
CYBERARK
PRIVILEGED ACCESS MANAGEMENT APPLIED TO THE SOLARWINDS BREACH
solarwinds

SOLARWINDS IS CONNECTED EVERYWHERE.

Router Admin

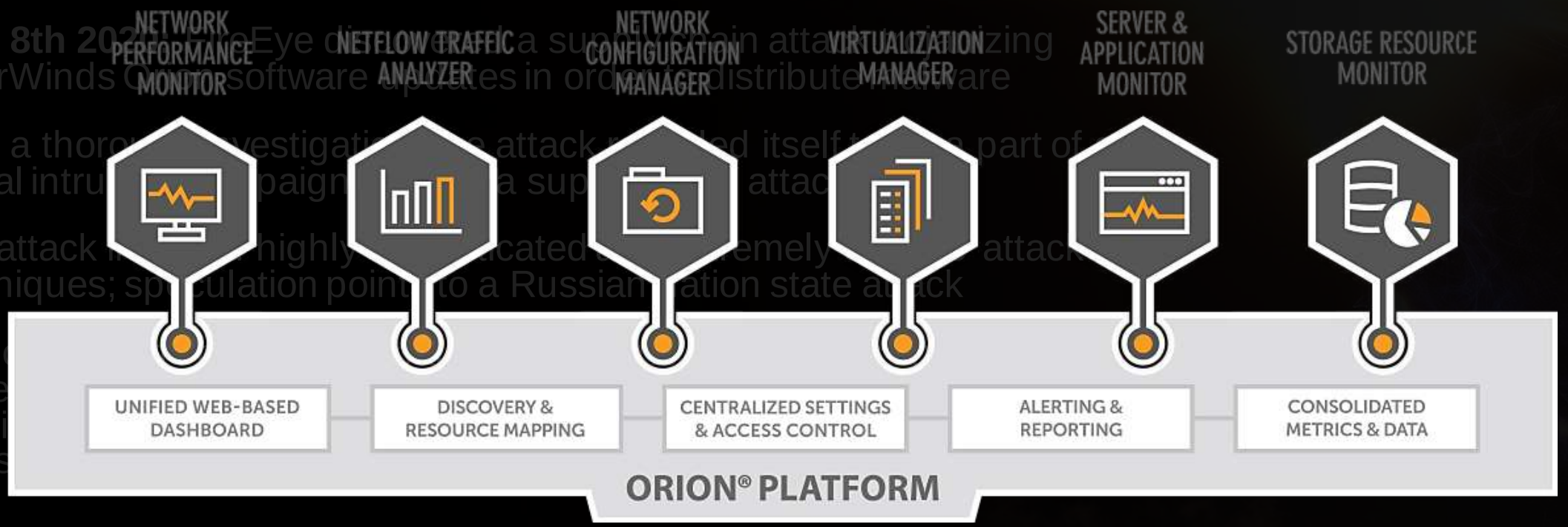
VMware Admin

SAN Admin

Switch Admin

FW Admin

Domain Admin



SOLARWINDS ATTACK CHAIN

STAGE 1

Orion Software
Pipeline Infection

STAGE 2

Target SolarWinds
Customers

STAGE 3

Privilege Escalation
to High Value Assets

TOP 10 LESSONS LEARNED FROM SOLARWINDS ATTACK

HIGHLIGHTS

- Even the most security-focused organizations can be breached
- Buying new products is not always the answer
- Privileged service account tools must be monitored
- Directory hygiene and anomaly monitoring are becoming a priority
- Privileged access management (PAM) tools should be used to protect privileged access
- Machine identity management is becoming a major imperative
- Endpoint detection and response (EDR) tools are now a mandatory security control
- Configuration of security tools has a major impact on the outcome
- Developers are a key target of advanced attackers and can no longer be excluded from endpoint protection policies
- The developer pipeline needs to be tested for known and unknown vulnerabilities


Gartner

Top 10 Lessons Learned From the SolarWinds Attack

Quick Answer

What are the top lessons learned from the SolarWinds attack?

More Detail

Gartner Top Lessons Learned From the SolarWinds Attack, Peter Firstbrook, February 17th 2021

THE RIGHT FRAME OF MIND: AN ASSUME BREACH MENTALITY

1. An “assume breach” mindset enables organizations to become vigilant and hyper focused on addressing weaknesses and vulnerabilities that exist within the environment, especially the areas that provide access to Tier0 systems (i.e. privileged access)
2. The majority of all cyberattacks involve the **compromise of identity and manipulation of privileged access** – *the SolarWinds breach is no exception to this trend*
3. CyberArk delivers deep Identity Security controls and expertise that **will buy organizations invaluable time** in detecting attacks earlier, and preventing attackers from reaching their end goals
4. CyberArk believes that a combined approach, whereby security **best practices and processes coupled with the right security solutions** will best secure high value targets and mitigate risk from advanced attacks like the SolarWinds breach

KEY CAPABILITIES TO STREAMLINE BREACH RECOVERY

MITIGATE RISK WITH CYBERARK SOLUTIONS

DEFENSE-IN-DEPTH SECURITY

LOCK DOWN CRITICAL ENDPOINTS

RESTRICT ACCESS TO TIER0

DETECT PRIVILEGED ANOMALIES

SECURE THE CI/CD PIPELINE

DEFENSE-IN-DEPTH SECURITY

- Implement tight PAM controls and processes to limit access to Tier0 targets and limit the access to critical resources by prioritizing a PAM solution deployment or validate existing foundational PAM controls to mitigate significant risk from advanced attacks
- Rotate credentials regularly, as often as after each individual use, and enforce MFA everywhere with specific recommendations (i.e. eliminate credential use without MFA)
- Enable risk aware, adaptive Multi-Factor Authentication (MFA) whenever possible.
- Enforce strong credential management practices:
  - **Unique**
    - Prevents lateral movement
  - **Complex**
    - Prevents brute-forcing
  - **Frequent Rotation**
    - Correlate frequency to risk/level of privilege

LOCK DOWN CRITICAL ENDPOINTS

- Implement privilege escalation and credential theft policies to prevent attackers from gaining administrative access to the environment – force the attackers to use methods that would expose their presence
  - Credential theft blocking capabilities help organizations detect and block attempted theft of Windows credentials, and those stored by popular web browsers and file cache credential stores
- Implement the removal of local admin rights on critical targets such as all Tier0 servers and VMs (i.e. Orion servers)
- **EPM Credential Theft Rules:**
  - NEW
  - Credential Theft from SolarWinds Orion
  - Duo Integration Secrets Dump
- **EPM Golden SAML policy:** Policy protects SAML signing certificates and MFA keys adding an additional control in protecting the secrets of Tier0 assets
  - Prevents forging SAML tokens in order to access various assets, a technique which has been highly used in this reported attack.
  - CyberArk Labs presented the potential of such an attack in 2017

RESTRICT ACCESS TO TIER0

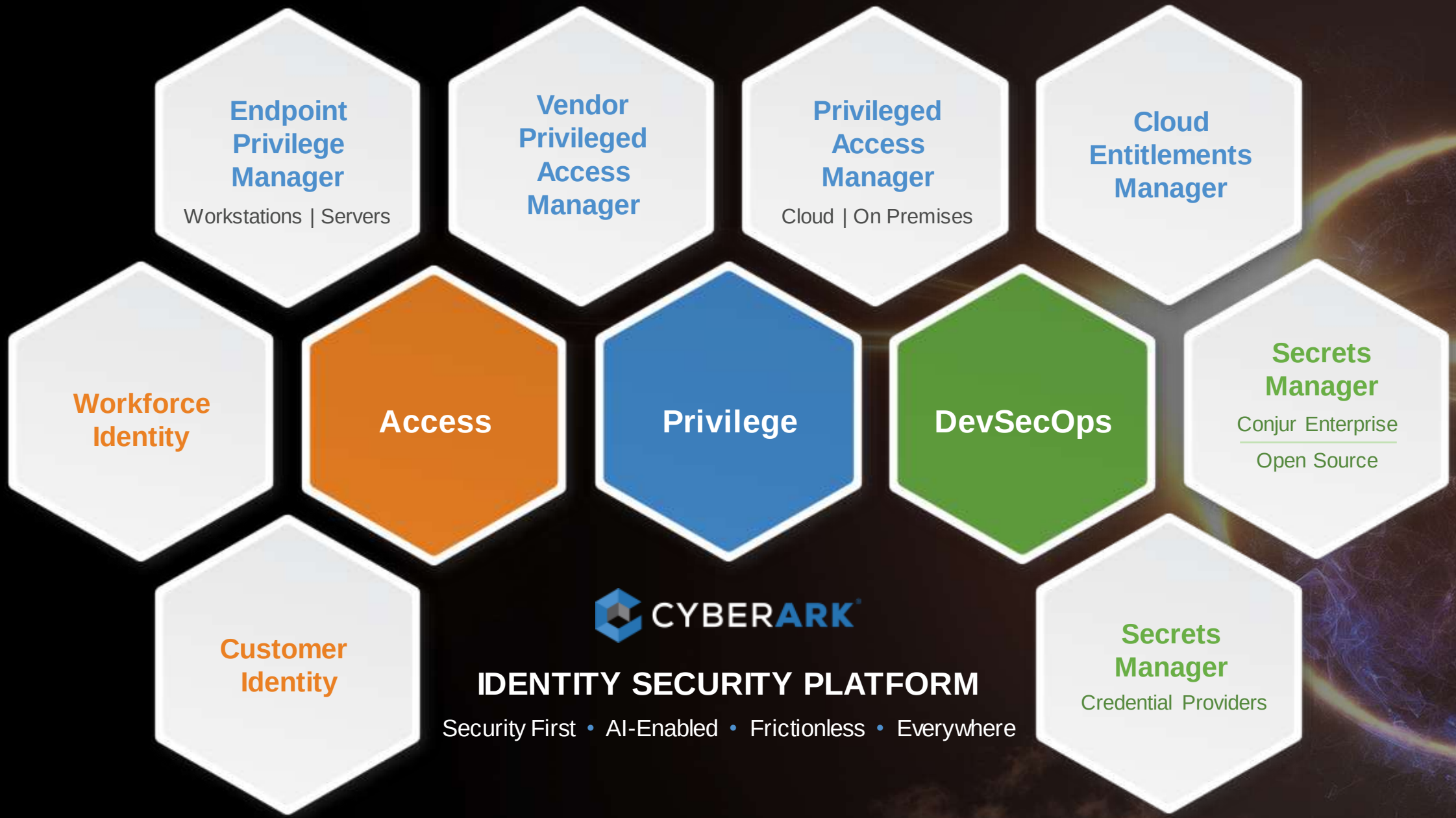
- Isolate, monitor and record privileged activity on Tier0 targets such as Azure AD
  - Privileged session management should be implemented when privileged sessions are used on Tier0 targets
- The removal of restrictions and attempts to access assets from unexpected sources could be detected, exposing the attacker in the process

DETECT PRIVILEGED ANOMALIES

- Identify malicious activity such as credential theft attempts and bypassing CyberArk controls (i.e. connecting to targets without checking out credentials from the Vault)
  - Detect backdoor account creation
  - Monitor for managed credential use outside the PAM solution
  - Establish normal behavior patterns of existing users and elevate to stronger authentication when anomalies are detected
  - Implement deception technologies
- Integrate PAM controls with other technologies for detection and response, such as **Splunk, Exabeam, IBM and Rapid7** to aid in detecting potential compromise
  - Bi-directional data feed provides privileged threat anomalies, and ingests detections from other solutions

SECURE THE CI/CD PIPELINE

- Privileged credentials are used throughout the software supply chain; integrations with orchestrators and infrastructure managers (i.e. Jenkins, Puppet) is critical in securing the pipeline
- Take a holistic approach to secure the supply chain
  - Establish policies and best practices
  - Control access to the CI/CD pipeline and dev tools
  - Manage the secrets used by applications to access sensitive resources
  - Secure developer endpoints


Endpoint Privilege Manager
Workstations | Servers
Vendor Privileged Access Manager
Privileged Access Manager
Cloud | On Premises
Cloud Entitlements Manager
Workforce Identity
Access
Privilege
DevSecOps
Secrets Manager
Conjur Enterprise
Open Source
Customer Identity
CYBERARK
IDENTITY SECURITY PLATFORM
Security First • AI-Enabled • Frictionless • Everywhere
Secrets Manager
Credential Providers

PAM RAPID RISK ASSESSMENT AND REMEDIATION OFFER

- SolarWinds Related PAM Security Readiness Assessment
- CyberArk Remediation Service (Recommended for relevant customers following assessment)
- Risk-based Remediation Programs
- Vendor Assurance and Training Services


CYBERARK
THANK YOU


CYBERARK
BACKUP SLIDES

PREEMPTIVE ACTIONS

- Organizations that may have been compromised by the SolarWinds breach, should take steps to implement Identity Security Controls and to help mitigate and possibly prevent these types of attacks
- Based on CyberArk's experience, the following steps are recommended to provide organizations quick and effective controls to regain command over privileged access and credentials and can be found in the CyberArk Security Fundamentals guide
- Once the immediate tasks outlined below are completed, organizations must next focus on strengthening and enhancing already deployed controls
- Organizations not directly impacted by the SolarWinds breach should strongly consider reviewing the strength of existing PAM controls, or prioritizing the implementation of a PAM program if one does not exist currently to mitigate the risk of similar attacks
- CyberArk is ready and willing to help organizations follow this process to maximize security in a short amount of time

IDENTITY SECURITY CONTROLS TO BE IMPLEMENTED IMMEDIATELY

- Run a scan to identify any new administrative accounts in the network **(CyberArk DNA)**
- Rotate credentials regularly, as often as after each individual use – enforce MFA recommendations (i.e. eliminate credential use without MFA) **(Core PAS: CPM + Idaptive)**
- Restrict access to Tier0 assets from a specific, hardened control point **(Core PAS: Privileged Session Manager)** implement session isolation when privileged credentials are used
- Protect certificates used to sign SAML assertions (and access to cloud hosted assets and data) on federation services servers (AD connect) or other IAM servers **(Endpoint Privilege Manager SAML certificate path protection)**
- Detect backdoor account creation **(Core PAS: Privileged Threat Analytics)**
- Deploy "least privilege" measures to endpoints and workstations, including those used to administer the PAM solution **(Endpoint Privilege Manager)**
- Monitor for managed credential use outside the PAM solution
- Enforce the registration of all endpoints and devices so that they are associated to a known end user and unknown ("untrusted") endpoints are not given access **(Idaptive)**
- Establish normal behavior patterns of existing users and elevate to stronger authentication on anomaly detection **(Idaptive)**
- Enable risk aware, adaptive Multi-Factor Authentication (MFA) whenever possible **(Idaptive)**

LONGER TERM IDENTITY SECURITY CONTROLS FOR CONSIDERATION

- Follow CyberArk's Blueprint strategy for PAM success
- Identify all possible points of entry (i.e. VPN, SSO etc.) and implement adaptive MFA
- Replace antiquated authentication protocols such as RADIUS with more modern ones like SAML, OIDC, OAuth 2.0. with MFA implemented
- Deploy "least privilege" measures to servers and applications
- Secure application credentials and continuous integration/development (CI/CD) pipelines
- Configure Active Directory based on credential boundaries (i.e. RedForest/ESAE)

C³ ALLIANCE

150+ CERTIFIED PARTNERS

250+ CERTIFIED JOINT SOLUTIONS

Analytics	ICS	Identity & Access Management	Authentication	ITSM	Detection	Orchestration & Response	DevOps	Robotic Process Automation	Discovery	SIEM	Governance	HSM	Vulnerability Management

200+ PLUG-INS

- CPM Plug-ins
- PSM Plug-ins