securonix

2022 Securonix Threat Report

Kayzad Vanskuiwalla

Sina Chehreghani

The 2022 Securonix Threat Report highlights the trends, required data, and detection summaries for key threats. Additionally, our report covers the techniques we've seen from the trenches across insider threat, cloud infrastructure misuse/abuse, and preemptive ransomware detection. Finally, we added a new section in this report covering IoT/OT.

Since the beginning of the year, we noticed a significant uptick in the number of threats observed globally. New reported vulnerabilities are being identified at nearly double the pace of 2021—in fact the NIST National Vulnerability Database shows they have increased by more than 2,000. Further data from Securonix Autonomous Threat Sweeper (ATS) shows a significant rise in the number of advanced threats, TTPs, and IOCs identified and scanned globally for customers.

Securonix ATS identified emerging threats at a steady pace throughout the first half of 2022, having distributed more than 800 threat awareness notifications to subscribers. Nearly 600 threats have been detected in environments so far this year and the pace of detected threats is expected to increase for the rest of the year as vulnerabilities and threat actors continue to develop in the wild.

The 2022 threat trends we've observed are highlighted below:

- **Awareness:** 867 threats observed
  482% increase from 2021
- **Discovery:** 35,776 IOCs
  380% increase from 2021
- **Investigations:** 582 threats detected, analyzed and reported
  218% increase from 2021

Table of Contents

Securonix Autonomous Threat Sweeper (ATS) identified emerging threats at a steady pace throughout the first half of 2022 having distributed more than 800 threat awareness notifications to subscribers. ATS provides continuously updated threat content for rapid response, automating exposure assessment and incident creation for subscribers. Nearly 600 threats were detected in environments so far this year. The pace of detected threats is expected to increase for the rest of the year as vulnerabilities and threat actors continue to develop in the wild.

Autonomous Threat Sweeper – 2022 Metrics

Threat Awareness Reports **867** | ↑ 481.9%

IOCs/TTPs Swept **35,776** | ↑ 380.0%

Threat Detection Reports **582** | ↑ 218.0%

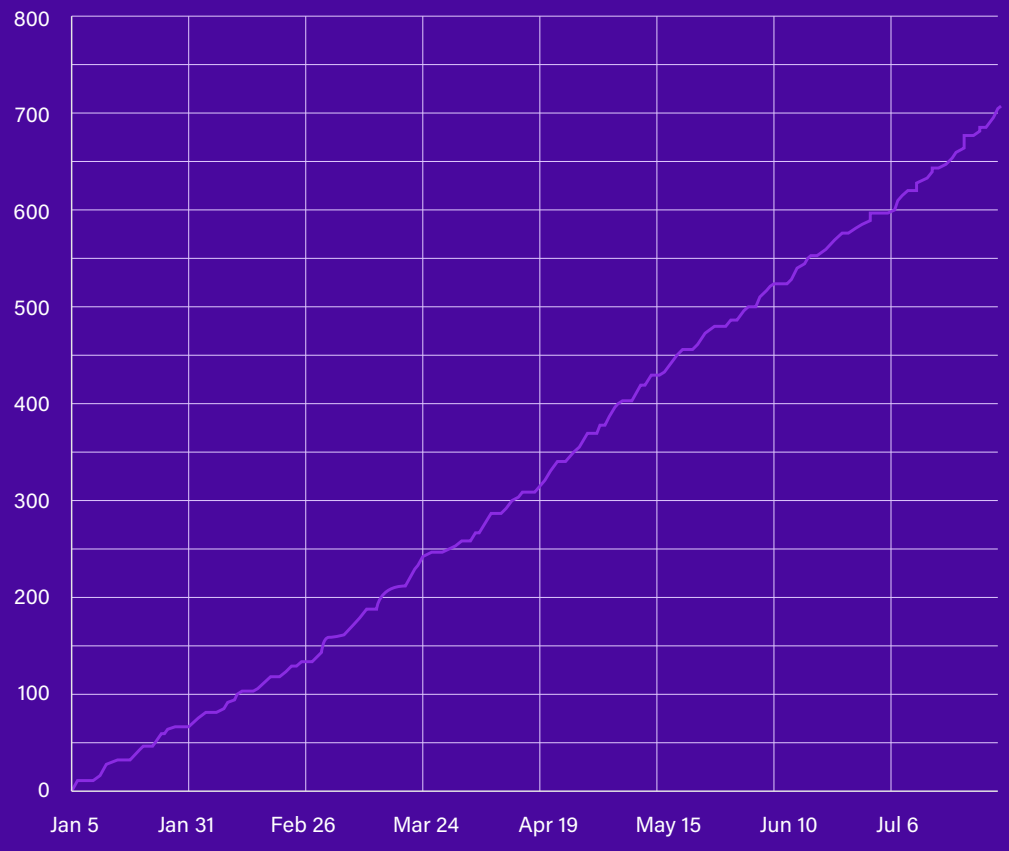


Table 1: Securonix Autonomous Threat Sweeper metrics in 2022

Executive summary

Organizations face greater risk as threats in an evolving, perimeterless environment are now more complex. As more organizations grow increasingly reliant on cloud infrastructure there is a shift in the methods used by insiders to steal data through cloud apps and platforms. Coupled with sophisticated ransomware attacks and managing IoT/OT environments, security teams need to plan to cover all these relevant areas for a stronger security posture. This threat report identifies four areas that security teams need to address to improve their security posture: insider threats, monitoring cloud infrastructure, preempting ransomware attacks, and IoT and OT attacks.

As cloud adoption grows then cloud infrastructure misuse and abuse remain high risk areas. Within those organizations adopting the cloud, users are the primary cause for potential risk to cloud infrastructure, from unintended platform modifications to changing access to data. In fact, we found insider threats remain persistently active over the last 12 months. Insiders are leveraging cloud apps to steal corporate data by using personal email and sharing platforms. The cloud represents a shift in egress methods by insiders who are increasingly using cloud apps to exfiltrate data, a shift from traditional methods such as USB and email.

The extended attack surface of cloud infrastructure is an opportunity for threat actors and sophisticated nation state–sponsored attackers alike. With corporate networks extending to the cloud to support a remote and global workforce, ransomware attacks are taking advantage of the larger attack surface and have increased their activities this year. By leveraging preemptive detection strategies, organizations can improve their security posture and stop attacks early in the ransomware kill chain.

Finally, we found that IoT and OT environments pose a different organizational footprint and are a growing area of concern for organizations. Understanding the unique nature and vulnerabilities of things in the IoT and the industrial section is crucial for security teams. Combining OT security with traditional IT security by collecting key data sources and monitoring for unusual behavior provides the most robust threat detection and coverage.

This report's overall recommendation is that organizations need to review anomalous user behavior and detection coverage to help improve their mean time to respond to insider threats and the increasing risks presented by cloud infrastructure adoption. Additionally, leveraging preemptive detection strategies can stop attackers earlier in the kill chain in ransomware attacks. For IoT and OT environments, combining the key data sources to look for unusual behavior provides better detection and response.

Special thanks to the Securonix Threat Labs Hunting and Threat Intel teams who identified core threat scenarios that helped us build the background for this report and the Securonix Threat Labs Data and Detections teams for providing engineering support and building the data and detections that provided the metrics used in this report.

Report sample data

For this report, our researchers pulled data from the security team's investigations over the last 12 months. The report uses telemetry from select anonymized data. Securonix Threat Labs curates the latest threat intelligence to provide a comprehensive view of emerging threat campaigns and threat actors in the wild. We cover insider threats, cloud infrastructure challenges, preemptive ransomware detection, and IoT/OT.

Our sample data included the following industries:

- Education technology
- Healthcare services
- Consumer goods and services
- Finance, banking and insurance
- Manufacturing
- State/local/government
- Construction
- Transportation
- Retail

Report key takeaways

2022 threat trends:

- Awareness: 867 threats observed (482% increase from 2021)
- Discovery: 35,776 IOCs (380% increase from 2021)
- Investigations: 582 threats detected, analyzed and reported (218% increase from 2021)

Insider threats:

- Securonix customers were well covered in detecting flight risk and exiting risk behavior by way of email. Inherent risk-aligned use cases were enabled in roughly 85% of available customer environments. Considering that 68% of the sample set ingests some form of email or email security logs, the ability of UEBA to leverage related use cases to proactively identify potential insider threats is a boon for an establishment.
- Email (68%) and content management products (68%) continue to be top egress vectors.
- The top insider threat-related data sources ingested include Microsoft Windows (78%), followed by email security and content management system at over 60% ingestion.
- An average of 83% of the sample set had inherent risk policies enabled in their SIEM, closely followed by 71% of sabotage policies and 67% aggregation policies.
- Cloud application security brokers (CASBs) have the most policies of any insider threat-related data source and exfiltration-related policies. However, only 13% are ingesting that data source into their SIEM, thus identifying an important gap in the visibility into insider threat-related exfiltration.

Cloud infrastructure

- Cloud content management, cloud services, cloud authorization, and MS Office 365 have the highest percentage of tenants that have use cases to detect cloud threats. This re-emphasizes the importance of cloud-centric security platforms and audit capabilities. Detecting cloud threats begins with monitoring insufficient identity and access management. Alert trends indicate misconfigured or inadequate access controls are increasingly responsible for cloud compromise.
- More than 80% of customers who have enabled suspicious activity-related policies demonstrated a higher success rate in detecting related threats. Of the data set that have enabled key cloud policies against MITRE ATT&CK tactics, nearly 84% have relevant key management abuse policies enabled, with credential access (79%), collection (77%), and persistence (76%) closely following.
- Despite access/identity management covering six MITRE ATT&CK tactics (nearly the majority of brute force and account manipulation detection policies), only 24% of environments ingest the data source. This data gap in access/identity management exacerbates the potential for creating detection gaps in credential access and persistence.
- Of the count of cloud policies covering MITRE ATT&CK tactics enabled by our sample, the most prominent cloud infrastructure coverage includes 25 policies for initial access, 23 for persistence, and 21 for both privilege escalation and defense evasion.

Ransomware

- Although raw EDR events provide more than 70% coverage of related MITRE ATT&CK tactics, just 25% have ingested the telemetry into their SIEM.
- Phishing is responsible for almost half of the top policy violations related to initial access, and 60% of customers have recognized that consistent threat by ingesting some form of email logs.
- Command and scripting threats account for six of the top 10 execution initial access policies. Adversaries continue to abuse interpreters across platforms to execute various payloads and scripts via PowerShell, Python, JavaScript, and Windows Command Shell among others.
- Windows/Unix/PowerShell logs provide coverage to 70% of MITRE ATT&CK tactic coverage, with customers recognizing its usefulness in a SIEM as 78% of customers are ingesting Windows logs. However, PowerShell logging and auditing is crucial for more robust visibility into malicious activities, and only 12% of customers are ingesting these logs, demonstrating a significant gap to bridge for in-depth ransomware coverage.
- Network (84%), Windows (81%) and antivirus and EDR logs (74%) lead the data sources ingested for ransomware detection coverage.
- Although 78% of the sample data set ingest some form of firewall logs, just under 14% ingest flow logs, despite flow logs providing the second-most coverage for discovery tactics. Additionally, just under 39% ingest DNS logs, a metric that needs to be increased for organizations to capture key command and control activity including, DNS beaconing, persistent DNS traffic, and excessive number of DNS responses.

Identifying Insider Threats

Many organizations aren't sure of the most efficient way to monitor for insider threats or if they currently have insider threats in their environment. Additionally, as organizations continue to migrate to the cloud and invest in cloud collaboration tools, data is more accessible to users than ever before. With easier access to critical data including intellectual property, users are empowered to help and hurt organizations. Monitoring critical data and users with access to that data is the first step to understanding abnormal activity from normal.

Combining critical data locations and attempts to collect this data with user behavior context (around intent to leave the organization e.g., flight risk or exiting risk behavior) helps reveal potential malicious intent to exfiltrate or delete data, thereby prioritizing insider threat scenarios for security professionals. For example, our research finds an increased use of cloud storage platforms including emails/blogs/content management like Google Drive being used for data exfiltration. Identifying regular behavior on cloud storage platforms versus data exfiltration helps lower risk to the organization.

There isn't a universally accepted framework like MITRE ATT&CK and Lockheed Martin's Cyber Kill Chain to guide investigations for insider threats. To help security professionals, Securonix recommends ensuring inherent risk variables, data collection, and data exfiltration or loss indicators, are optimized in tandem to provide the best detection and response to insider threats.

Use inherent risk indicators to be more proactive

It's important to first consider who is most likely to become an insider threat and proactively monitor them. Inherent risk indicators of insider threats include those users who are exhibiting flight risk or exiting risk. These users may have upcoming termination dates or were added to watchlists due to restructuring, acquisitions, mergers, or layoffs.

Create or update watchlists containing users to include those with poor performance ratings or individuals who might not share an organization's core values due to changes in the existing corporate climate. Potential triggers to add users to a watchlist may include the organization's intent to enforce employees' vaccinations (or not) and requiring employees to return to the office. Such situations require permission from legal and HR, but organizations should also look to integrate these issues in relation to workforce acceptance. Combining all indicators related to exfiltration along with data aggregation and watchlisted users yields the best results.

Users identified as flight risk or exiting risk or associated with other inherent risk indicators had a 60-70% likelihood of being associated with insider threats. Leveraging inherent risk indicators would help preemptively detect and respond to insider threats.

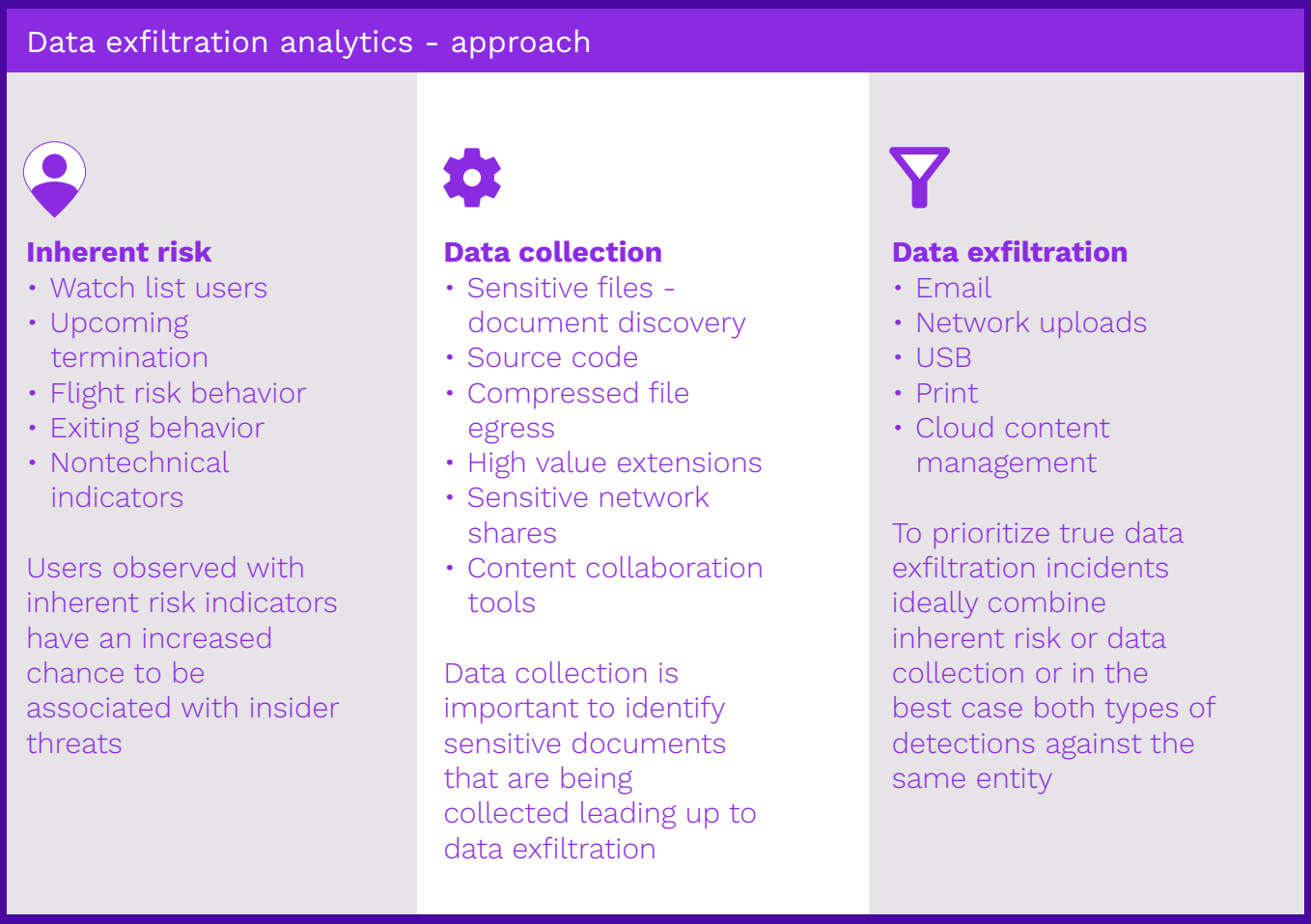
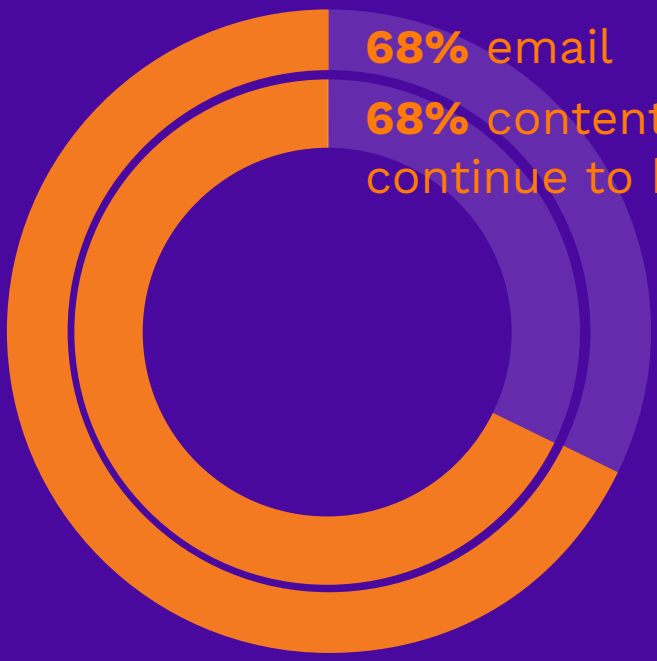


Figure 1: Analyzing for data exfiltration includes watching for inherent risk and collecting data to prioritize incidents for investigation.

Collect data from these key sources to help identify data exfiltration or loss

After identifying the inherent risk indicators, next you should ensure your organization is collecting the most important data sources into your detection and response platform. Data collection encompasses all actions related to a user or entity observed accessing files, shares, or even network locations they haven't accessed before—in addition to any abnormal downloading of large amounts of data. We recommend including data collected from content management repositories and from network shares via network sources or Windows Security events.

Collect data from common egress vectors for data exfiltration. Common egress vectors include email, USB devices, network uploads, or uploads to an external collaboration platform including external, non-business accounts via a content management system (CMS). Often users might not be aware of the acceptable use policy, so emails involving personal files and data might be observed passing over the network. Users sending personal emails to a non-business freemail domain increase the number of alerts insider threat analysts have to review however we've observed email as one of the top egress vectors so it's important to combine the inherent risk indicators and data collection so you don't chase false positives like tax documents or personal photos.



68% email

68% content management products continue to be top egress vectors.

Recommended data sets

Securonix recommends these data sets for the widest insider threat detection coverage:

- CASB
- Data loss prevention/ network DLP
- Print/removable media
- Email/email security
- Content management system (CMS
- Web proxy

Security professionals should include the data feeds located in Figure 2 for their detection and response solution to monitor for behavior changes inherent to data exfiltration. These feeds help to provide a more comprehensive picture of non-technical inherent risks to improve insider threat detection:

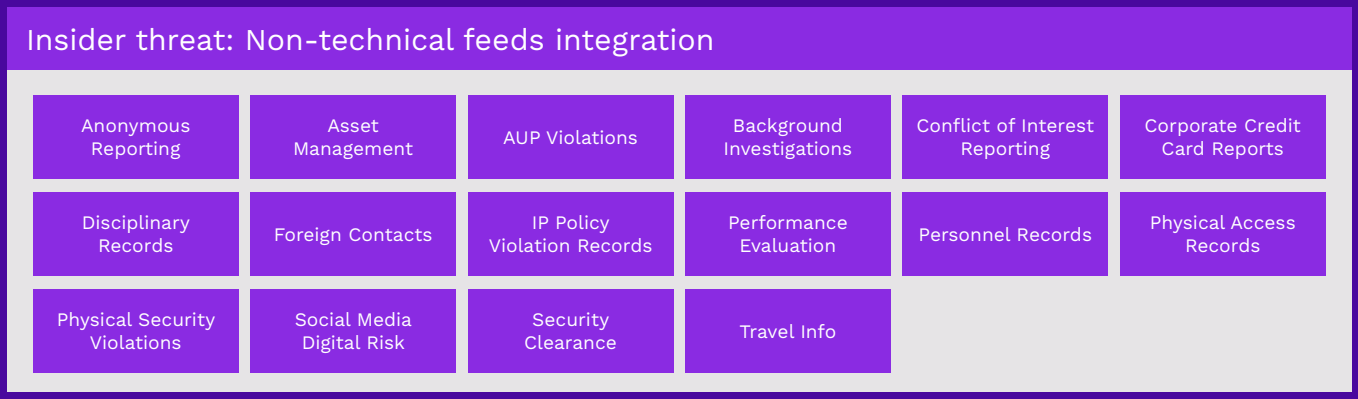


Figure 2: Integrating non-technical feeds for insider threat detection

Monitoring for intentional/ unintentional data exfiltration and loss

Monitoring for activity surrounding the deletion of critical files, objects, and accounts might reveal indicators of sabotage, although such activities usually amount to routine activity. Nevertheless, identifying trends pertaining to data deletion frequency, along with users observed having known inherent risk indicators (e.g., poor performance, flight, exiting risk) yield the best results.

Insider threat-related policies encompass a range of data sources. Several use cases detect core scenarios—primarily potential insiders leveraging their access and knowledge. Nearly 59% of the sample data set ingested a key sabotage data source (cloud application audit) into their SIEM; 60% ingested two (email security and content management system). All provide valuable insight into exfiltration, aggregation, inherent risk, and sabotage.

Cloud application security brokers (CASB) have the most policies of any insider threat-related data source and exfiltration-related policies. However, only 13% are ingesting that data source into their SIEM, thus identifying an important insider threat gap related to exfiltration visibility.

Observations of insider threats from the trenches

We did not see a significant shift in the types of alerts triaged in the past 12 months overall. Insiders continue to use or misuse business collaboration services. Securonix observed critical insider threats involving cloud data exfiltration, but with a decline in the use of traditional egress channels such as USB.

We've broken out two observations from our research below to provide insight into common investigated threats.

Data Exfiltration Scenario #1

Prior to termination, an employee shared documents with their personal freemail account and created a backdoor. No activity was observed until the employee was terminated. A month later the freemail account suddenly became active and started downloading sensitive data. In this example, data was directly shared with an external domain.

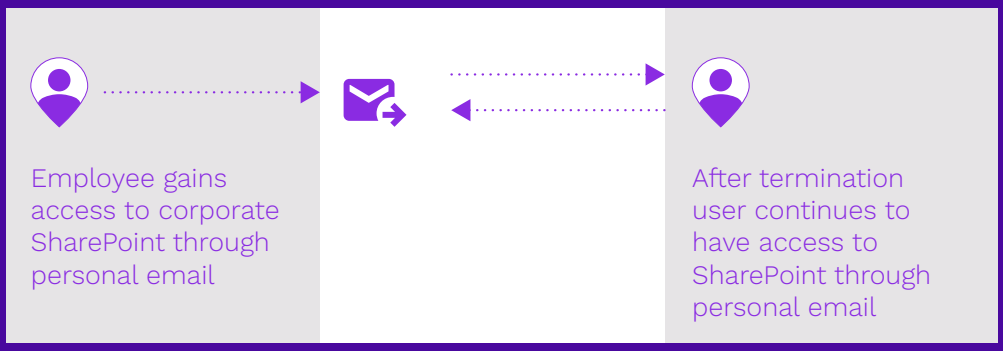


Figure 3: A user shares material from the corporate SharePoint to a freemail account.

Data Exfiltration Scenario #2

Monitoring outbound email account activity is noisy with many alerts. To reduce the volume of alerts, Securonix monitored for users shown to have an intent to leave an organization by visiting job search websites—some even having applied to jobs through the corporate network. One user was slowly collecting sensitive data from critical network shares. Ultimately, they emailed that data to personal email accounts. We observed this single account performing activity on the web proxy (flight risk behavior), firewall (data aggregated from SMB ports) and email (data exfiltration using personal email accounts).

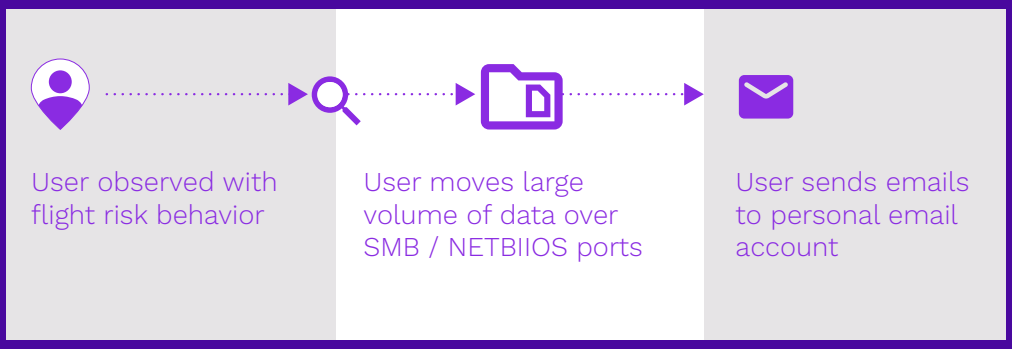


Figure 4: A user visits a job site over the corporate network before sending data to a personal email account.

Add context to more efficiently detect data exfiltration

With the advent of cloud migration, traditional egress vectors such as USB are used less frequently. While platforms such as the Google Docs Editors suite have improved workforce collaboration, they have also increased the ease with which data exfiltration can occur.

Most organizations field a large number of alerts related to users sending emails to a freemail domain, or uploading personal documents and images to a shared personal drive. While such action does not always indicate a true positive, adding context to aggregated data that leads to exfiltration via email or network uploads yields better results. Correlating the same document sizes aggregated and exfiltrated against the same entity has helped to significantly reduce alert noise and highlight real data exfiltration cases.

The more robust an organization's data classification, the better it can detect insider threats with higher precision. Continuously monitoring watchlisted users with context from non-technical indicators aids insider threat detection.

Data source coverage

CASB solutions provide a large range of telemetry to help detect aggregation and exfiltration scenarios. Yet a very small subset of customers (<13%) are ingesting these logs into the SIEM calling out the need for enhanced telemetry to detect scenarios around insider threat in the cloud. This results in a possible coverage gap that 60% of the sample addresses through ingesting CMS logs, DLP solutions, and next-generation layer 7 devices (e.g., proxies, firewalls) that provide visibility for data moving within the cloud platform realm.

% Ingesting insider threat related data sources:

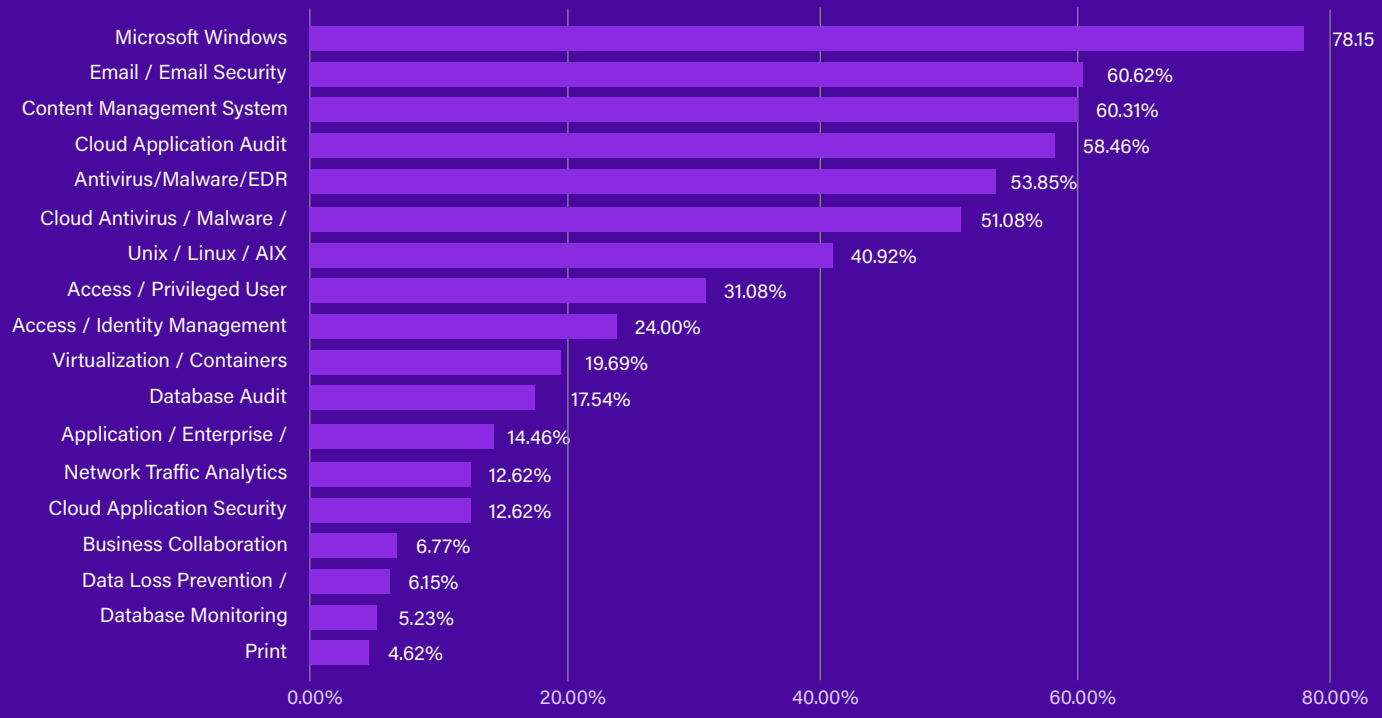


Table 2: The top insider threat related data sources ingested, include 78% of the data set ingesting Microsoft Windows, followed by email security and content management system at over 60% ingestion.

Despite CASB covering most aggregation and exfiltration policies of any data source, only 12% ingest this data into their SIEM.

Exfiltration had (by far) the most coverage of any insider threat, encompassing 10 data sources. Most of the identified exfiltration scenarios were related to documents made public— highlighting issues with consistent cloud controls. Other traditional exfiltration means (e.g., email) were also prominent—specifically emails to non-business domains, email forwards, and emails to personal accounts (identified via fuzzy-logic pattern matching).

Average % with enabled core focus policies

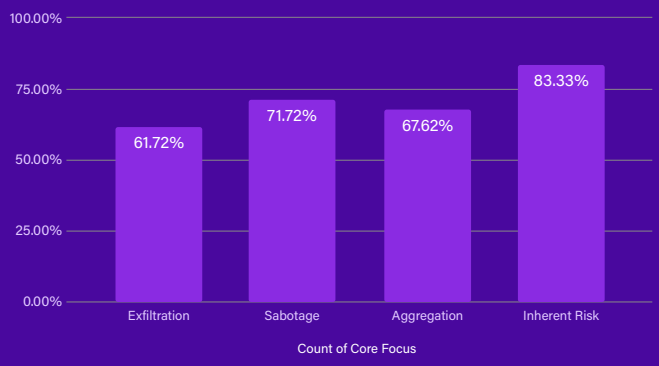


Table 3: Insider threat core focus policies identify potential internal threats that leverage access and knowledge. Our data sample demonstrates an average of 83% of the sample set with inherent risk policies enabled in their SIEM, closely followed by 71% of sabotage policies and 67% aggregation policies.

Content management systems are the leading data source for recognizing sabotage-related activities. By consuming CMS event logs, 60% of environments reflect that detection priority.

Inherent risk helps identify potential insider threats by understanding a user's access and knowledge to potentially harm an organization. With 60% of environments ingesting some form of email security logs, the ability to detect activities such as flight risk and job exiting behavior is crucial for remaining secure against insider threat activities.

Insider threats % of core focus data sources ingested

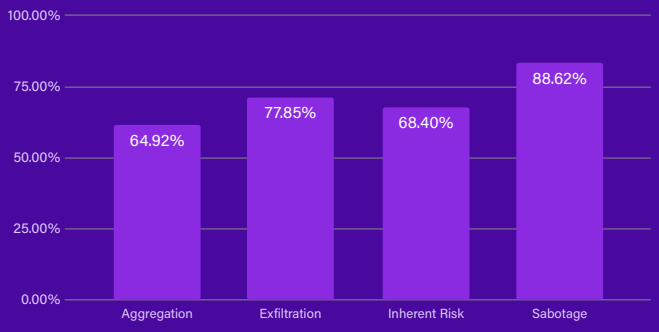


Table 4: Leading at 88%, the percentage of sabotage-related data sources that are ingested in the data set provide significant coverage for detecting related activities. Exfiltration and inherent risk data sources follow at 77.85% and 68.40%, with 64.92% having aggregation-related data sources ingested by their SIEM.

Insider threat key takeaways

Securonix customers were well covered in detecting flight risk and exiting risk behavior by way of email. Inherent risk-aligned use cases were enabled in roughly 85% of available customer environments. Considering 68% of them ingest some form of email or email security logs, the ability of UEBA to leverage related use cases to proactively identify potential insider threats is a boon for an establishment.

Organizations should add additional inherent risk indicators, such as watchlists related to those users exhibiting poor performance and those who should be closely monitored.

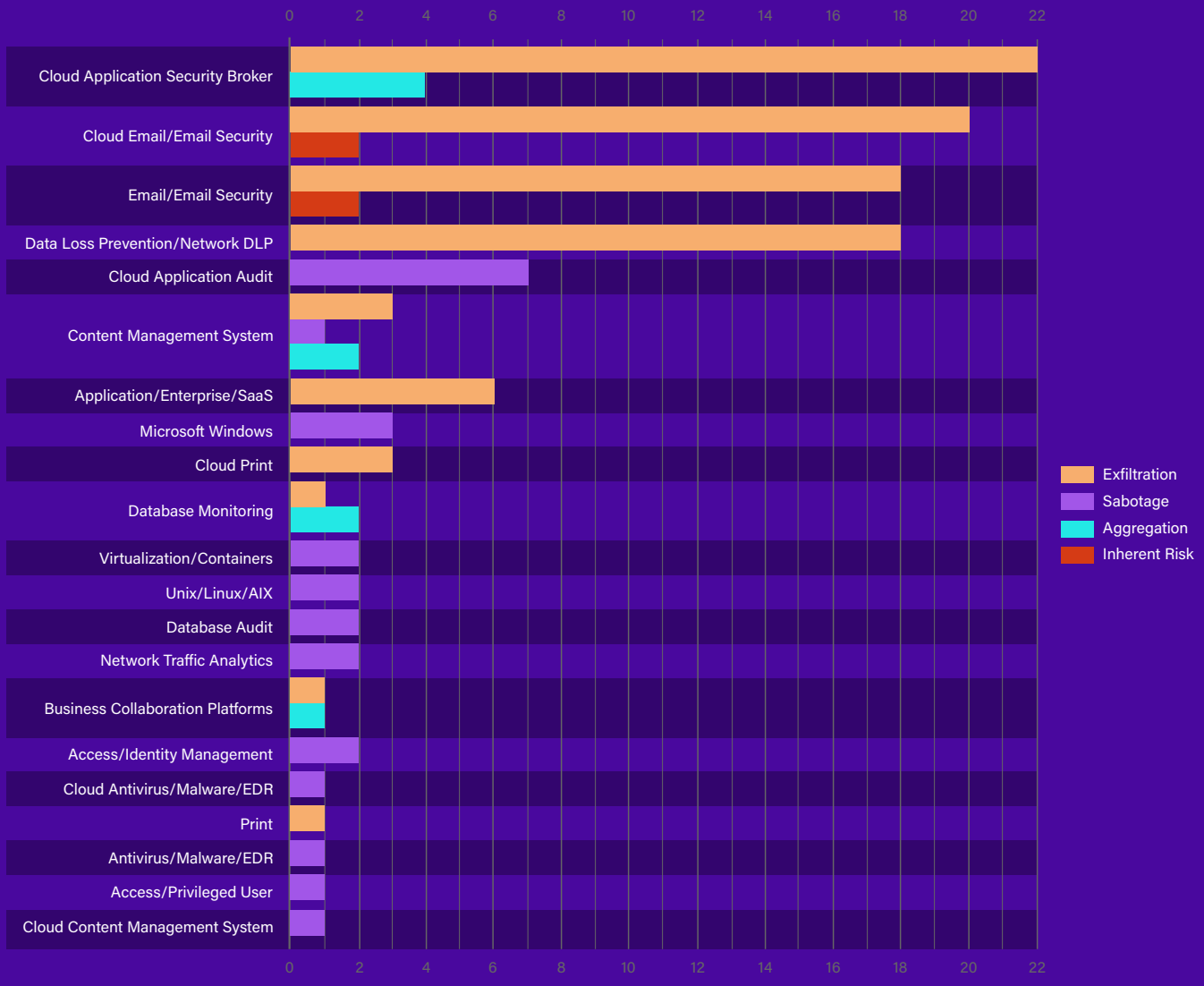
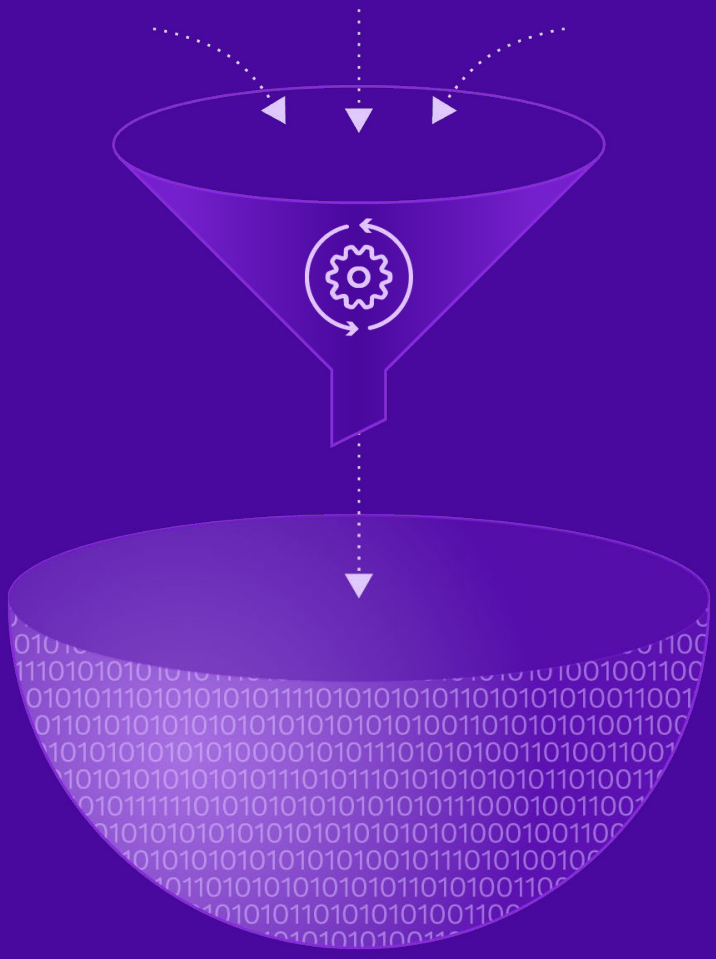
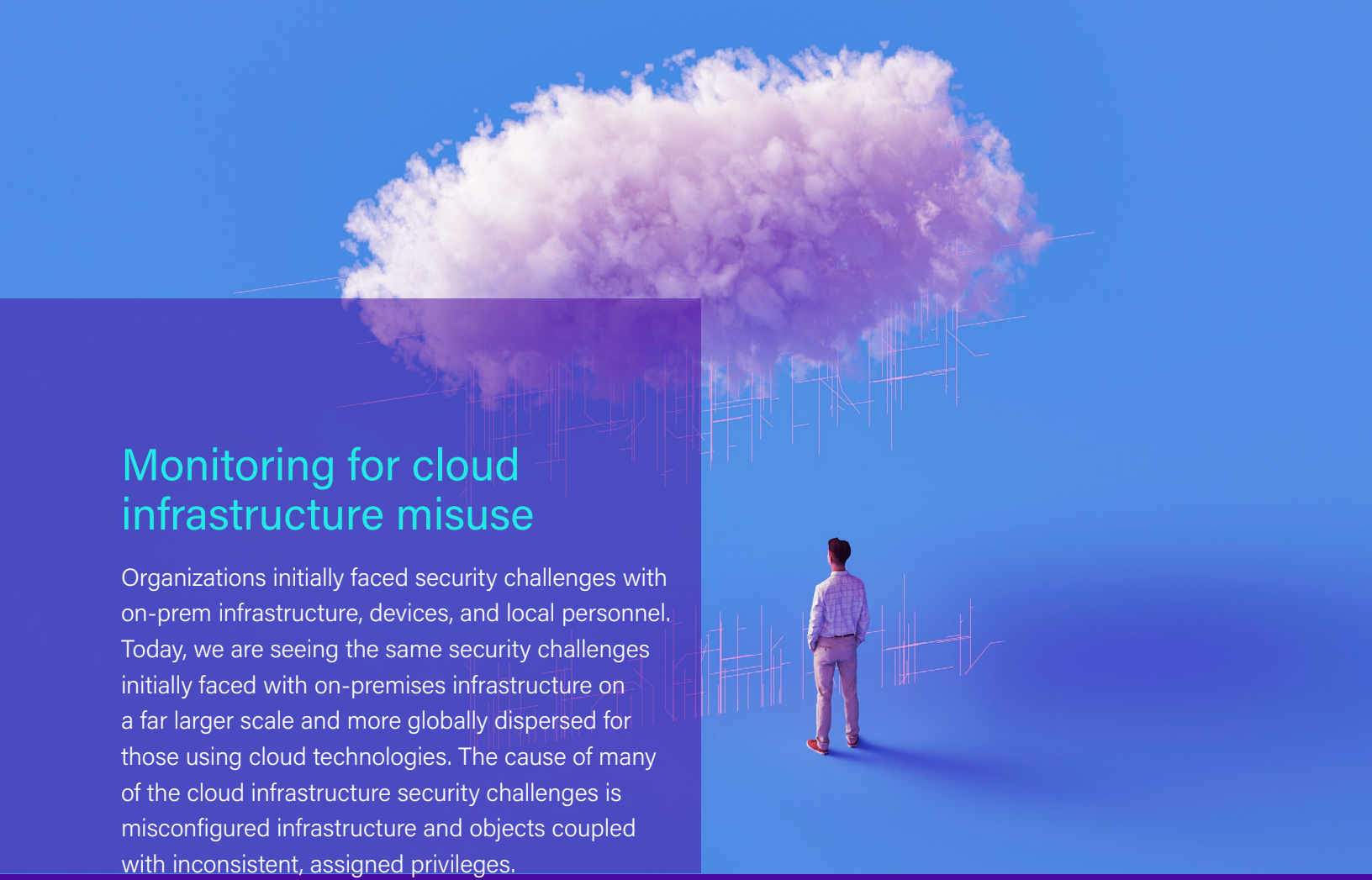


Table 5: The count of insider threat related policies separated by core focus areas are as follows; cloud application security broker leads the way with 26 overall policies, 22 of which encompass exfiltration and four involving aggregation. Email security and data loss prevention closely follow with 18 policies covering exfiltration.

Top data aggregation policies included information held in databases and content management systems. These policies emphasize the importance of establishing a baseline via machine learning for your entities and users; this aids in assessing what is normal regarding the type and amount of data users typically access/download. By itself, this data collection indicator would be a precursor to exfiltration; it should be combined with exfiltration/inherent risk-based indicators.

Email and related security coverage led the way for exfiltration policy coverage, with 68% of the sample ingesting the data source—demonstrating its overall usefulness for insider threat detection. Despite DLP and CASB accounting for more coverage holistically, they are ingested by less than a third of the data set. This identifies clear priorities for organizations seeking insights into potential exfiltration events.





Monitoring for cloud infrastructure misuse

Organizations initially faced security challenges with on-prem infrastructure, devices, and local personnel. Today, we are seeing the same security challenges initially faced with on-premises infrastructure on a far larger scale and more globally dispersed for those using cloud technologies. The cause of many of the cloud infrastructure security challenges is misconfigured infrastructure and objects coupled with inconsistent, assigned privileges.

Enterprises are learning to balance the ease of cloud service and platform with required security controls and policies. Controls that are too strict defeat all the benefits of migrating to the cloud, while those that are too loose enable attackers or even unintentional insiders to potentially disrupt operations.

Important cloud infrastructure controls are either inconsistent or not generally available. We advise security professionals to monitor users for inherent risk indicators because they can potentially open controls or unintentionally update an object's settings causing security challenges. Given cloud capabilities such as auto scalability, elasticity, and automation, minor misconfigurations could come at a great cost related to service unavailability or increased expenses.

Securonix Threat Labs observed an increase in nation state actors misusing public cloud infrastructure services, thereby evading defenses (e.g., known whitelists). The ease with which cloud services can be leveraged is a double-edged sword, with nation states finding it easier to set up an attack infrastructure on major cloud platforms.

Detecting cloud threats begins with monitoring insufficient IAM. Alert trends indicate misconfigured or inadequate access controls are increasingly responsible for cloud compromise.

Comprised of many granular detections and scenarios, threat types related to cloud infrastructure can be broadly categorized into the following categories:

- **Insufficient IAM** – Insufficient identity and access management (IAM) relates to accounts being misused or compromised. This includes authentication anomalies such as multifactor authentication (MFA) being disabled and users misusing or elevating their privileges and roles.
- **Misusing controls** – Examples of cloud infrastructure problems include:
  - Abuse of controls by modifying policies and/or access control lists (ACLs)
  - Unapproved operations on key vaults that manage encryption for all cloud services
  - Discovery of accounts and services that can be misused and abused
- **Impact** – Service disruption, data loss, and/or data breach can all adversely affect your organization. Deletion or modification of encryption keys can result in data loss. A breach might mean data becomes available to anyone across the internet. Or other abuse might occur, such as crypto mining that strains systems and runs up costs.

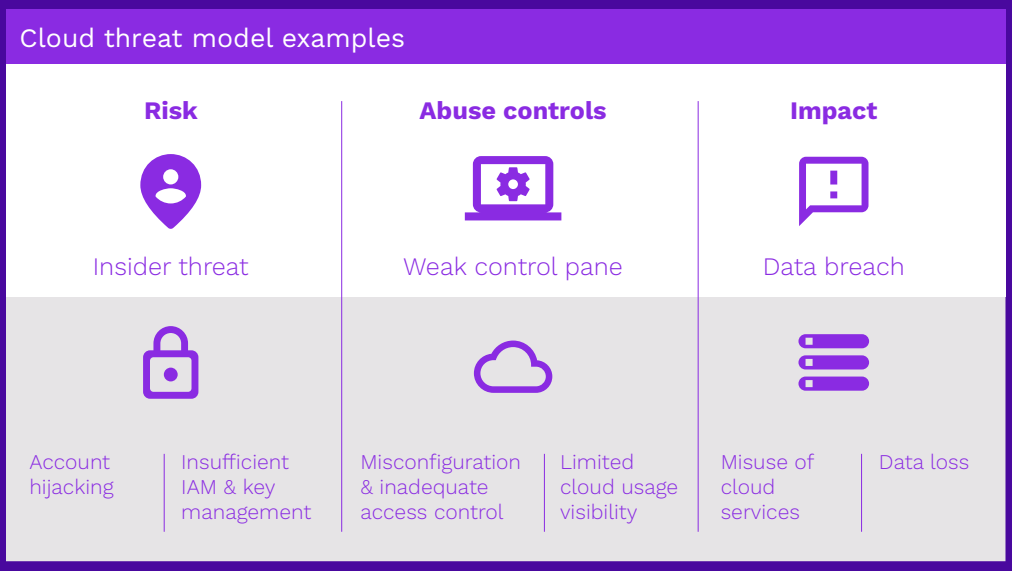


Figure 5: An example of a cloud threat model or kill chain that can be considered by grouping various threat scenarios as described by CSA's egregious 11.

Leveraging the right telemetry from cloud services and applications via audit trail is extremely important not only to help proactively detect security incidents but also to help identify and improve on the cost associated with these services being misused. For example, compromising or abusing the key management console of a cloud service provider would provide an attacker or malicious insider complete control over all cloud services thereby rendering other

defenses moot. Account hijacking either via stolen/compromised credentials or via phishing could be another initial access vector. Once an adversary has sufficient rights/privileges, they can misuse or abuse the cloud infrastructure or any cloud object by modifying existing controls and configurations.

Recommended data sets for cloud infrastructure security

The following data sets provide the widest threat detection coverage within your cloud infrastructure.

- Cloud services/applications – Includes all data related to monitoring (including adding, updating, or deleting users/roles/objects, in addition to the cloud platform itself)
- Access/identity management

Observations of cloud infrastructure misuse/abuse from the trenches

The Securonix Threat Labs team observed one example of an account that mistakenly modified the permissions for an Amazon RDS instance, making it accessible for configuration by any internet user. The change allowed traffic from any IP address (0.0.0.0/0) to any port (0-65535). This unintentional error ultimately caused service disruption, where an attacker deleted records after gaining system access.

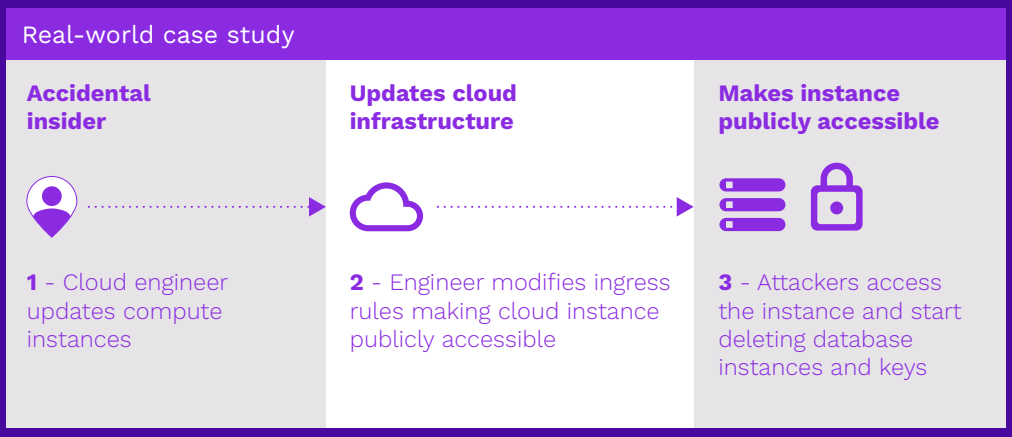


Figure 6: An insider accidentally updates the cloud infrastructure making the instance publicly available.

We also observed an account having elevated privileges modified access rights to an object, rendering it publicly accessible seen in Figure 6. And a third example revealed a misconfigured storage object that allowed all users to access data stored on it.

Cloud infrastructure key takeaways

Most actionable use cases relate to accounts and IAM activity, thus reiterating the attention that should be given to insufficient or inconsistent IAM visibility and controls.

Consequently, cloud content management, cloud services, cloud authorization, and MS Office 365 have the highest percentage of tenants with threats. This re-emphasizes the importance of cloud-centric security platforms and audit capabilities.

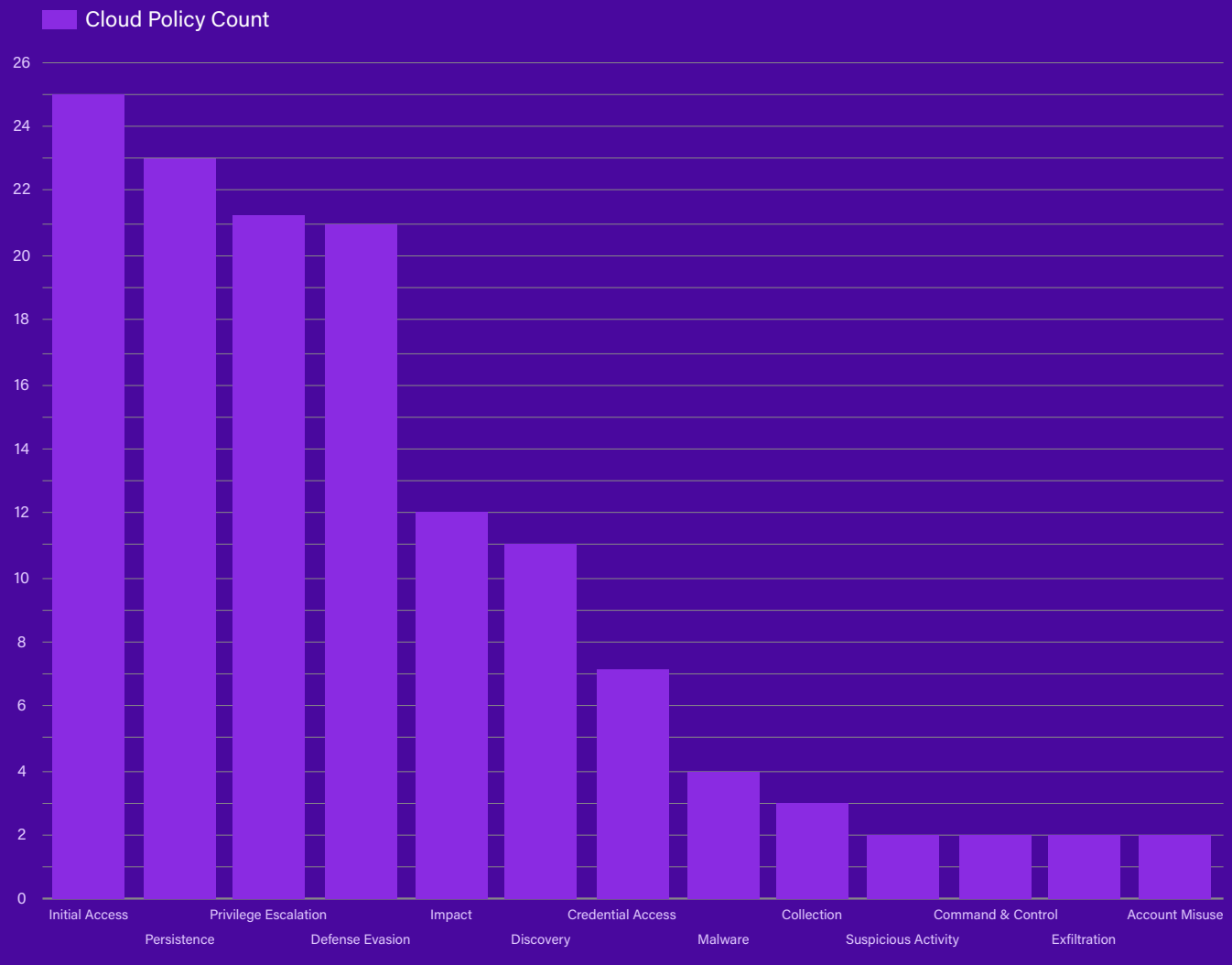


Table 6: This graph represents the count of cloud policies covering MITRE ATT&CK tactics enabled by our sample. The most prominent cloud infrastructure coverage includes 25 policies for initial access, 23 for persistence, and 21 for both privilege escalation and defense evasion.

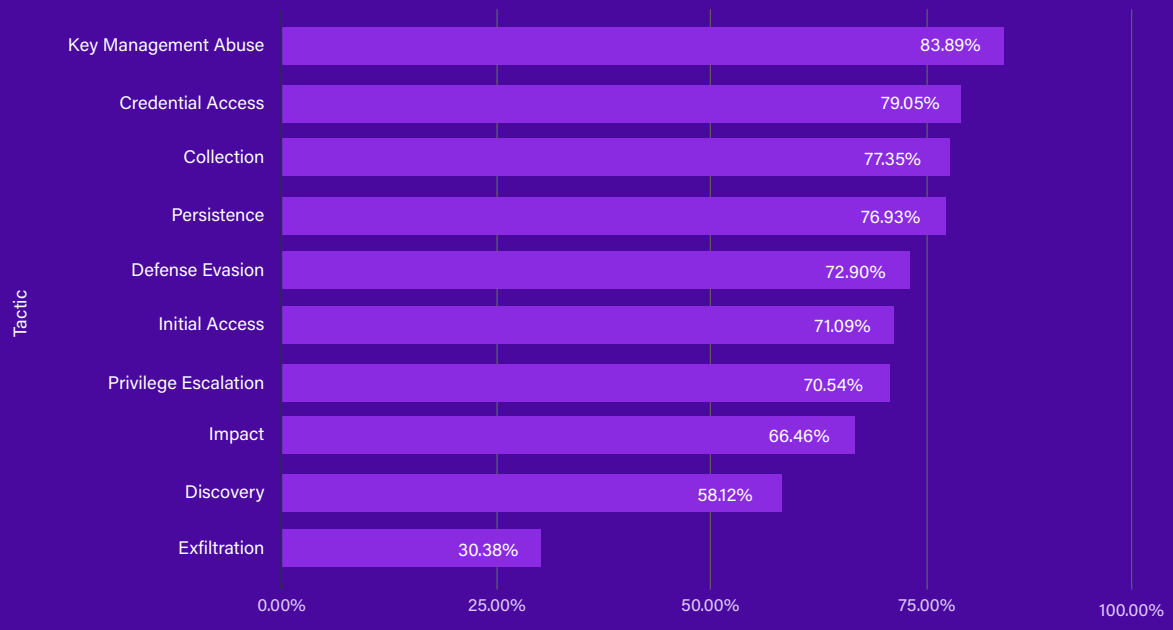


Table 7: This graph represents the average percentage of the data set that has enabled key cloud policies against MITRE ATT&CK tactics. Nearly 84% of the sample set have relevant key management abuse policies enabled, with credential access (79%), collection (77%), and persistence (76%) closely following.

More than 80% of customers with suspicious activity-related policies enabled demonstrate a higher success rate in detecting related threats. More than 70% have initial access policies and nearly 80% have persistence policies enabled.

Cloud services or infrastructure audit data sources encompass 13 MITRE ATT&CK tactics. These MITRE ATT&CK tactics were identified by 67% of environments ingesting key events required to detect cloud infrastructure threats across the framework. Cloud services or infrastructure audit data had the third-highest ingestion rate overall across the data set.

Despite access/identity management covering six ATT&CK tactics (nearly the majority of brute force and account manipulation detection policies), only 24% of environments ingest the data source. This data gap in access/identity management exacerbates the potential for creating detection gaps in credential access and persistence.

Referencing Table 7, there is an average of nearly 70% of policies enabled across key cloud ATT&CK tactics in our data set. This high percentage reflects the need for organizations to provide for strong cloud visibility as their infrastructure migrates from on-premises devices to the cloud.

Ransomware: Preempting and detecting sophisticated attacks

Most organizations attempt to detect threats during early attack phases, before it leads to data being exfiltrated, lost, encrypted, and/or deleted. For early detection, robust endpoint and network data telemetry are recommended to detect threats such as ransomware. In fact, around 70% of MITRE ATT&CK techniques, tactics, and procedures (TTPs) require some type of endpoint telemetry. In the absence of raw EDR data, an organization would need to rely completely on signatures and detections that their EDR or antivirus solution provides.

As we observed with SolarWinds and other past incidents, there is a growing need to collect data to proactively investigate and detect threats. Correlating alerts from various technologies such as single sign-on (SSO), networks, and endpoints against the same entity helps prioritize and detect meaningful alerts.

A larger attack surface with higher value assets available in hybrid work environments presents an attractive landscape for nation state threat actors—or even malicious insiders who can circumvent existing controls and defenses. Availability of compromised user credentials as well as phishing continue to be the primary vectors for gaining a foothold. That said, nearly 40% of the sample set are not ingesting email security logs, thereby making it more difficult to identify scenarios such as typosquatted domains and business email compromise. Using MITRE ATT&CK framework techniques, ransomware attacks can be detected by monitoring raw EDR and network traffic. Collecting raw EDR or network traffic analytics alone improves detection of more than 70% of methods described by MITRE ATT&CK.

Observations of preemptive ransomware detection from the trenches

With organizations migrating to hybrid and remote work environments, detecting initial indicators of account compromise via SSO and VPN authentication events is extremely important.

Preemptive Ransomware Detection - Scenario #1

Authenticating from multiple geolocations indicates account sharing and compromise. In one example (shown in Figure 7), a user tried to log in from an unusual geolocation at the same time as their primary US location. The user then anomalously requested a large number of Kerberos service tickets. A combination of suspicious authentication patterns and multiple service tickets accessed confirmed that the compromised privileged account was being misused. Combining the two alerts from authentication events and Windows Kerberos service ticket requests preemptively prevented a larger issue and ensured faster detection. The user was then attempting to laterally propagate to multiple systems which confirmed the activity to be malicious.

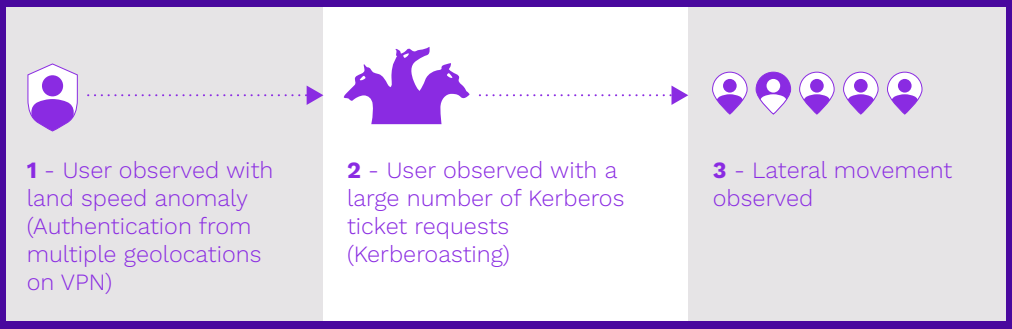


Figure 7: A user logs in from multiple locations in rapid succession and sends several helpdesk tickets indicating lateral movement.

By preemptively detecting ransomware, organizations can aim to detect scenarios before files are encrypted. Although raw EDR events provide more than 70% coverage of related MITRE ATT&CK techniques, just 25% have ingested the telemetry into their SIEM.

Preemptive Ransomware Detection - Scenario #2

Another scenario included a compromised HR business email containing a malicious Microsoft Word payload being sent to a specific set of users, seen in Figure 8. When some users downloaded and opened the document, it spawned additional processes/Python scripts that attempted to disable firewall rules on the endpoint. Because the organization combined raw EDR telemetry with inbound email logs, the attack was preemptively detected and further impact was prevented.

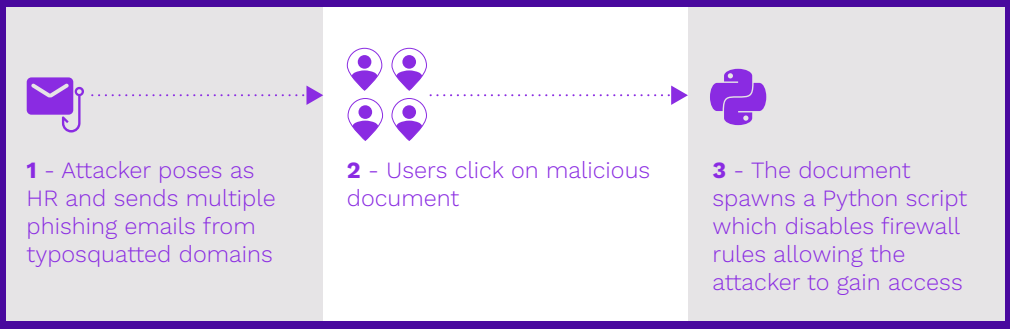


Figure 8: In this scenario, preemptive ransomware detection recognizes multiple phishing emails from typosquatted domains masquerading as HR.

Organizations should strive to preemptively detect ransomware and malware while the attack propagates through the kill chain. Encompassing 70% of MITRE ATT&CK techniques, such detection requires raw EDR or network traffic analytics to be collected. Yet only 25% of our data set store and log these in a SIEM. The lack of this information requires other log telemetry to detect potentially weaker signals.

Average % of ransomware data sources ingested

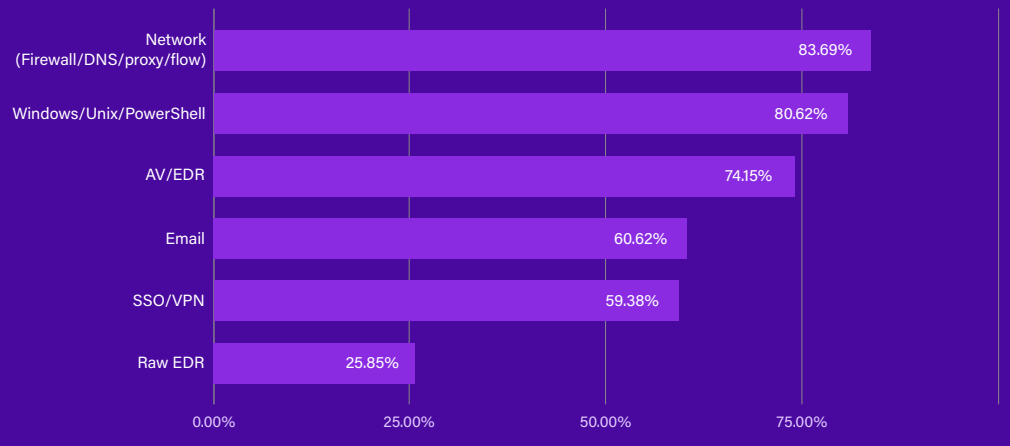


Table 8: Network, Windows and antivirus and EDR logs lead the data sources ingested for ransomware detection coverage.

Trends and egress vectors for ransomware

Next we look at trends and primary vectors such as phishing and log sources for ransomware coverage and detection.

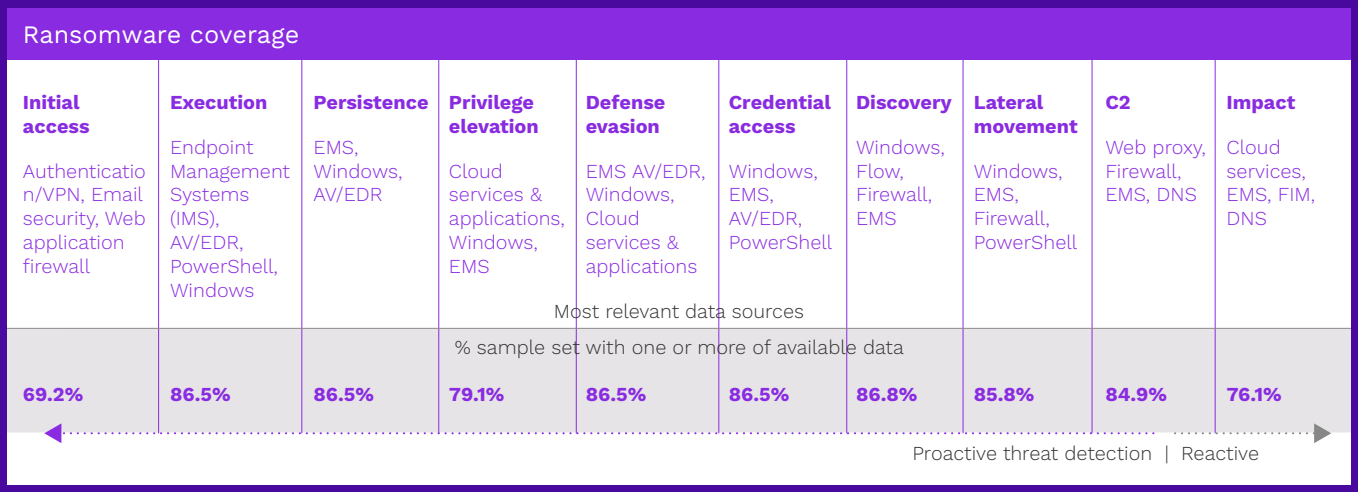


Figure 9: Proactive threat detection monitors for tactics that comprise the ransomware kill chain.

For proactive detection of ransomware, recognizing privilege escalation is critical. Our research found that 33% of privilege escalation policy coverage involves cloud services logs, 67% of customers have responded to that by ingesting these logs into their SIEM (the third-highest data source ingested).

For initial access policies shown in Figure 9, the top data sources include VPN authentication, email security, and web application firewall. 47.8% of the sample set are ingesting at least one of these data sources. For execution policies, top data sources include raw EDR, AV/PowerShell, Microsoft Windows, and PowerShell. Fifty percent of the sample set are ingesting at least one of these.

The top four ingested data sources are next-generation firewall (NGFW) and Windows, being leveraged by 78% of customers. They are closely followed by cloud services at 67%, and 60% ingesting content management system logs.

Windows Security events can be leveraged across more tactics but require additional logging telemetry—including enabling advanced auditing to log command line parameters along with both parent and child processes.

Windows/Unix/PowerShell provide coverage to 70% of MITRE ATT&CK tactic coverage, with customers recognizing its usefulness in a SIEM as 78% of customers are ingesting Windows logs. However, PowerShell logging and auditing is crucial for more robust visibility into malicious activities, and only 12% of customers are ingesting these logs, demonstrating a significant gap to bridge for in-depth ransomware coverage.

Network events are an important overall data source for security programs, specifically with ransomware coverage for detecting discovery, lateral movement, command and control, and impact tactics.

Although 78% of customers ingest some form of firewall logs, just under 14% ingest flow logs, despite flow having the second-most coverage for discovery tactics. Additionally, just under 39% ingest DNS logs, a metric that needs to be increased for organizations to capture key command and control activity (e.g., DNS beaconing, persistent DNS traffic, excessive number of DNS responses).

Recommended data sets for preemptive ransomware detection

Securonix Threat Labs recommends these data sets for the widest ransomware detection coverage:

- Raw EDR (endpoint management systems – EMS)
- Microsoft Windows + PowerShell
- Antivirus/malware/EDR
- Cloud services/applications
- Firewall

Preemptive ransomware detection key takeaways

Endpoint management systems (EMS) or raw EDR telemetry have the most coverage overall with nine tactics that include persistence, credential access, execution, and defense evasion (larger than the next three data sources combined). Despite this coverage, EMS is ingested by less than 26% of the sample, highlighting the need for additional data sources to provide similar coverage.

Microsoft Windows is the second most covered tactic with seven tactics. Windows logs are only generated for system access control lists (SACLs) that have been enabled. Regarding registry modifications, it is extremely important to enable auditing for both successes and failures at a minimum, among other objects.

If you lack raw EDR telemetry, some combination of email/authentication (VPN/SSO) and network sources such as flow, firewalls, web proxy, and DNS provide decent proactive ransomware coverage.

With 14 initial (IA) policies requiring an email data source (more than any other source), the need for a strong email gateway product with email authentication (DMARC/DKIM) and SIEM detection policies is emphasized. Email authentication and SIEM detections help enable an organization to be more proactive in threat detection with respect initial access stages of MITRE.

Phishing (typosquatted domains/business email compromise) accounts for almost half of top policy violations related to initial access.

Command and scripting threats account for six of top 10 execution IA policies. Adversaries continue to abuse interpreters across platforms to execute various payloads and scripts (via PowerShell, Python, JavaScript, and Windows Command Shell, among others).

IoT and OT: Navigating virtual and physical security landscapes

By **Edward Rhyne** and **Nick Evancich**

The consequences of an IoT security breach can be highly damaging because it affects both virtual and physical systems. The volume and diversity of things that comprise IoT mean it contains a considerable amount of user data.

The adoption rate of IoT devices continues to be extremely high as an increasing number of devices are connected to the internet. Cisco predicts 4.8 ZB of internet traffic by 2022, and IP traffic is expected to triple in two years, thus extending the attack surface for adversaries. Being connected further provides an attractive target and opportunity for cybercriminals—especially insiders who have access to operational processes and systems.

Unique to IoT and OT, cyber-physical system (CPS) environments, are industrial control and management systems. They are generally deployed on a large scale, allowing the monitoring, management and administration of critical infrastructures in various fields such as health, transport, nuclear, electricity, gas, and water.

Internet and ubiquitous networks have changed how CPS communicates. In this context, IoT success is attributed to advancements in hardware and communications technologies.

The following are seven characteristics of IoT and OT that can be vulnerable and exploited by cybercriminals.

- **Deficient physical security** – The majority of IoT devices operate autonomously in unattended environments. With little effort, an adversary might obtain unauthorized physical access to such devices and thus take control. Consequently, an attacker could cause physical damage to the devices, possibly unveiling employed cryptographic schemes, replicating their firmware using malicious nodes, or simply corrupting their control or cyber data.
- **Limited energy capacity** – IoT devices characteristically have limited energy and do not necessarily possess the technology or means to automatically renew it. An attacker might drain stored energy by generating a flood of legitimate or corrupted messages, rendering devices unavailable for valid processes or users.
- **Inadequate authentication** – The unique constraints within the context of the IoT paradigm (e.g., limited energy, computational power) challenge the implementation of complex authentication mechanisms. To this end, an attacker might exploit ineffective authentication approaches to append spoofed malicious nodes or violate data integrity, thus intruding on IoT devices and network communications. Under such circumstances, the exchanged and employed authentication keys are also at risk of being lost, destroyed, or corrupted. Sophisticated (or otherwise effective) authentication algorithms become insufficient when keys are not securely stored or transmitted.
- **Improper encryption** – Data protection is of paramount importance in IoT realms, especially those operating in critical CPS (e.g., power utilities, manufacturing plants, building automation). Encryption is a more effective means for storing and transmitting data in a way that only authorized users can use it. As the strength of cryptosystems depends on their designed algorithms, IoT resource limitations affect the robustness, efficiency, and efficacy of the latter. Given this, an attacker might be able to circumvent deployed encryption techniques to reveal sensitive information or control operations with little effort.

- **Unnecessary open ports** – Various IoT devices have open ports while running vulnerable services, permitting an attacker to connect and exploit a plethora of vulnerabilities.
- **Insufficient access control** – Strong credential management can protect IoT devices and data from unauthorized access. The majority of such devices in conjunction with their cloud management solutions do not force a password of sufficient complexity. And devices do not request a change of default user credentials after installation. Moreover, most of the users have elevated permissions. Hence, an adversary could gain unauthorized access to a device, thereby threatening data and potentially the entire system.
- **Improper patch management capabilities** – IoT operating systems and embedded firmware/software should be regularly patched to minimize attack vectors and augment their functional capabilities. Numerous cases report that many organizations either do not recurrently maintain security patches or do not have automated patch updating in place. When available update mechanisms lack integrity guarantees, rendering them susceptible to being maliciously modified and applied at large.

Aggregating and analyzing IoT and OT logs can provide analysts with clues regarding anomalies and behavioral changes they can match with potential techniques. The ability to link and correlate alerts provides them with a better understanding of what is transpiring in an environment, thereby assisting them in preventing adversaries from gaining access.

Conclusion

The rise in the number of threats globally poses a challenging landscape for organizations and the public. A combination of persistent insider threats, cloud infrastructure misuse/abuse, and sophisticated nation state–sponsored attacks has fostered a riskier environment.

Given the extensible environment of corporate networks and the remote workforce, exploitation through ransomware is on the rise. It is important to review any gaps in telemetry and detection coverage to improve faster reaction times and accuracy before data loss/exfiltration is realized.

The potential vulnerability of IoT and OT environments pose a growing area of concern. Collecting key data sources and monitoring for unusual behavior is a critical approach for security teams to secure data. OT security must be combined with traditional IT security for robust threat detection.

Securonix collaborates closely with many partners with many security professionals globally to detect and respond to threats. If you are interested in learning more about our solutions, please request a demo today.

References

National Vulnerability Database (NVD) | NIST

Securonix Autonomous Threat Sweeper

Top Threats to Cloud Computing: Egregious Eleven Deep Dive | CSA

Audit Registry (Windows 10) - Windows security

Cisco Visual Networking Index: Forecast and Trends, 2017–2022

Get in touch with Securonix

securonix

For more information visit securonix.com, info@securonix.com

Follow us @securonix