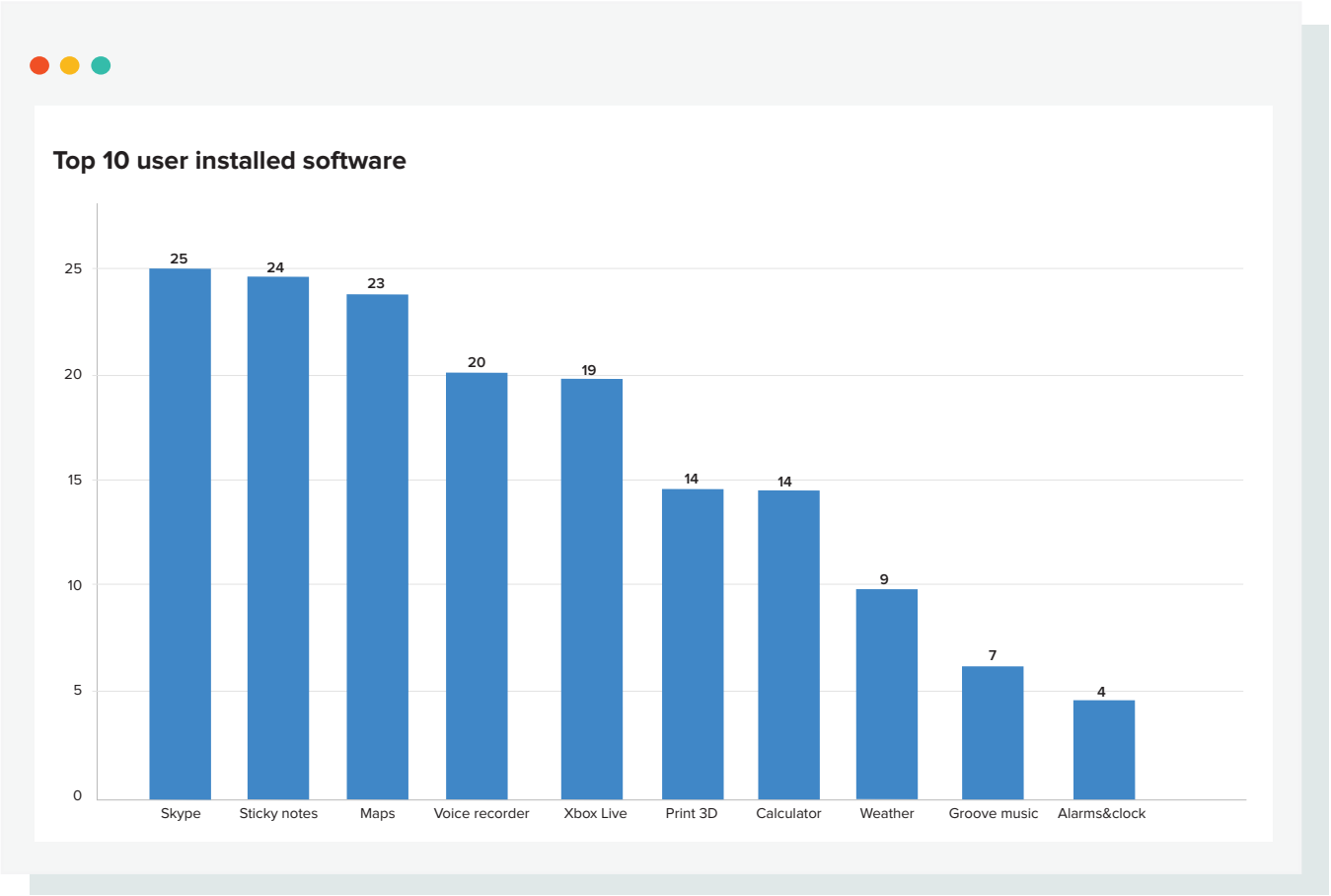
The report above shows the list of users who have logged on to your systems during non-business hours. Typically, not all off-hour logons can be classified as a security hazard, as they could be due to several reasons such as users extending work hours or logging on early to compensate for lost work hours. However, from a security standpoint, it's always necessary to track such deviations from normal behavior.

Malicious insiders with intent to steal data from the organization usually do so in short but frequent spurts. Tracking the total hours users have logged on to shared accounts will help you spot such behavior easily.

From the report above, it's clear that one of my users accounts, Mdm-345, has recorded the maximum logon hours, a noticeable 30 percent more than the others. Further analysis as to why this user account has witnessed extended logon hours will reveal if this is a result of extra work done by the user or an act done with malicious intent.

2. Set a cap on user-installed software

While corporate-owned laptops and mobiles give users the freedom to work from anywhere, anytime, they also bring many security challenges, such as the use of personal or entertainment applications that require access to photos, files, or documents stored in those devices, i.e., Netflix or Amazon Prime on mobile devices, or VLC media player on laptops. While it's not feasible to ban all personal applications, it definitely helps to monitor and set a cap on the number and type of user-installed software.



The report above shows the top 10 applications installed by users on their corporate devices. While the top three most-installed applications are Skype, Sticky notes, and Maps, you can also see several users have installed Xbox on their corporate devices. Since this application is not directly related to work and tends to take up a lot of disk space, security personnel can reach out to users and ask them to remove these apps from their devices.

3. Educate users on security threats

When it comes to data security, there's nothing as powerful as a well-informed and security-aware user—one that truly understands their contributions in keeping the organization's data safe from prying hands. User awareness doesn't even have to be anything extravagant; simple actions such as refraining from clicking untrusted links, opening emails marked as spam by the security team, or downloading files without scanning them first can go a long way in ensuring you remain protected against phishing, ransomware, spyware, and other threats.

Another way users can help ensure data security is by using strong passwords. People using obvious passcodes such as 0000, 123456, Baseball123, or Password123 has become common practice. This may be because users are mandated to change passcodes frequently; also, users have simply too many accounts or systems that require passcodes. However, passwords are still a great way to protect your accounts and keep them safe. A report like the one shown below gives you an organization-wide view of the passcode compliance status of various devices in use.

While strong passwords alone don't guarantee security, organizations can bolster their security further using multi-factor authentication (MFA). With so many applications and devices fully equipped to support MFA effortlessly on the market, there's no reason for organizations not to use them.

Chapter 2: Assets

Assets owned by an organization can be broadly classified into four categories: hardware assets, software assets, cloud assets, and endpoints, which include all handheld devices like mobile phones, tablets, etc. While the responsibility of ensuring the security of cloud assets can be relegated to the concerned cloud server provider such as platform as a service (PaaS), software as a service (SaaS), or infrastructure as a service (IaaS), the responsibility of ensuring the security of the other three classes of assets falls entirely on the IT and security teams. Organizations should keep in mind that this classification also includes corporate-owned and personal or bring your own devices (BYOD), which is significant particularly in the face of growing inclination from people across all industry verticals towards remote work.

The only way to traverse this diverse and sometimes even confusing IT asset landscape is to ensure you have a solid inventory of all your assets. For example, if you have a PC, you should have the following details in your asset inventory: asset type, user(s), physical location, location in the network, software installed, and patches installed. This will provide real-time visibility into each of your systems, and enable you to envision vulnerabilities present in them. It will also help you trace data movement to and from the system, facilitating faster threat detection.

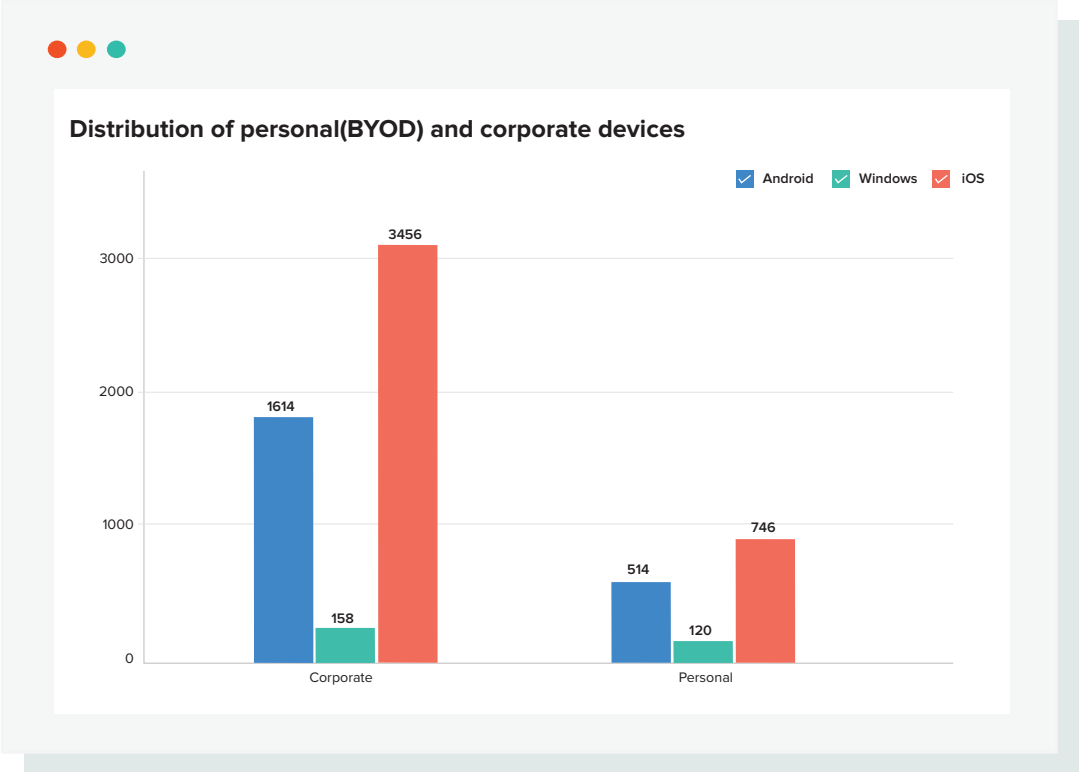
However, having the grid-view of system details in your inventory alone isn't enough to ensure cybersecurity; it's important to assess the details as well so you can identify threats and risks in real time.

To help you leverage your inventory data to identify vulnerabilities successfully and ensure complete data security, we've laid out a list of best practices that can be adopted by your security teams:

1. Always know what you have in your arsenal

The downside to hybrid work culture is the rampant use of both corporate and BYOD devices for work. Corporate-owned devices follow standard naming conventions and have built-in security protocols, such as authentication mechanisms, to connect to secure networks and applications. However, BYOD devices don't have these authentication protocols, but are fully capable of accessing secure data by logging in to virtual private networks (VPN) or Microsoft Remote Desktop Protocol (RDP). These devices also have haphazard naming conventions that make it difficult for the security team to trace the user or owner.

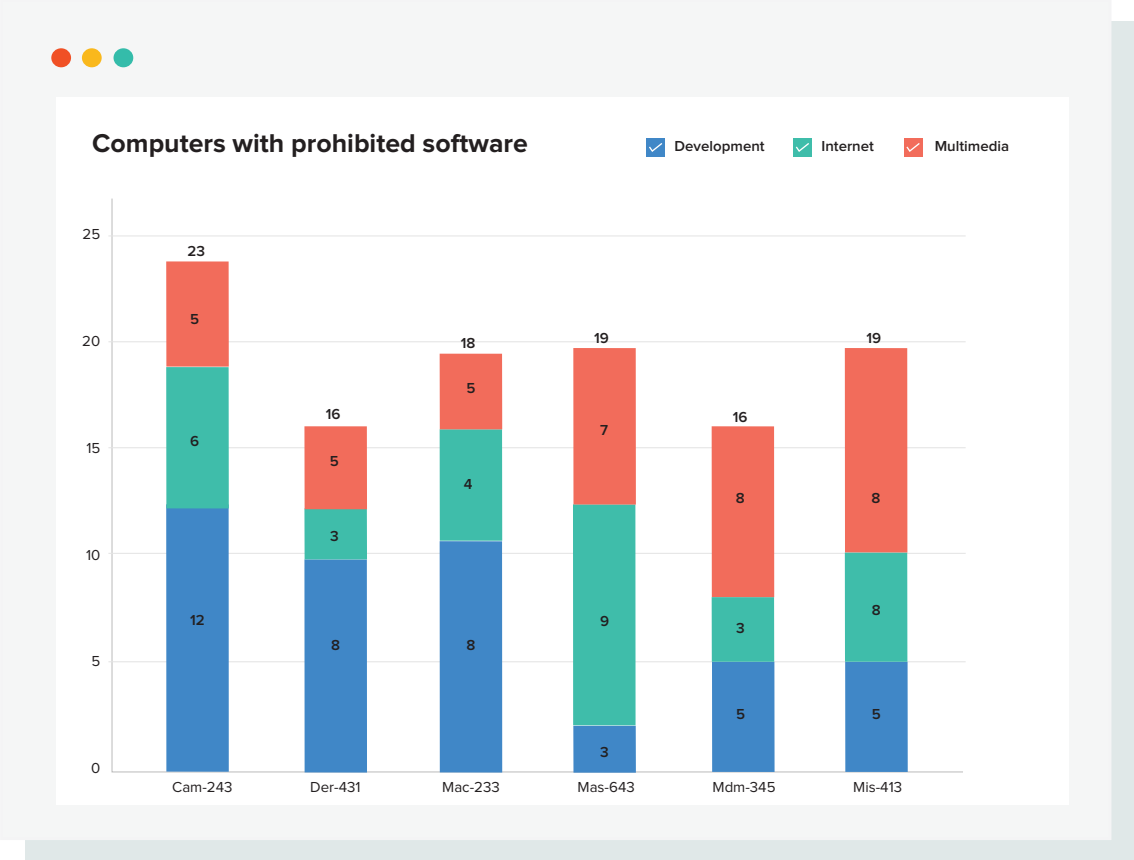
The report below gives you a clear idea of the split between corporate-owned and personal devices in use, along with their operating systems.



Once you know how many assets there are in your arsenal, the next step is to pin them down by their geographical location. The spatial location view of assets used by the people in your organization makes it easier to raise an alarm when a device moves out of its designated area. This enables you to lock down the device remotely, or selectively delete all the corporate data present in the device in case of a security emergency. Report done already

2. Monitor software installed in endpoints

Security teams always walk the tightrope between security and usability when it comes to applications installed in endpoints. While marking software as blacklisted or prohibited sets clear expectations for users on what they can and can't use, users often feel restricted given the limited number of applications. However, from the organization's standpoint, it's important to prioritize data security and productivity, and restrict applications that might risk the organization's security stance or hamper user productivity.

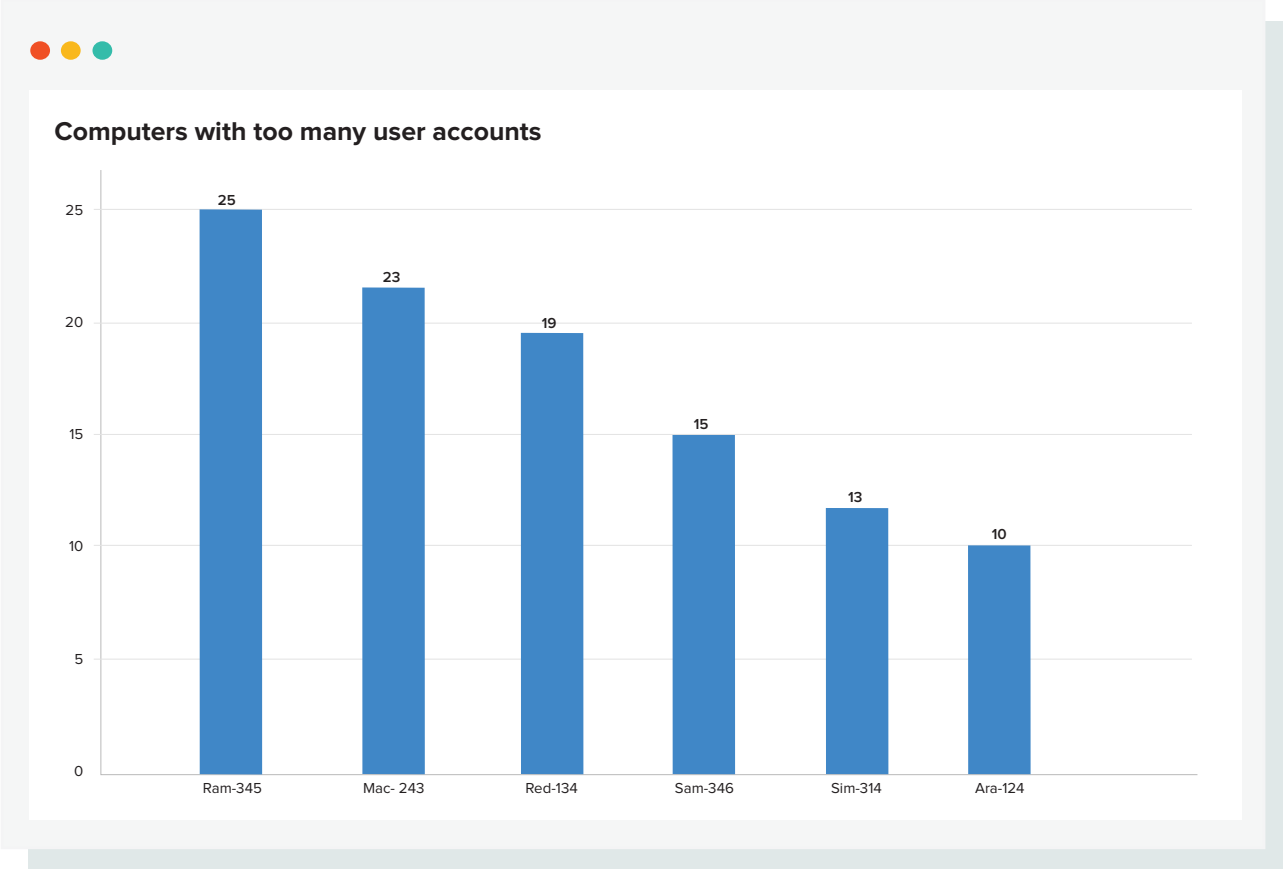


The report above gives you an overview of the different endpoints in your organization that contain blacklisted or prohibited applications. The graph also shows the distribution of these prohibited applications by category, such as software used for development, entertainment (multimedia), and browsers. With this information, security teams can take measures to remove prohibited software from these computers.

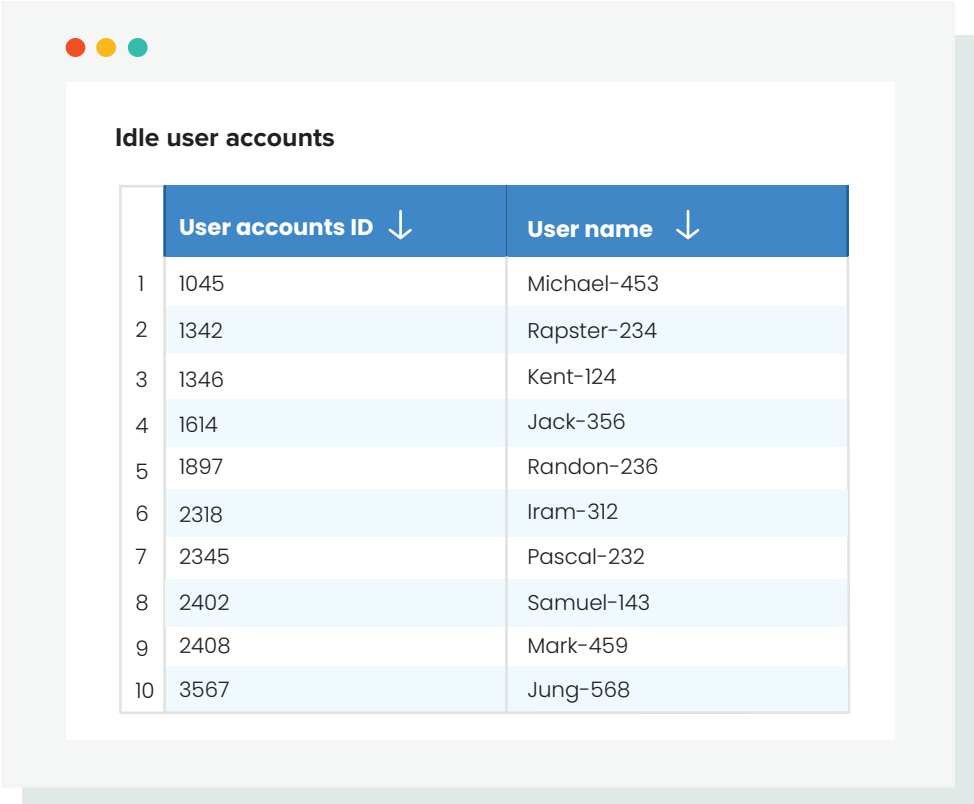
3. Keep an eye on shared systems and their users

Ask anyone in DevOps or testing teams, and they'll tell you shared systems are a godsend. Shared systems allow several users to collaborate and work collectively on important activities that often can't be performed on individual systems, or require advanced tools and technologies that aren't readily available in their own systems. However, shared systems also pose major security threats because many people have access credentials to these systems. Also, most of them tend to share their access credentials with others in the organization, further broadening the access range of these systems. This is not limited to people in DevOps or testing teams; people from a variety of departments such as HR, legal, IT, finance, and even administration are guilty of sharing access credentials with other users in the organization.

The problem with having too many users in shared systems is that even if a single account is compromised, it opens up the gateway to the organization's secure network and applications. What makes this a serious threat is that not many organizations can visualize the extent to which such a security threat can impact the organization. Here's a report that shows you systems that have 10 or more user accounts.



From the report, it's easy to see that there are several systems that have 20 or more users. Security teams can consider limiting the number of users accounts to ten, and commission more shared systems for the remaining users. Alternately, they can run a quick audit on user accounts that are inactive and remove them. Here's a pivot table that shows inactive users accounts that haven't been logged into in over 90 days.



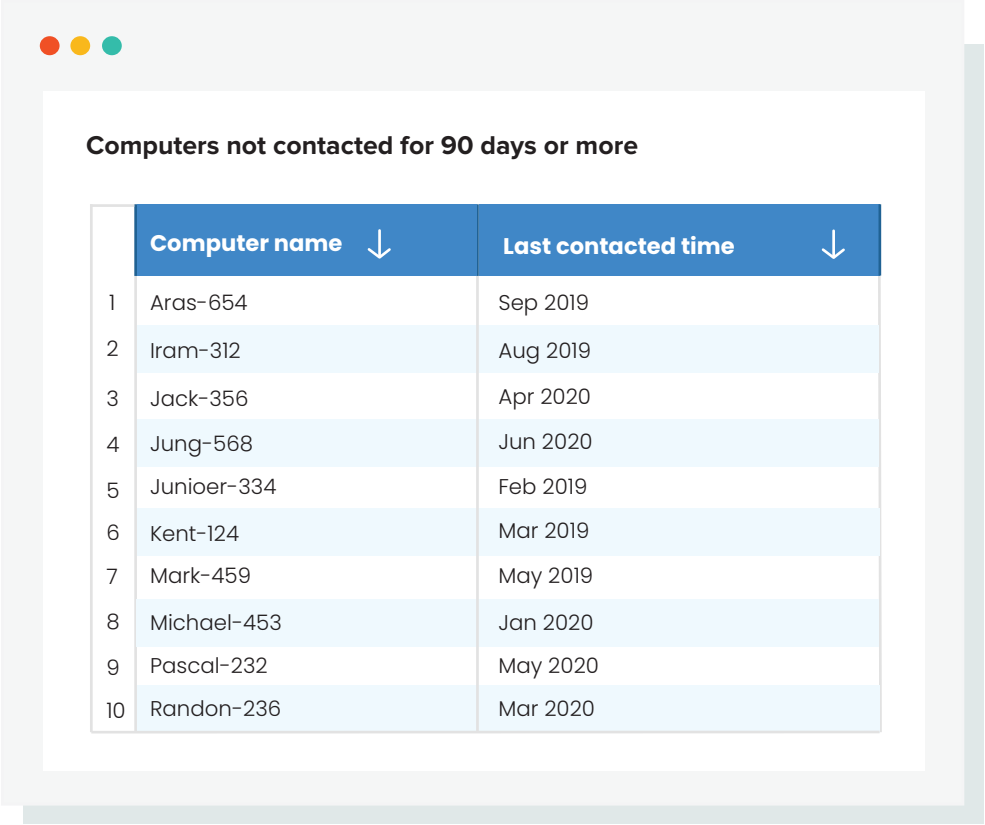
Idle user accounts

	User accounts ID	User name
1	1045	Michael-453
2	1342	Rapster-234
3	1346	Kent-124
4	1614	Jack-356
5	1897	Randon-236
6	2318	Iram-312
7	2345	Pascal-232
8	2402	Samuel-143
9	2408	Mark-459
10	3567	Jung-568

From the report, you can see that there are several inactive user accounts which can be revoked to free up the computer for use by other active users.

4. Ensure systems are in frequent contact with your endpoint management server

Endpoint management applications like Desktop Central are attuned to be in contact with the endpoint infrastructure regardless of their geography. In situations when computers lose contact with the Desktop Central server for prolonged periods of time, security staff may not be able to remote in to the computers to address security breaches. Additionally, the loss of contact for prolonged periods means systems will not receive periodic updates or patches, leaving them vulnerable to security threats.



Computers not contacted for 90 days or more

	Computer name	Last contacted time
1	Aras-654	Sep 2019
2	Iram-312	Aug 2019
3	Jack-356	Apr 2020
4	Jung-568	Jun 2020
5	Junioer-334	Feb 2019
6	Kent-124	Mar 2019
7	Mark-459	May 2019
8	Michael-453	Jan 2020
9	Pascal-232	May 2020
10	Randon-236	Mar 2020

The pivot report given above lists the computers that haven't contacted the Desktop Central server in the last 90 days. The next step is to check if the computers are available in the network, if the device owner is traveling with the device, if the name of the computer was modified, or if the computer no longer exists, and then take remedial measures to secure non-communicating devices.

Chapter 3: Security controls

It's no secret that cyberattacks are on the rise; what's alarming is the frequency, sophistication, and the dynamic nature with which these attacks occur. Experts cite technology disruption as one of the biggest known threats to cybersecurity. Constantly evolving technology requires organizations to quickly update their hardware and software to keep with the changes, greatly disturbing the multilayer security blanket put up by the security teams to protect organizations from internal and external threats.

In the last quarter of 2018:

British Airways (BA)[4] fell prey to a 15-day security breach where the personal and financial information of

380,000
passengers was stolen

Though the airline was able to discover the breach, it was unable to discover the specifics that led to the breach. It wasn't until much later that security expert **Yonathan Klijnsma**[5] discovered its source. Apparently, the security scripts for its baggage claim information page were changed just before the attack started. The hackers exploited a weakness hidden in the script to steal valuable information that cascaded into a huge problem, affecting several other organizations in the process. **UK-based online bank**[6] Monzo had to reach out to several of its customers affected by the breach to cancel their existing cards, and issue new ones to safeguard their accounts.

The threat landscape today is rampant with such examples, where changes in existing processes or systems have compromised the overall security of the organization. A practical defense mechanism against such threats is to stay vigilant and look out for early warning signs of threats. Deep analysis of data from endpoint management systems can provide vital clues into threats and vulnerabilities. Security personnel can then use these clues to investigate further, and assess the validity of these threat indicators.

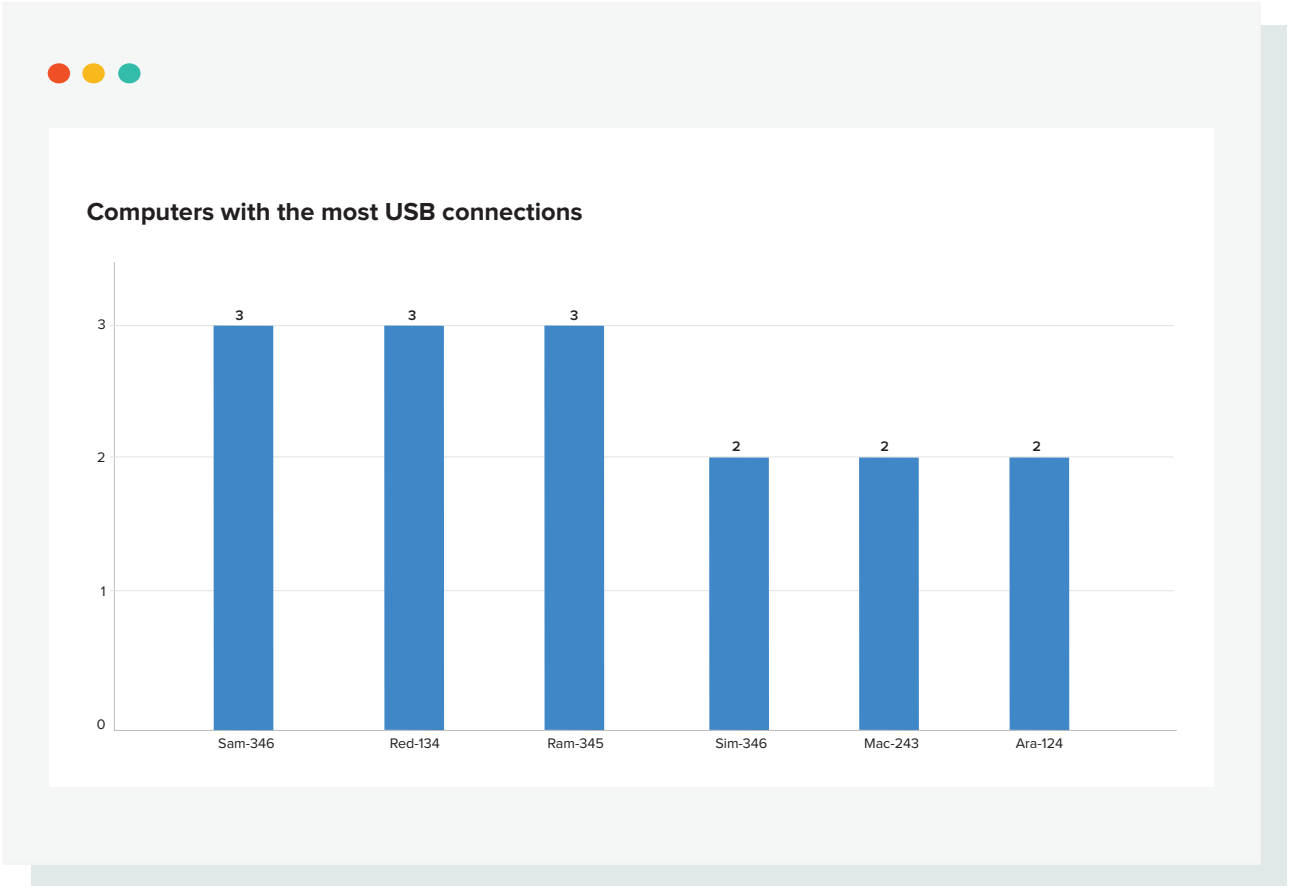
An essential factor that most organizations and even security personnel tend to forget is that these hackers, attackers, or any sort of threat agents are powerless in the absence of loopholes within the organization's security posture. Except for perimeter attacks such as SQL injections, most security threats can be detected by following a few security control measures such as the ones given below:

1. Look out for rogue IoT devices

What do you know about Raspberry Pi? What about BeagleBone? **Raspberry Pi**[7] is a tiny, affordable, single-board computer that fits in your pocket, but can perform complex tasks ranging from playing chess to building a model of an international space station. Similar to the Raspberry Pi, the **BeagleBone**[8] is a also high-performance, low-power, single-board computer that's powered by an open-source Linux operating system. These devices put the power of a complete computer in the hands of its users—proof of astounding leaps in technology. If you're a security personnel, by now you're already worried about how this device can hamper your organization's data security. These palm-sized, single-board computers fall under the broad spectrum of Internet of Things (IoT) devices that can be connected to any endpoint using USB ports.

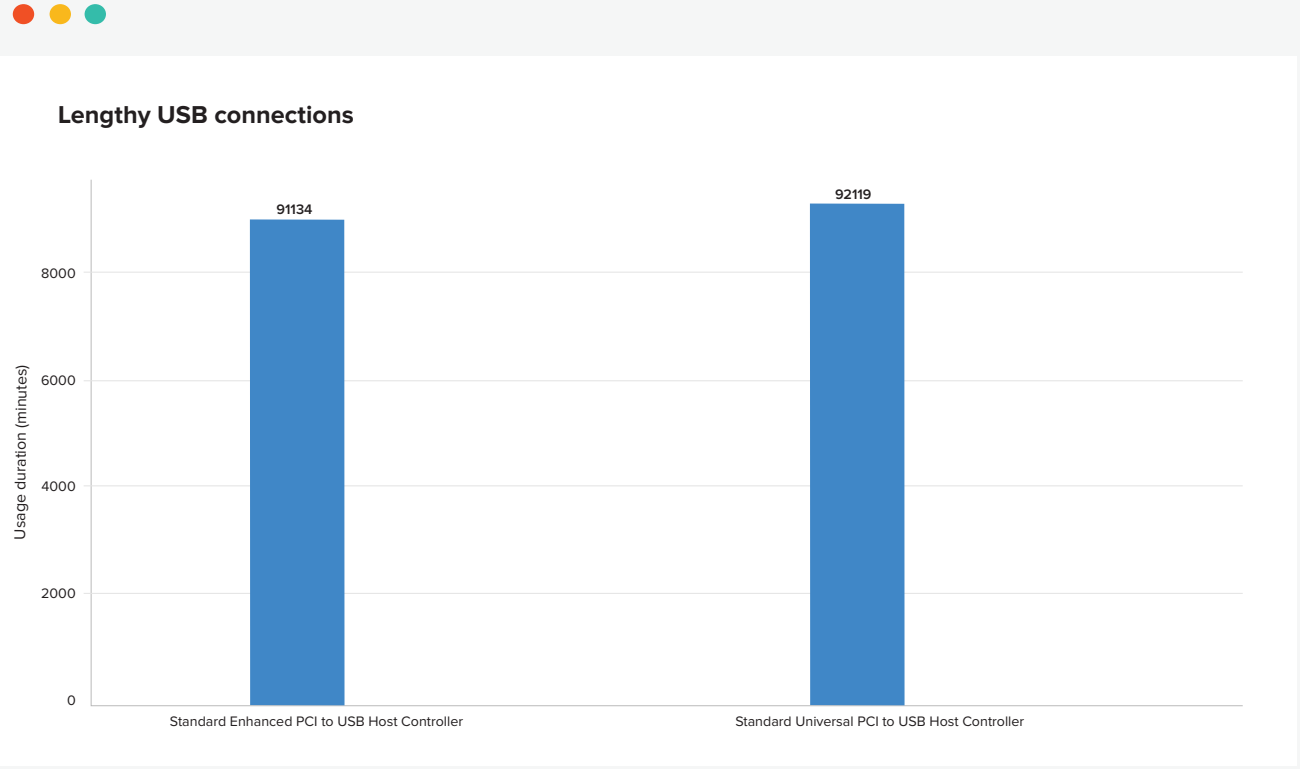
What makes these tiny devices lethal is that they aren't confined within the orgnanization's security measures, and they don't follow any standard naming protocols. These devices are also programmed to learn about their environments via multicast, which means they constantly learn and adapt, making them deadly to the organization's security.

While there may not be many ways to catch these devices hiding in your systems yet, you can prevent their entry into your secure network. Audit the history of peripheral devices accessed by users, in this case USB ports, and look into the number and duration of USB connectivity. This will easily pinpoint threat actors hiding with your systems.



The report above shows computers with the most number of USB connections. It's not necessary to flag computers with too many USB connections as a security hazard yet, but it is good to have an idea of the actual number of USB connections.

The next step is to look into the duration of these connections.

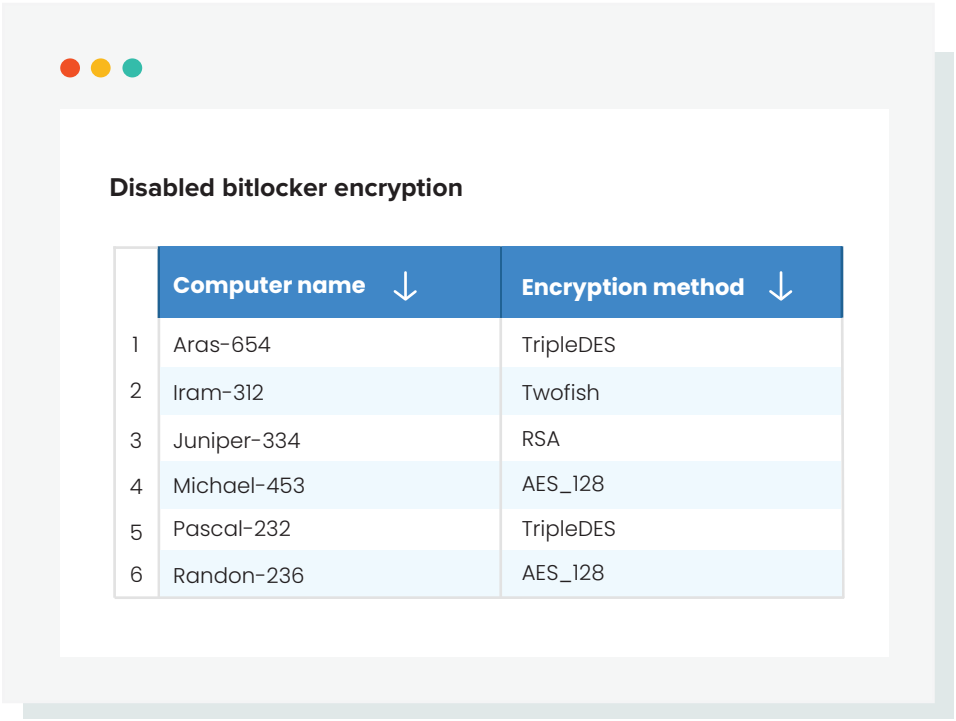


In the report, for the purpose of this investigation, I've filtered out the results for the computers that have recorded the most USB connections in the earlier report. That leaves me with two USB devices that have been connected for over 90,000 minutes; that is, 1,500 hours. The next step is to check in with the device owners, and figure out the reasons for such lengthy USB connections.

2. Spot and remove threat actors

While it's important to trust your employees, it's also important to keep on eye on their activities to be able to spot bizarre behavior such as removal of security encryption. Windows Encrypting File System (EFS), such as BitLocker, enables organizations to protect confidential data from attackers by encoding logical drives. Once the BitLocker encryption is enabled for a drive, any file(s) moved into the folders within that drive will be automatically encrypted. This ensures complete data security for the files and feeds stored in computers in the event of a breach.

The report below shows the list of computers that have disabled the BitLocker encryption.



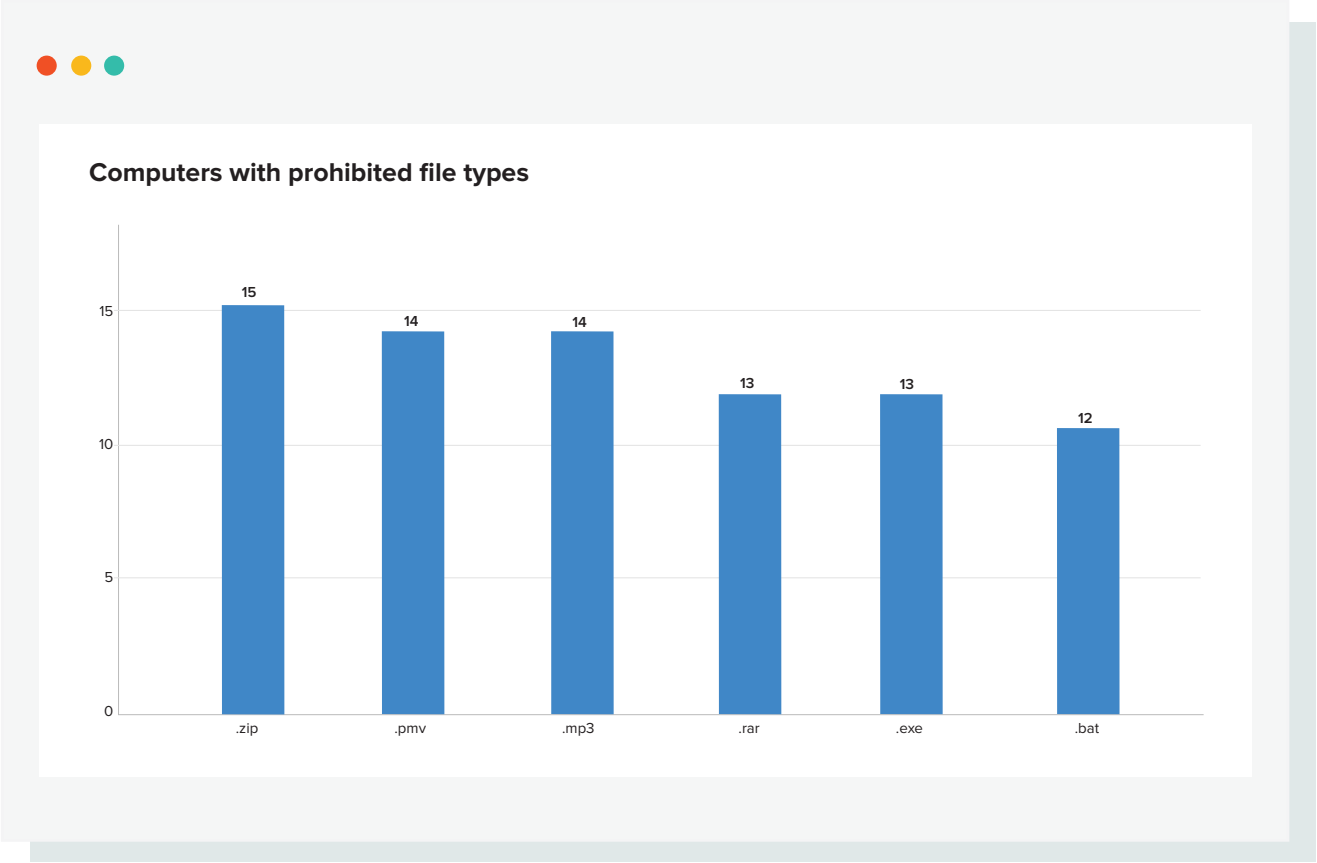
Disabled bitlocker encryption

	Computer name	Encryption method
1	Aras-654	TripleDES
2	Iram-312	Twofish
3	Juniper-334	RSA
4	Michael-453	AES_128
5	Pascal-232	TripleDES
6	Randon-236	AES_128

While some users might want to disable encryption temporarily in order to decrypt the files in their drives, it's important for the organization to ensure security encryption is always on so data loss can be prevented in case of a security threat.

3. Stop data from leaving your systems

The key to preventing data loss from internal systems is to put up barriers that prevent it from ever leaving your secure networks. A typical behavior pattern of malicious insider behavior is siphoning off data in smaller packets stored in ZIP or RAR files. Complete visibility into data movement of such files is a surefire way to catch users in the act.



The report above shows the various file extensions and the number of computers with such files. You can see there are only a few users with RAR or ZIP files, which is perfectly normal for any organization. However, it would help to add this report to the security watch list to see if there's any change in this number, and reach out to the users in case of sudden spikes.

Chapter 3: System configuration

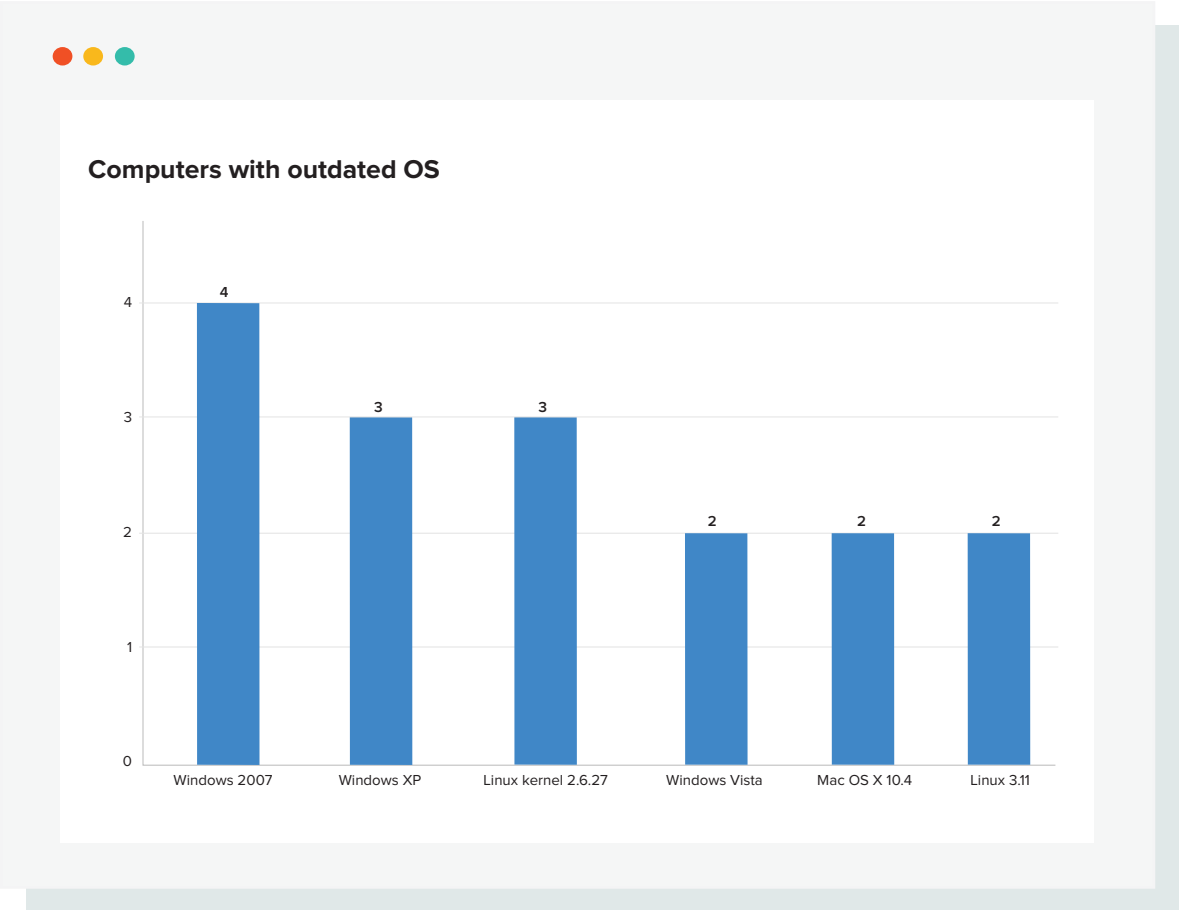
Imagine this: You have a Windows system running on an older version of the Microsoft Windows operating system (OS). There's nothing wrong with it, right? That's exactly what the **UK's National Health Service (NHS)**[9] thought. That is, until one of their outdated Windows machines was hit with a WannaCry ransomware that locked out 600 computers, resulting in the cancellation of 19,500 medical appointments and five emergency centers out of service. WannnaCry ransomware is a type of computer worm that moves between systems in an interconnected network, and takes everything down in its wake. The damage could have been much worse if it hadn't been for one of NHS' technicians who found the kill-switch to the ransomware.

Security experts commented that this incident could have been prevented in the first place had the NHS updated their Windows operating system properly. Legacy operating systems often have security gaps that make them vulnerable to certain ransomware. This isn't just limited to operating systems; several data misconfigurations in Google Cloud Platform, such as confusing the *allUsers group* with the *allAuthenticatedUsers group* could put systems at risk.

To ensure your systems are properly configured and protected from security threats, ensure you follow the steps below:

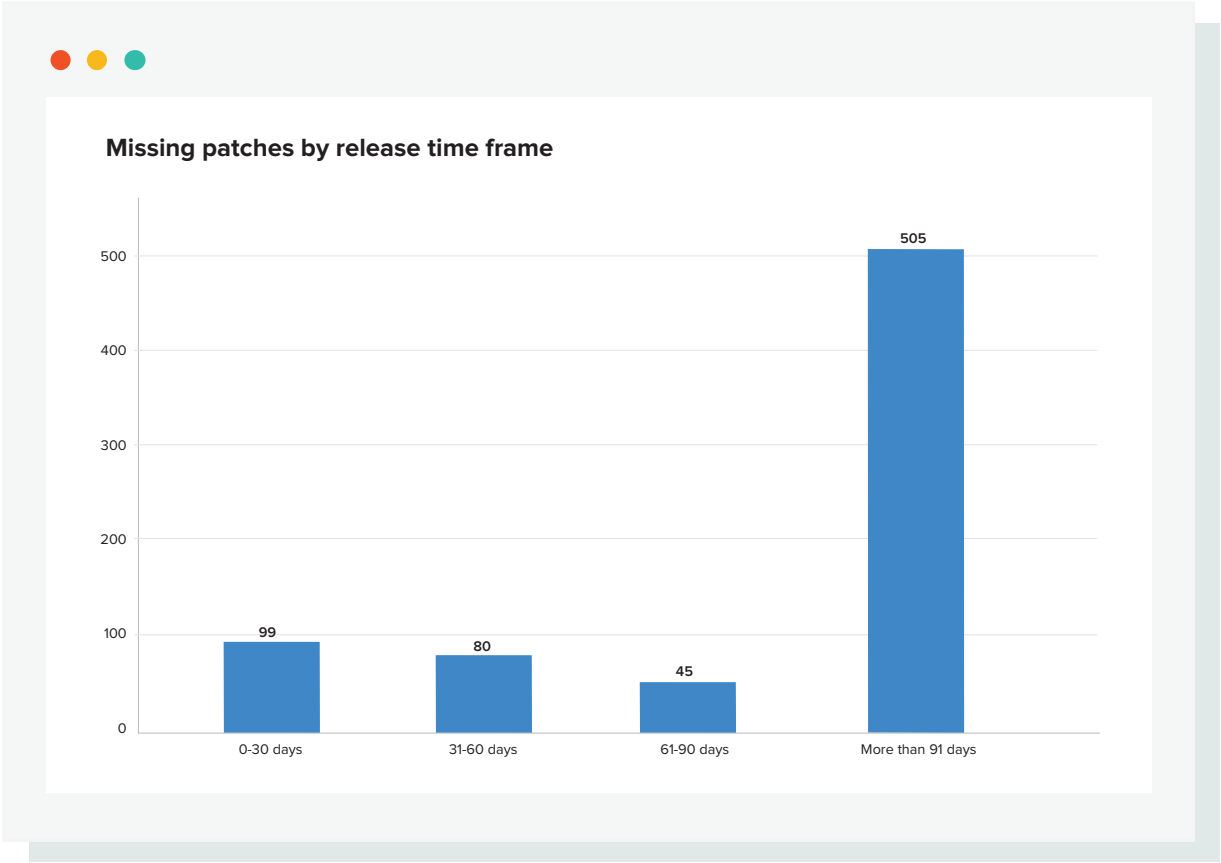
1. Update systems with outdated software and OSs

In addition to putting organizations' data at risk, systems with outdated OSs and software lack basic ransomware protection that could disrupt business services and functions. For example, if you're an educational institution providing students with remote access to your digital libraries, any disruptions as a result of outdated software could lock the entire student community, along with the teaching staff, out of digital libraries until the issue is resolved. To see if any system in your organization has an outdated OS, use this report.



From the report, it's obvious that some systems are actually running on Windows XP, which is outdated. Microsoft has also issued several notifications for corporations and individual users to upgrade their XP operating systems. The next course of action here is to do an OS update for at-risk systems highlighted in this report.

Another way to see if your systems are up to date with the latest software and OS updates is to identify systems with missing patches by the patch release time frame. What you're doing here is looking at the number of missing patches by the number of days that have passed since the time of the patch release. This gives you an overview of the vulnerability status of your systems due to missing patches.



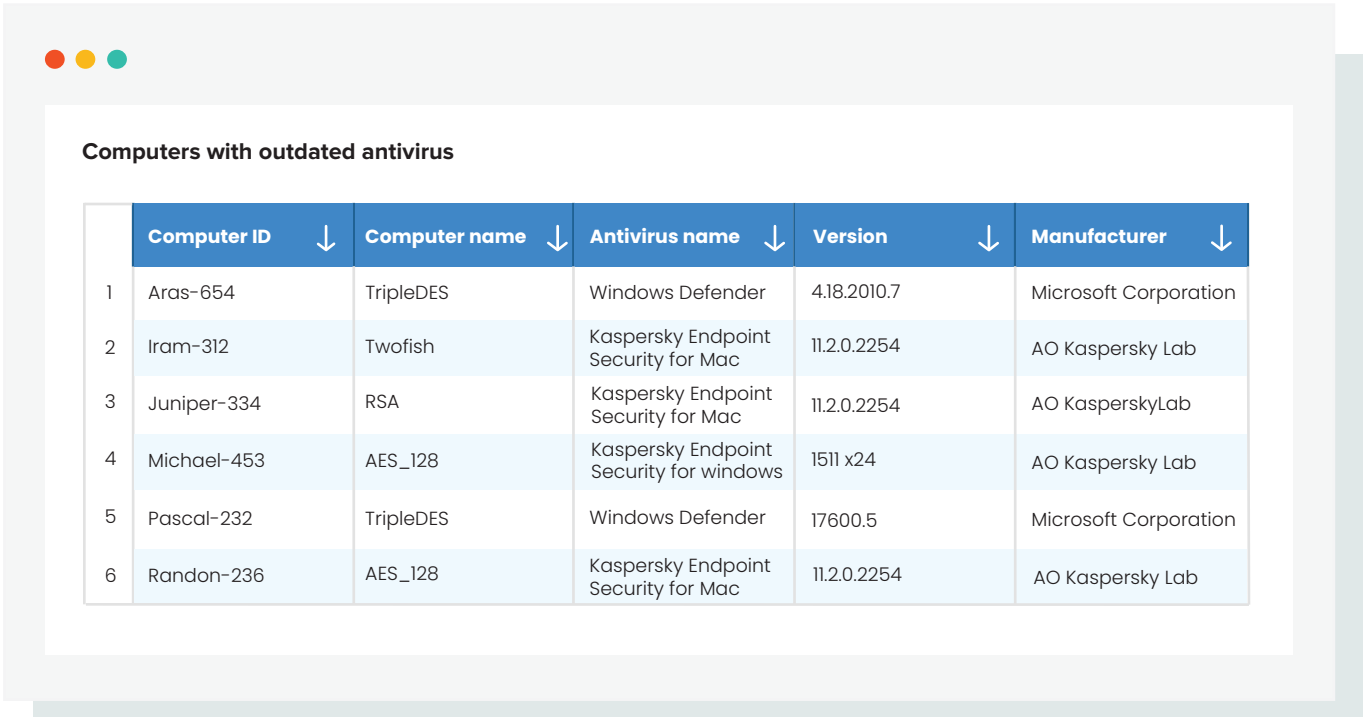
The report above indicates that there are over 500 systems with missing patches that were released 90 days ago. This report can be useful for security staff to prioritize patch updates and ensure systems are updated.

2. Update computers with outdated antivirus

Systems using outdated antivirus software are almost as risky as systems without antivirus. In a way, it creates a false sense of security that leads users to believe they are indeed covered under the security blanket, while in reality they're exposed to the latest security threats. Most antivirus software today sends out automatic updates and patches.

Microsoft[10] conducted a study recently where it discovered that almost 10 percent of Windows 8 computers are running on expired antivirus software. It also found that malware infection rates for these computers are almost the same as those with no antivirus protection at all. In fact, Windows 8 computers with outdated antivirus were at four times greater risk than those with an updated antivirus software.

The pivot report given below provides an overview of computers with outdated antivirus protection.



Computers with outdated antivirus

	Computer ID	Computer name	Antivirus name	Version	Manufacturer
1	Aras-654	TripleDES	Windows Defender	4.18.2010.7	Microsoft Corporation
2	Iram-312	Twofish	Kaspersky Endpoint Security for Mac	11.2.0.2254	AO Kaspersky Lab
3	Juniper-334	RSA	Kaspersky Endpoint Security for Mac	11.2.0.2254	AO KasperskyLab
4	Michael-453	AES_128	Kaspersky Endpoint Security for windows	1511 x24	AO Kaspersky Lab
5	Pascal-232	TripleDES	Windows Defender	17600.5	Microsoft Corporation
6	Randon-236	AES_128	Kaspersky Endpoint Security for Mac	11.2.0.2254	AO Kaspersky Lab

The report shows three computers with outdated antivirus. The immediate step for security personnel is to run an automated patch update, and update these computers with the latest version of antivirus software.

Conclusion

Ensuring data security is a never-ending task that's challenging but also rewarding. Hopefully this e-book gave you a comprehensive overview of the four pillars of your organization's security—people, assets, security controls, and system configurations—along with some helpful tips to secure and reinforce them. With the aid of advanced analytics, you can confidently step towards total security by identifying and eliminating vulnerabilities and threats even before they shape up into a viable threat. This can go a long way in ensuring total security for your organization.

Chapter 3: An introduction to Analytics Plus

ManageEngine Analytics Plus is a business intelligence and IT analytics solution that brings together data from several IT applications to provide a 360-degree view of the IT landscape in one console. Analytics Plus integrates out of the box with Desktop Central to provide endpoint management teams a bird's-eye view of their endpoints and their current security status, along with timely updates on security gaps and vulnerabilities in their endpoints, buying them enough time to patch or secure these gaps before they even shape up into a viable security hazard.

Built with a self-service approach, Analytics Plus banks on its computational horsepower, making it easy for everyone in the organization—from frontline security engineers to senior managers and CISOs—to process data and gain complete visibility into corporate-owned and personal devices. Analytics Plus offers several sharing and collaboration options to bring your team closer to data, making it easy for them to collaborate collectively, and work towards the common goal of making the enterprise more secure.

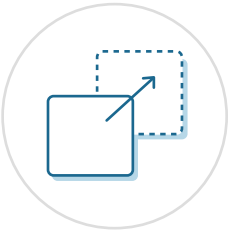
Discover more powerful features of Analytics Plus that can help you make sense of the data from your Desktop Central application.

Standout features of Analytics Plus

Out-of-the-box insights

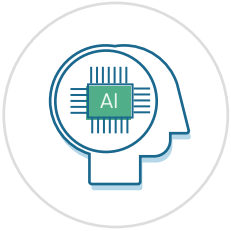
Regardless of whether you're just getting started with analytics or a pro who knows their way around authoring report queries, Analytics Plus' prebuilt reports and dashboards for Desktop Central are the best way to monitor and gain insight into your endpoints. Built on industry-acclaimed metrics, these prebuilt dashboards cover specific areas of endpoint security management such as vulnerability management, threat assessment, hardware and software inventory analysis, patch management, mobile applications management, and more.

In response to the ever-evolving threat landscape, we'll continue to release more dashboards and reports with product updates that users can avail simply by upgrading the application.



Intuitive drag-and-drop UI

So you want to create your own reports? Analytics Plus' reporting interface lets you drag and drop columns into your axes for an effortless report building experience. The application also suggests charts that will better your suit your data. What's more? Once you've created your charts, you can easily toggle between different chart types and visualize your data in different chart forms. Analytics Plus' UI is designed with one goal in mind: Users should be able to get insights into data easily, regardless of their technical expertise.



Augmented analytics

Today's cyberthreats are becoming more and more sophisticated, so the analytics application that helps you catch those threats should also become sophisticated, right? Analytics Plus comes with a built-in AI-assistant, Zia, that intuitively interprets user questions and responds with rich insights into endpoint data. Experience hands-free reporting by asking Zia questions about your data, then sit back and watch as Zia gets you insights you need at lightning speed.

Predictive insights

At Analytics Plus, we understand that the battle against cybersecurity threats is a difficult one. So, we made it easy for you to visualize the future, and secure your endpoints in advance. Running a patch update? Use our trend forecasting to see which systems and how many need patches in the next three or six months, and prioritize patch deployment to address the most imminent threats.

That's not all! You can use trend forecasting to foresee resource requirements, hardware and software asset requirements, license expiry, compliance status, and more.

Data blending

Analytics Plus integrates with a whole suite of IT applications from ManageEngine (ServiceDesk Plus, ServiceDesk Plus MSP, OpManager, Applications Manager, Password Manager Pro, PAM360), as well as from third-party applications (ServiceNow, Zendesk, Jira). You can get a unified vision of your IT from several applications in one console using data blending. You can also blend data from a variety of local files, cloud and local databases, cloud drives, and web feeds with your endpoint management data using Analytics Plus.

Historical snapshots

Capture and record changes in your data periodically using historical snapshots. For instance, how many patches did you update in April 2019? Who are the users who don't regularly update their OS and require IT intervention? Details like these tend to get overridden when the patches or the OS are updated. Historical snapshots enable you to store these details for future reference and analysis.

Sharing and collaboration

Use fine-grained access controls when you email reports and dashboards to your team to control what data each person can view or access. Embed status reports and dashboards in intranet portals, forums, or webpages to let your organization know where you stand in terms of security. Export or create slideshow of dashboards to share with vendors or partners, or present them at your monthly meetings.

Report commenting

Analytics Plus enables users to contextually collaboratate over shared concerns without ever leaving the Analytics Plus UI. Users can tag other users to bring their attention to specific reports or dashboards, annotate reports to pinpoint sections of the report that need attention, or show support to colleagues by upvoting their suggestions and recommendations to improve security.

Free trial and consultation

ManageEngine Analytics Plus is available for a free, **30-day, all-access trial** for Desktop Central users. Just download the application, set up the integration with Desktop Central, and start gaining insights from the get-go. Need help setting up the integration? **Reach out** to our analytics experts any time, and we'll be happy to help you.

You can also **sign up for a free consultation session** with our in-house analytics experts who'll listen to your reporting requirements and show you how to leverage Analytics Plus to achieve your reporting needs.

Reference

1. https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem#:~:text=Information%20security%20spending%20is%20expected,its%20December%202019%20forecast%20update.
2. https://www.absolute.com/go/study/2019-endpoint-security-trends/
3. https://www.observeit.com/cost-of-insider-threats/
4. https://www.forbes.com/sites/bishopjordan/2018/09/09/british-airways-hacked/?sh=282dea1167ae
5. https://www.riskiq.com/blog/labs/magecart-british-airways-breach/
6. https://twitter.com/monzo/status/1038042015286607872
7. https://www.raspberrypi.org/
8. https://beagleboard.org/black
9. https://www.informationsecuritybuzz.com/articles/why-managing-your-it-inventory/
10. https://www.darkreading.com/attacks-breaches/expired-antivirus-software-no-1-cause-of-unprotected-windows-8-pcs/d/d-id/1317440

ManageEngine Analytics Plus

www.manageengine.com/analytics

18K
customers
across the world

18+
years of IT
management experience

90+
products
and free tools

190+
countries
served