IAITAM ACE

May 7–9, 2024 The M Resort Las Vegas, NV

Robbie Plourde, USU

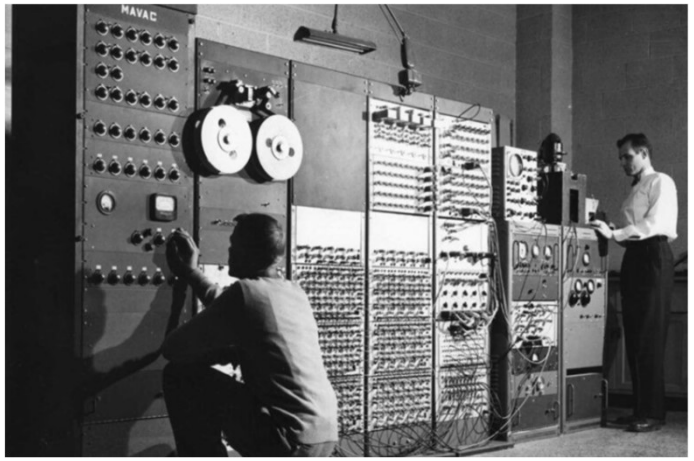
Enhancing Asset Security in the Digital Age

How ITAM can help Safeguarding Your Assets in an Evolving Landscape

Finding your IAITAM Oasis

History of Asset Security

- The first Cyber Attack took place in **1834**
- The first virus was created in **1971**
- The first spam E-Mail was sent in **1978**



IAITAM Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

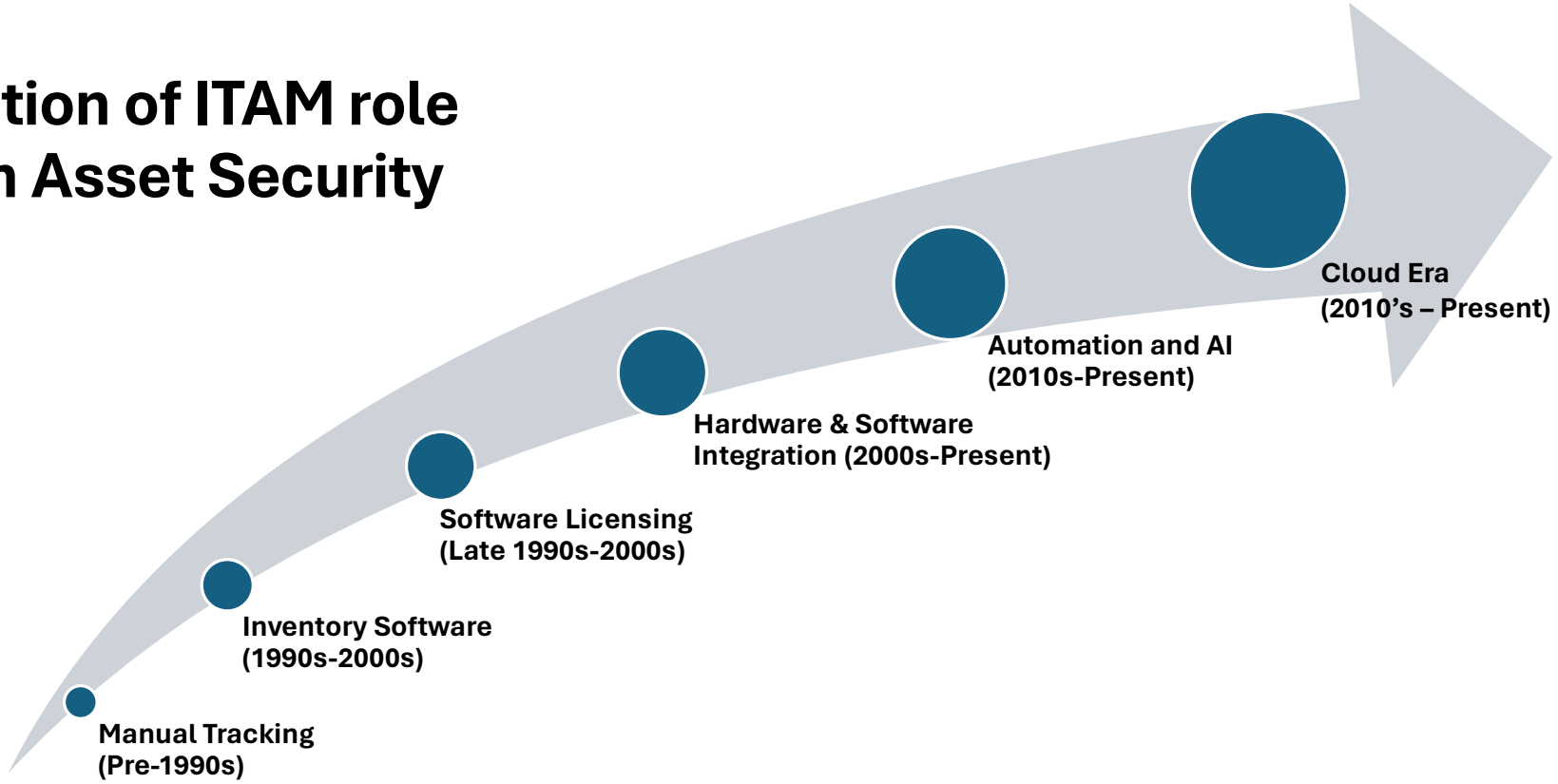
USU

Emerging threats

Cyber threats to asset security are diverse and constantly evolving as technology advances. Some of the top cyber threats include:

- Malware
- Phishing Attacks
- Data Breaches
- Ransomware
- Insider Threats
- Distributed Denial of Service (DDoS) Attacks
- Social Engineering

Evolution of ITAM role within Asset Security



Challenges of Asset Security (in the Cloud Era)

Asset Visibility

In a traditional on-premises environment, assets were physically present within the organization's infrastructure. However, cloud assets are dispersed across various platforms, providers, regions, and accounts, making visibility challenging. With data stored across multiple servers and locations, the risk of unauthorized access and data breaches increases..

Misconfiguration

Cloud environments offer a high degree of flexibility and scalability, but this also means there's a greater chance of misconfigurations. Misconfigured security settings can inadvertently expose sensitive data or services to unauthorized access.

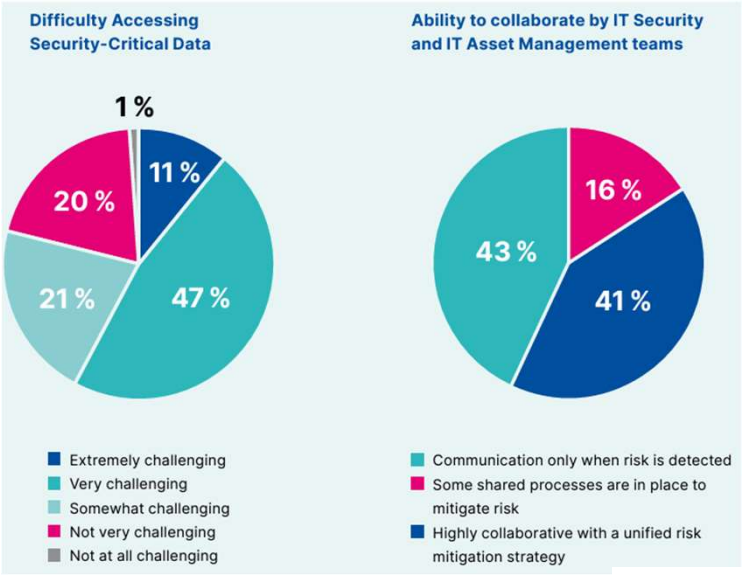
Shadow IT

Employees may use unauthorized cloud services or applications without IT department approval. This can lead to security vulnerabilities and data leakage if these services lack adequate security controls or compliance measures.

Security has Never Been More Essential

The most successful Cybersecurity teams work with ITAM teams to ensure products are up to date, patches installed, end of support/life products removed, and other types of vulnerabilities identified.

However, according to IDG report, nearly 80% find it challenging to access the data needed to make sound decisions.



IAITAM Finding your ITAM Oasis

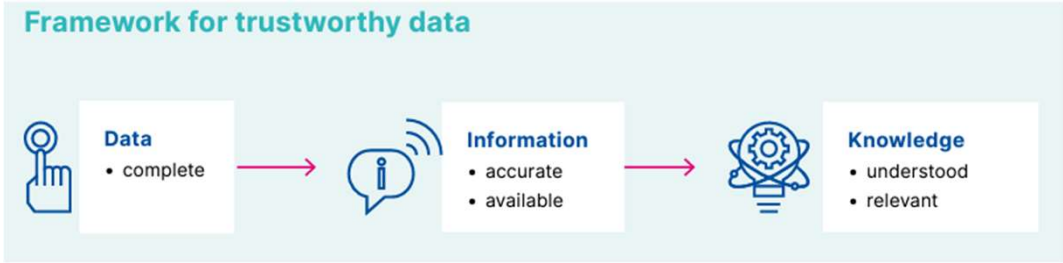
USU

May 7–9, 2024 The M Resort Las Vegas, NV

Critical Importance of Trustworthy Data

- Trustworthy Data is the foundation of IT Asset Management according to ISO 19770-1
- “Trustworthy Data is data that is accurate, complete, relevant, readily understood by and available to those authorized users who need it to complete a task.”
- Security, Procurement, IT Ops, Finance, FinOps, and ITAM all make decisions based on the same trustworthy data.

The goal is to combine and normalize data to generate rich data which can serve all stakeholders.



Why we should heed the warnings

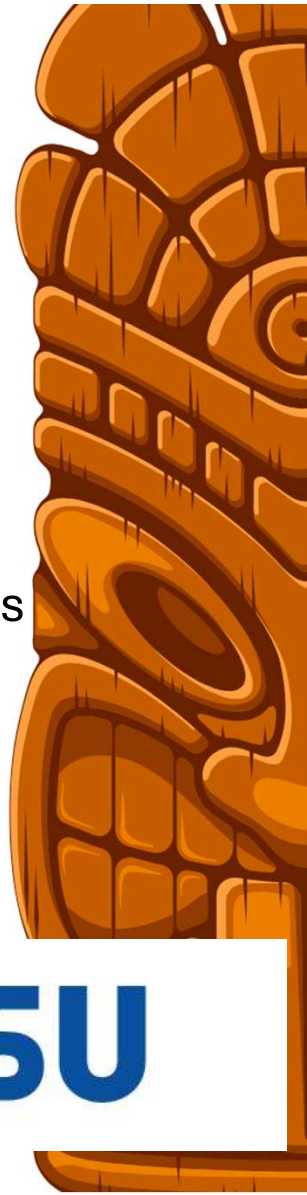
- Less than 1% of organizations have visibility of at least 95% of their assets.
- Nearly 90% of device assets in the modern organization are cloud-based, meaning physical devices represent less than 10% of total devices.
- Only 45% of organizations have advanced asset intelligence with visibility and insight for over 75% of their assets.
- The average organization has well over 500 cyber assets for every human employee.
- 80% of organizations are pursuing a hybrid or multi-cloud strategy, and many organizations are experiencing cloud protection challenges.
- Difficulty coordinating activities among hybrid environments is the No. 1 challenge in understanding IT asset inventory.
- The average time to identify and contain a data breach is 277 days (about 9 months). —IBM
- The total number of annual cyber-attacks increased 38% in 2022, compared to 2021.

2022-the-state-of-cyber-assets-report-reveals-security-vulnerabilities.aspx
*Gartner 2023 Hype Cycle for Security Operations

Strategies -

Enhancing asset security in the digital age

- Identify and Classify Assets
- Conduct Risk Assessment
- Implement Access Controls
- Update and Patch Systems
- Monitor and Detect Anomalies
- Stay Informed About Emerging Threats
- Security in the cloud
- Make known what ITAM can provide



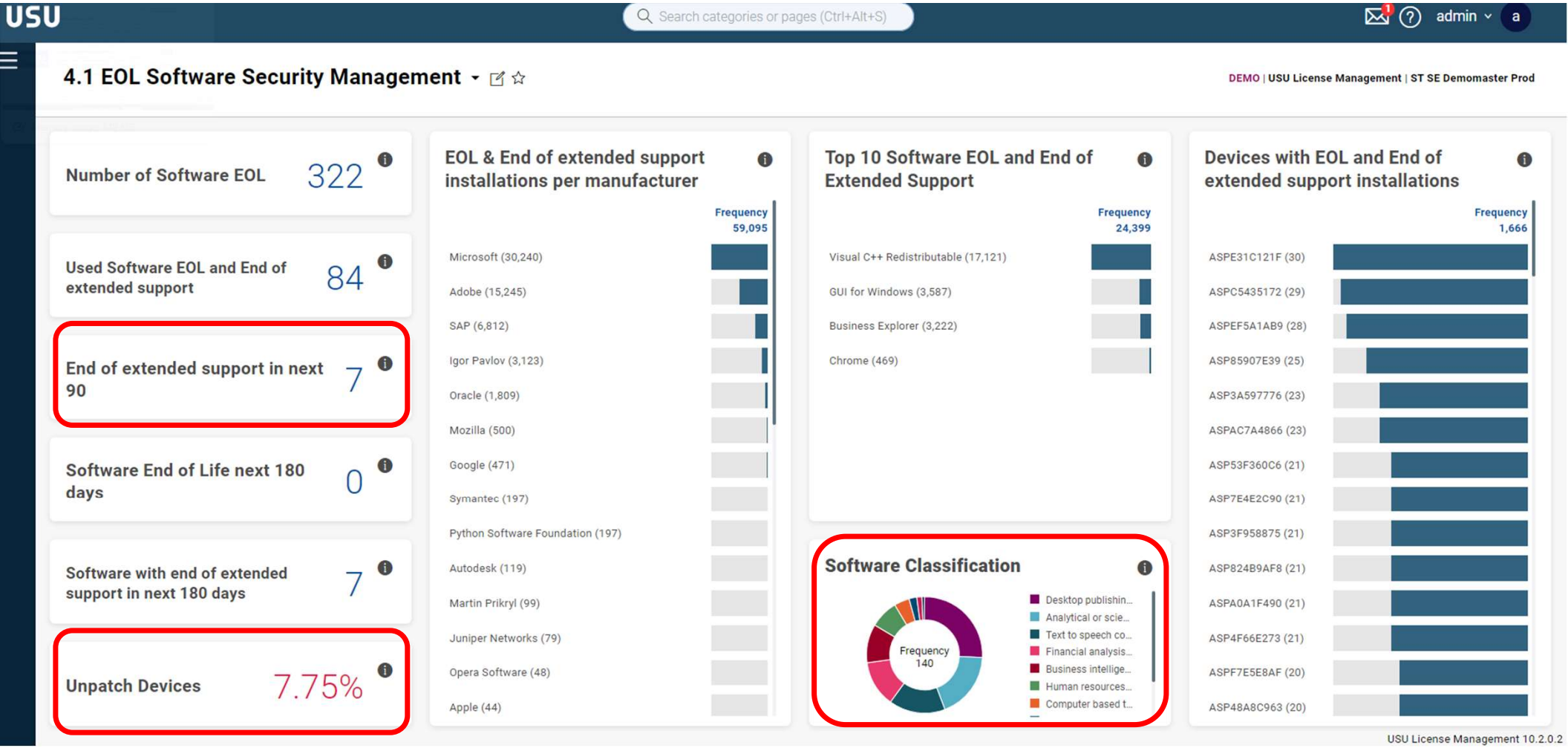
IAITAM Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

USU

Identify and Classify Assets

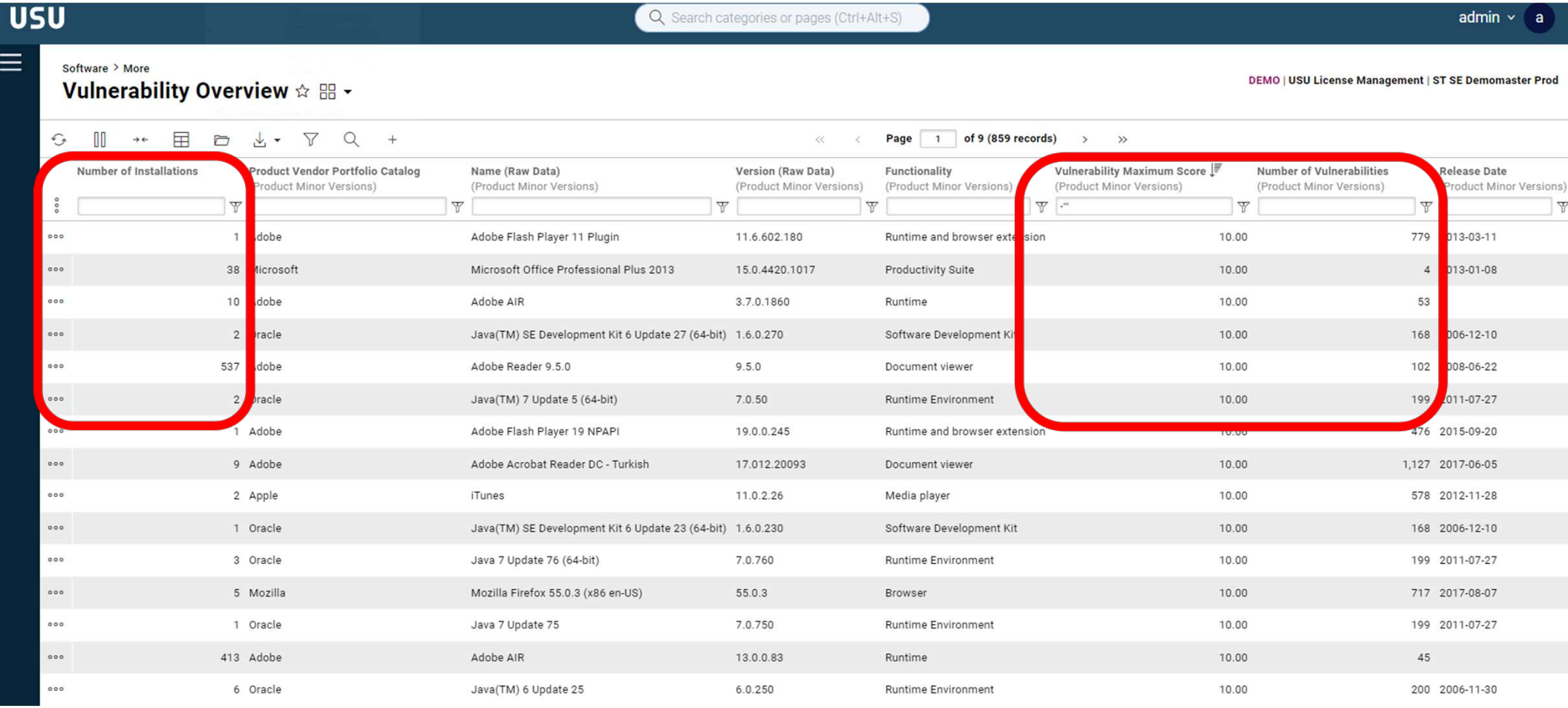
- Begin by **identifying all assets** within your organization, including data, systems, applications, and devices.
- **Classify** these assets based on their sensitivity and criticality to prioritize security efforts.
- **Utilize automated tools and technologies** to discover and inventory assets across your organization's networks, systems, and cloud environments.
- Periodically review and **update your asset inventory** and data classification policies to reflect changes in your organization's infrastructure, technology landscape, regulatory environment, and business priorities.



May 7–9, 2024 The M Resort Las Vegas, NV

Conduct Risk Assessment

- Perform a thorough risk assessment to **identify potential vulnerabilities** and threats to your assets.
- Evaluate the likelihood and impact of various security risks to determine **where** to focus your security efforts.
- Develop **risk mitigation strategies** and controls to reduce the likelihood and impact of identified risks to an acceptable level.
- Establish mechanisms for **ongoing risk monitoring**, measurement, and review to track changes in the risk landscape and assess the effectiveness of risk mitigation efforts.
- Foster a culture of **continuous improvement** by incorporating lessons learned from the risk assessment process into future risk management activities

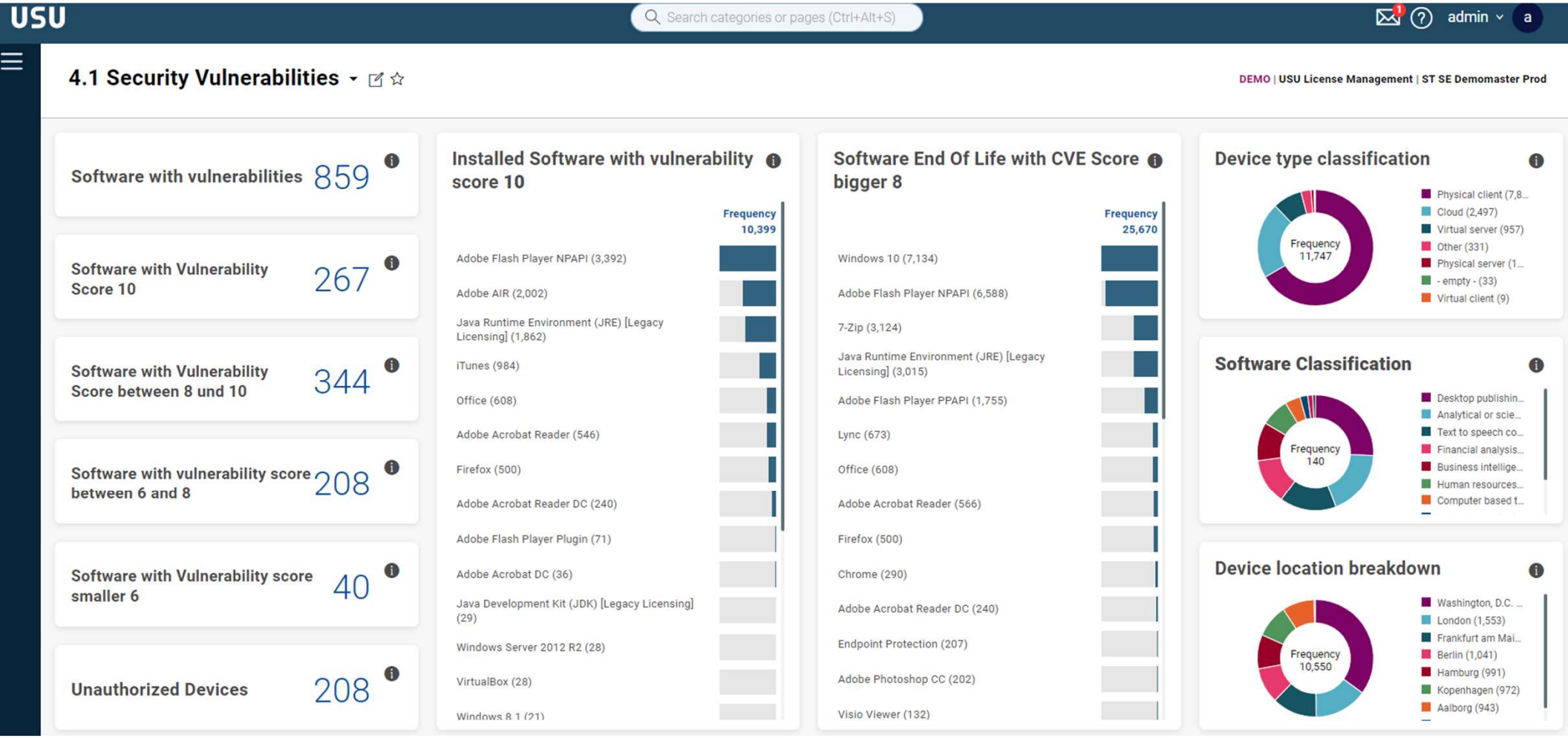

USU
Search categories or pages (Ctrl+Alt+S)
admin
a
Software > More
Vulnerability Overview
DEMO | USU License Management | ST SE Demomaster Prod
Page 1 of 9 (859 records)
Number of Installations
Product Vendor Portfolio Catalog (Product Minor Versions)
Name (Raw Data) (Product Minor Versions)
Version (Raw Data) (Product Minor Versions)
Functionality (Product Minor Versions)
Vulnerability Maximum Score (Product Minor Versions)
Number of Vulnerabilities (Product Minor Versions)
Release Date (Product Minor Versions)
1 Adobe Adobe Flash Player 11 Plugin 11.6.602.180 Runtime and browser extension 10.00 779 2013-03-11
38 Microsoft Microsoft Office Professional Plus 2013 15.0.4420.1017 Productivity Suite 10.00 4 2013-01-08
10 Adobe Adobe AIR 3.7.0.1860 Runtime 10.00 53
2 Oracle Java(TM) SE Development Kit 6 Update 27 (64-bit) 1.6.0.270 Software Development Kit 10.00 168 2006-12-10
537 Adobe Adobe Reader 9.5.0 9.5.0 Document viewer 10.00 102 2008-06-22
2 Oracle Java(TM) 7 Update 5 (64-bit) 7.0.50 Runtime Environment 10.00 199 2011-07-27
1 Adobe Adobe Flash Player 19 NPAPI 19.0.0.245 Runtime and browser extension 476 2015-09-20
9 Adobe Adobe Acrobat Reader DC - Turkish 17.012.20093 Document viewer 10.00 1,127 2017-06-05
2 Apple iTunes 11.0.2.26 Media player 10.00 578 2012-11-28
1 Oracle Java(TM) SE Development Kit 6 Update 23 (64-bit) 1.6.0.230 Software Development Kit 10.00 168 2006-12-10
3 Oracle Java 7 Update 76 (64-bit) 7.0.760 Runtime Environment 10.00 199 2011-07-27
5 Mozilla Mozilla Firefox 55.0.3 (x86 en-US) 55.0.3 Browser 10.00 717 2017-08-07
1 Oracle Java 7 Update 75 7.0.750 Runtime Environment 10.00 199 2011-07-27
413 Adobe Adobe AIR 13.0.0.83 Runtime 10.00 45
6 Oracle Java(TM) 6 Update 25 6.0.250 Runtime Environment 10.00 200 2006-11-30

Implement Access Controls

- Establish robust user **identity management** practices, including user authentication, authorization, and account management.
- Use **Principle of Least Privilege** (PoLP) to restrict access to only those who need it to perform their job responsibilities.
- Implement **Role-Based Access Control** (RBAC) to assign permissions and access rights based on users' roles, responsibilities, and organizational hierarchy.
- Use strong authentication methods such as **multi-factor authentication** (MFA) to verify user identities and prevent unauthorized access.
- Provide **comprehensive training and awareness** programs to educate users about access control policies, best practices, and security awareness.

Update and Patch Systems

- Use automated scanning tools to **detect vulnerabilities** and prioritize patching efforts.
- Keep all software, operating systems, and firmware **up to date** with the latest security patches and updates.
- Regularly **patching known vulnerabilities** helps prevent attackers from exploiting weaknesses in your systems.
- Establish a **patch management policy** that outlines procedures, responsibilities, and timelines for updating and patching IT systems.
- Conduct regular vulnerability assessments and scans to **identify security vulnerabilities** in IT systems, applications, and infrastructure.
- **Educate users** about the importance of updating and patching IT systems to mitigate security risks and protect against cyber threats.



May 7–9, 2024 The M Resort Las Vegas, NV

Monitor and Detect Anomalies and Vulnerabilities

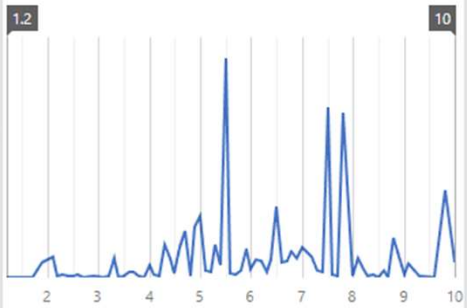
- Implement **continuous monitoring solutions** to detect and respond to security incidents in real-time.
- Use security information and event management (SIEM) tools to **aggregate and analyze** security logs for signs of suspicious activity.
- Establish **baseline patterns** of normal behavior for IT systems, networks, and user activities.
- Provide regular **security awareness training** to all employees to educate them about the importance of security and how to recognize and report potential security threats and anomalies.
- Continuously **review and update your** monitoring and detection **processes** to adapt to evolving threats and vulnerabilities. Regularly evaluate the effectiveness of your controls and make necessary adjustments.

DASHBOARDS AND REPORTS ▸ DATA ANALYSIS ▸ VULNERABILITY MONITORING ▸ VULNERABILITY OVERVIEW

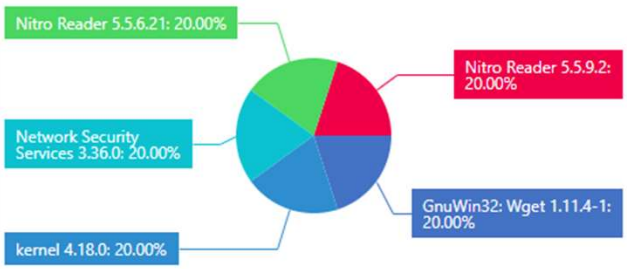
DISCOVERED CVE
4.98K

VULNERABLE PRODUCTS/VERSIONS
157/ 431

Score range filter



Top 5 vulnerable software



Averaged vulnerability score

Software name

Select...

Name	Raw version
Adobe ColdFusion Add-on Servic...	2021.0.0.2
Adobe Flash Player Plugin	12.0.0.77
ADSelfService Plus	5.8
AIX	6.1
AIX	7.2
Alfresco Community	5.0.d
alsa	1.1.0
ansible	2.4.2.0
ansible	2.6.20
ansible-runner	1.4.6

CVE ID	Score	Published	CVE status	Summary	CWE ID	Affected compu...
CVE-1999-0033	7.2	12/6/1997	published	Command execution in Sun systems via buffer overflow in t...		733
CVE-1999-0057	7.5	11/16/1998	published	Vacation program allows command execution by remote us...		733
CVE-1999-0524	2.1	1/8/1997	published	ICMP information such as (1) netmask and (2) timestamp is ...	CWE-200	34
CVE-1999-0566	5	1/8/1997	published	An attacker can write to syslog files from any location, causi...		733
CVE-1999-0656	5	1/1/1999	published	The ugidd RPC interface, by design, allows remote attackers ...		34
CVE-1999-1119	10	4/27/1992	published	FTP installation script anon.ftp in AIX insecurely configures a...		733
CVE-2000-1219	7.5	1/11/2000	published	The -ftrapv compiler option in gcc and g++ 3.3.3 and earlier...		18
CVE-2001-0529	7.2	8/14/2001	published	OpenSSH version 2.9 and earlier, with X forwarding enabled,...		17
CVE-2001-0816	7.5	6/12/2001	published	OpenSSH before 2.9.9, when running sftp using sftp-server ...		17
CVE-2001-0872	7.2	12/21/2001	published	OpenSSH 3.0.1 and earlier with UseLogin enabled does not ...		17
CVE-2001-1061	10	8/31/2001	published	Vulnerability in lsmcode in unknown versions of AIX, possibl...		733
CVE-2001-1323	7.5	5/16/2001	published	Buffer overflow in MIT Kerberos 5 (krb5) 1.2.2 and earlier all...	CWE-120	14
CVE-2001-1380	7.5	10/18/2001	published	OpenSSH before 2.9.9, while using keypairs and multiple ke...		17

Stay Informed About Emerging Threats

- Subscribe to Industry Newsletters and Blogs
  - Krebs on Security -> https://krebsonsecurity.com/
  - Dark Reading -> https://www.darkreading.com/
  - The Hacker News -> https://thehackernews.com/
- Follow Security Thought Leaders on Social Media
  - Bruce Schneier: @schneierblog - renowned security technologist, author, and cryptographer.
  - Brian Krebs: @briankrebs - investigative journalist who covers cybersecurity, cybercrime, and technology security.
  - Troy Hunt: @troyhunt - Cybersecurity expert, and the creator of the "Have I Been Pwned?" breach notification service.
  - Nicole Perlroth: @nicoleperlroth - Cybersecurity journalist for The New York Times
- Join Online Communities and Forums
- Monitor Vulnerability Databases and Threat Feeds
  - National Vulnerability Database (NVD)
  - Common Vulnerabilities and Exposures (CVE)
- Engage in Continuous Learning and Professional Development

Stay Informed About Emerging Threats

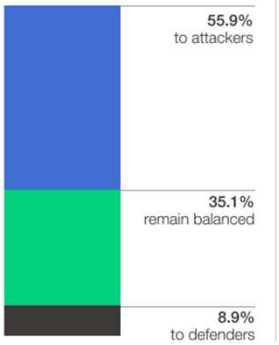
Organizations will increase data protection investment but recover less in 2024, according to a survey by Veeam Software. Data protection budgets are expected to increase by 6.6% in 2024 amid continued threats from ransomware and cyberattacks.

CYBERSECURITY

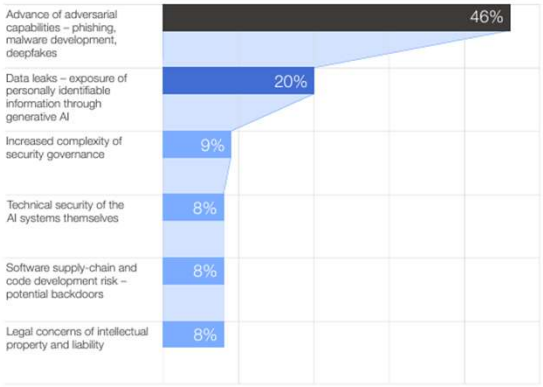
AI will make bogus emails appear genuine

Emerging technologies will exacerbate long-standing challenges related to cyber resilience

In the next two years, will generative AI provide overall cyber advantage to attackers or defenders?



What are you most concerned about in regards to generative AI's impact on cyber?



2. Ransomware attack on key US and UK water companies

Two major water utility companies in the US and UK have been targeted by separate ransomware attacks resulting in apparent data breaches, *Security Week* reports.

Finland Blames Chinese Hacking Group APT31 for Parliament Cyber Attack

Mar 28, 2024 Cyber Espionage / Malware

The Police of Finland (aka Poliisi) has formally accused a Chinese nation-state actor tracked as APT31 for orchestrating a cyber...

NPR

AT&T data breach leaks info of 7.6M customers to dark web

Finding your ITAM Oasis

USU

May 7–9, 2024 The M Resort Las Vegas, NV

https://www.weforum.org/agenda/2024/01/ransomeware-ai-cybersecurity-news-roundup/
World Economic Forum - https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

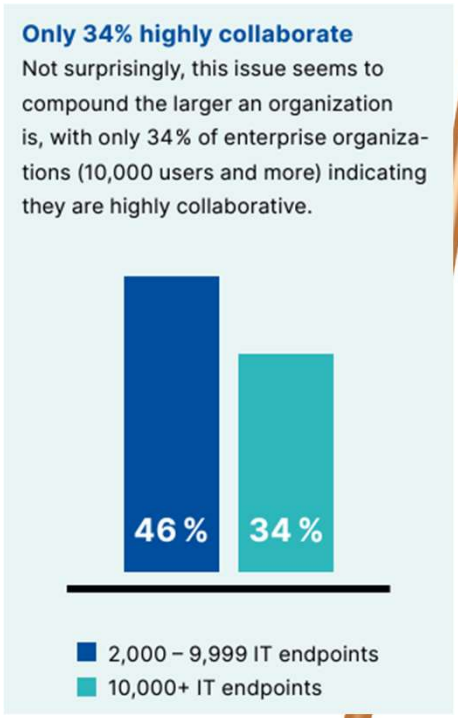
Security in the cloud

- Adopt a Zero Trust security model
- Implement robust Identity and Access Management (IAM) controls to manage user identities, permissions, and access to cloud resources.
- Encrypt sensitive data both in transit and at rest.
- Leverage built-in security services provided by cloud service providers, such as AWS Security Hub, Azure Security Center, and Google Cloud Security Command Center.
- Implement continuous monitoring solutions to track user activities, configuration changes, and security events in real time.
- Establish governance policies and procedures to enforce security, risk management, and data protection practices across cloud environments.
- Foster collaboration and information sharing with your secur

How to promote better collaboration - ITAM and Cybersecurity

According to the IDG report, 59% report their IT security and IT asset management teams are lacking a unified risk mitigation strategy.

- Create an advisory group with the goal of sharing information about strategy, plans, projects, goals, and objectives.
- It may be advantageous to bring both functions into a common governance framework
- Ultimately, collaboration between Cybersecurity and ITAM teams benefits all areas of the organization.



IAITAM

Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

Things to remember and review

- Asset Inventory and Classification
- Access Control and Privilege Management
- Data Encryption
- Patch Management & Endpoint Security
- Implement security awareness
- Continuous Monitoring & Threat Detection
- Security Culture and Governance
- Emerging Technologies and Trends

IAITAM Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

USU

Robbie Plourde
Principal Solution Engineer
FinOps Certified Practitioner
+1 (757) 525.0075
Robbie.plourde@usu.com
www.usu.com

IAITAM

Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

USU