VECTRA
SECURITY THAT THINKS

2020 Spotlight Report

Does privileged access equal trusted access?

VECTRA
SECURITY THAT THINKS

TABLE OF CONTENTS

Vectra research shows that privileged access from unknown hosts occurs inside every industry, leading to unintended exposure of critical systems. Yet these privileged accounts rarely receive direct oversight or technical control of how they are used, even when privileged access management tools are in place. It is this lack of oversight or understanding of how privileged accounts are being used that creates the operational and financial risk for organizations. If used improperly, privileged accounts have the power to cause much damage, including data theft, espionage, sabotage, or ransom.

Why does observing how privileged access is used (and abused) matter?

Privileged access is a key part of lateral movement in cyberattacks because it leads to the most valuable capabilities and information because privileged accounts have the widest range of access to critical information. Adversaries leverage privileged accounts to gain unauthorized access using multiple techniques, ranging from stolen credentials, protocol abuse, malware, phishing, or merely guessing at simple and default account names and passwords.

Then there is sometimes case of misuse by an employee who intentionally causes damage or steals data. Or problems as simple as an authorized employee making configuration mistakes that exposes accounts or systems.

Adversaries and security practitioners are both aware of the exposure and risk of privileged access. A recent report from Gartner reveals privileged access as the top priority among security practitioners. Additionally, Forrester estimates that 80 percent of security breaches involve privileged accounts.

Yet nearly every breach involves some form of privilege access abuse.

Exploiting privileged access in the real world

Capital One was a victim of privileged access from an unauthorized system.

The simple misconfiguration of a web application firewall (WAF) – which is designed to stop unapproved access – enabled an unauthorized person to obtain an access token that was leveraged to carry out the breach.

AWS enables organizations to issue tokens that give trusted users temporary security credentials that control access to AWS resources. Temporary security credentials work almost identically to long-term access key credentials by providing the same permissions for specific administrative actions.

A temporary token is a good way to give a user the right to perform specific tasks and it reduces the need to manage access to certain accounts. However, it runs the risk of exposing information when abused.

The misconfiguration of the Capital One WAF enabled an unauthorized person to generate a temporary AWS token that could then be used to fetch data from an AWS simple storage service (S3) bucket.

Access tokens were retrieved from the AWS Metadata API via a web application with a server-side request forgery (SSRF), which means a simple set of commands from an unknown host could make the public facing web application firewall (WAF) request commands to internal servers that should not be accessible from outside the virtual private cloud.

With full access to the web servers, the unauthorized user executed a simple script of AWS commands used for system administration. The first was the S3 list-buckets command to display the names of all the AWS S3 buckets.

This was followed by a sync command that copied 700 folders and buckets of data containing customer information to an external destination. These are AWS commands used every day by cloud administrators that manage data stored in AWS virtual private clouds (VPCs).

The challenge in detecting this type of attack is not the threat behaviors, but the data source. The attack did not use malware, was not persistent on hosts, and did not exhibit unusual network traffic. And the attacker blended in with normal cloud administrative operations. The key indicator was that the commands were executed using a privileged credential from an unusual host.

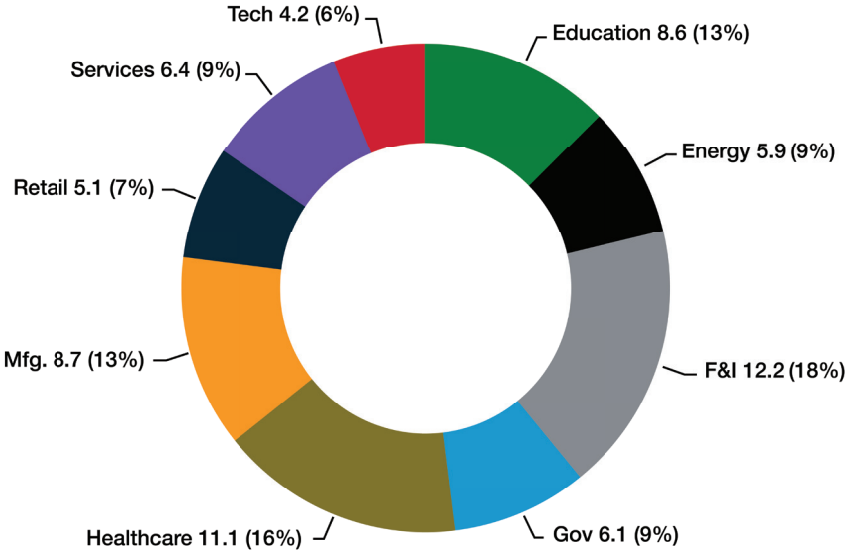
It would be easy to say Capital One should have not made this kind of mistake, but when organizations transition to the cloud, these type of mistakes and misconfigurations are unfortunately common. The “Shared Responsibility Model” is a fault here – whenever two different entities with different skill sets, operating knowledge, or even just simple incentives (operational, financial, or otherwise) are both responsible for an activity or entity, gaps will occur.

Is privileged access from an unusual host a regular problem?

By analyzing anonymized customer security metadata in the 2020 Attacker Behavior Industry Report from Vectra, trends in privileged access behaviors from July – December 2019 have been identified. This data allows us to quantify how regular certain behaviors are, both malicious and intentional.

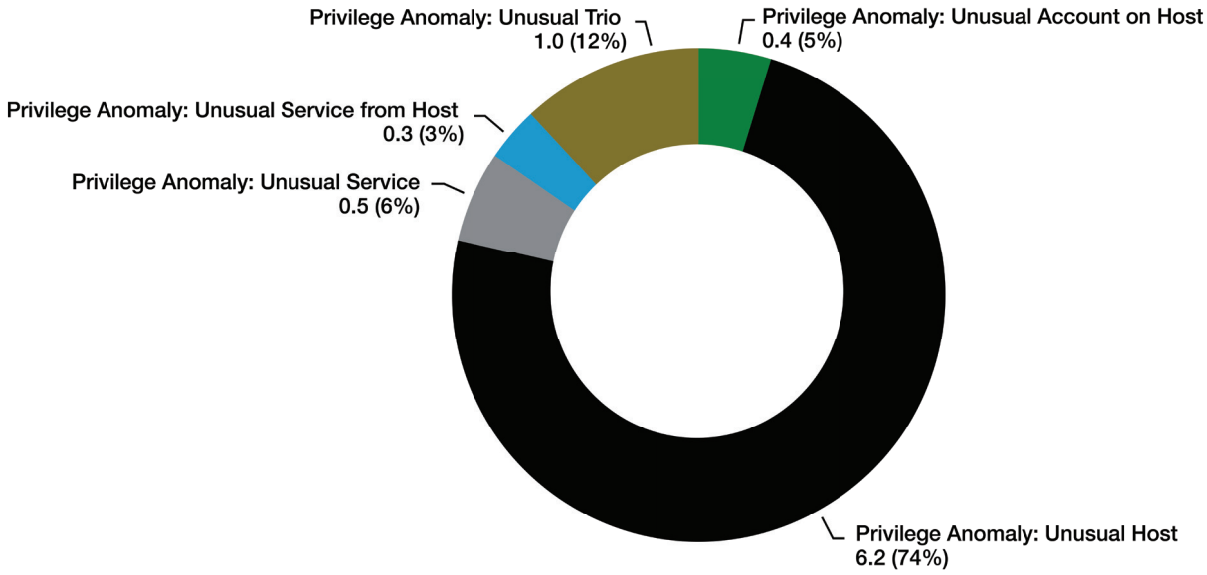
Over that six-month period from July to December 2019, 26,800 privilege access anomaly behaviors were detected by the Cognito network detection and response platform. To understand prevalence per organization, we can normalize that data to understand current trends. Throughout the rest of this report, detection counts are normalized to the number of detections per 10,000 workloads or devices to enable comparisons between organizations of different industries and sizes.

What we learned is that overall, finance and insurance, healthcare and education organizations exhibited the most privilege access anomalistic behaviors across nine different industries. These 3 industries together account for almost half (47%) of all privilege access anomaly behaviors detected.



Privilege Access Anomaly by Industry per 10k

For further analysis, when breaking down behaviors by specific type, privilege access from an unusual host proves to be the most common behavior observed, accounting for 74% of all privileged access anomaly behaviors. These are behaviors like what transpired in the Capital One breach.

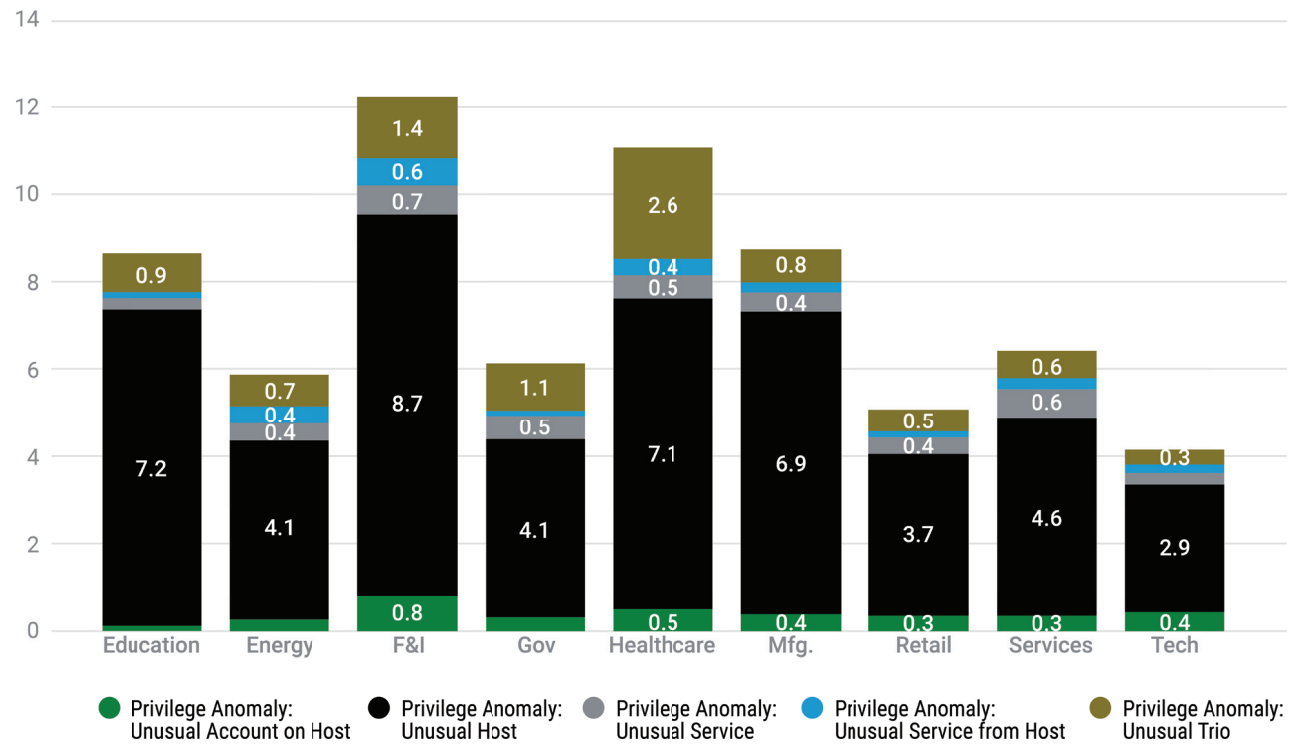


Privilege Access Anomaly by Type per 10k

Privilege access from an unusual host

Privilege access from an unusual host occurs when an account is used to access a service from a host which the account is not usually on and from which the service is not usually accessed.

There are two scenarios where this type of behavior occurs. An account is under the control of an attacker and is being used from an unusual host to connect to one or more services which are normal for the account but abnormal from the host. Or an employee or contractor with approved access to the network who consistently works from a set of hosts has been assigned a new host or has temporarily decided to work from another host.



Privilege Access Anomaly by Industry per 10k

By analyzing privilege access analytics data from the last six months of 2019 based on volume and industry, we can see the finance and insurance organizations exhibit privilege access from unusual hosts more often than any other industries as well as more often than any other privilege access anomaly behavior. Most unusual access is benign, as in it represents employees leveraging privileged access from unknown systems performing legitimate work. But the fact this type of access is allowed represents a continuing risk to financial organizations as well as every organization that does not manage where and how privilege access occurs inside the organization. It highlights a weakness in privileged access management policy and its enforcement.

Think like an attacker to stop breaches

Identifying the misuse of privilege access has largely been treated as a static problem, with approaches that are prevention-oriented or rely on manual entitlements that identify threats the moment they occur, leaving little time to properly respond. Other approaches treat all entities as of equal value and employ pattern-based techniques resulting in excessive volumes of alerts that are impossible to operationalize.

Rather than relying on the granted privilege of an entity or being agnostic to privilege, security operations needs to focus on how entities are utilizing their privileges within the network, e.g. observed privilege.

This viewpoint is like how attackers observe or infer the interactions between entities. It is imperative that defenders think in a similar fashion to their adversaries. This can occur in two parts:

- Observe the interactions between entities. Based on the behavioral interactions between entities and the sensitivity of assets that are eventually accessed, dynamically determine each entity's level of privilege. Entities with similar access patterns are grouped as peers. This can be achieved using artificial intelligence and machine learning models.
- Determine abnormalities of interactions between privileged entities. Compare a given access request to the access history to determine distance from normal group distance. Focus on the abnormalities that have security implications and consequences.

By observing privilege, we can see five specific patterns of account usage behavior.

1. An account is used to access a service from a host which the account is not usually on and from which the service is not usually accessed.
2. An account which is typically used from a specific host is accessing a service which the account has not been observed accessing from any host.
3. An account is used from a host to request access to a service where none of the pairings (account-host, account-service and host-service) are consistent with prior observed behavior.
4. A privileged account is used to access a privileged service but is doing so from a host which the account has not been observed on but where the host (using other accounts) has been seen accessing the service.
5. A privileged account is used to access a privileged service and is doing so from a host which the account has been observed on but where the host has not been seen accessing the service.

Conclusion

It is critically important to monitor cloud-native and hybrid cloud environments as well as determine how to correlate data and context from both into actionable information for security analysts. This means not just watching the hosts and the network, but also understanding how privilege access occurs across an organization between local networks, private data centers and cloud instances.

Visibility into privileged access and other attacker behaviors is dependent on the implementation of proper tools that leverage both network and cloud-specific data. Combining data sources in the cloud with network data can stitch together a powerful combination of information that can increase the likelihood of detecting the post-compromise activities before a catastrophic breach occurs.

Monitoring this access is essential because monitoring exploits only misses most modern lateral movement use cases, and taking a host-centric view exclusively gives the attackers the most noise to hide in — thus, service/account views set up more trip wires to improve detection rates.

The importance of monitoring this type of activity cannot be overstated given its prevalence in real world attacks. The use of unusual hosts for privileged access are easily the most common type of anomalistic behavior, which underscores the importance of having additional focus around accounts and services, as a strictly host-based approach gives attackers the most noise to camouflage their activities inside.

Changes to production systems can be difficult to detect. But with 360-degree visibility into the entire organization infrastructure, it is much easier to detect attacker behaviors in compromised systems and services that are clearly operating beyond the scope of what is normally observed.

Ideally, when security operations teams have solid information about expectations for that infrastructure, malicious behaviors and privilege abuse will be much easier to identify and mitigate.

To learn more about cyberattacker behaviors seen in other real-world cloud, data center and enterprise environments, read the 2020 Attacker Behavior Industry Report from Vectra.

VECTRA®
SECURITY THAT THINKS

Email info@vectra.ai www.vectra.ai