

Increasing resilience against Solorigate and other sophisticated attacks with Microsoft Defender

microsoft.com/security/blog/2021/01/14/increasing-resilience-against-solorigate-and-other-sophisticated-attacks-with-microsoft-defender/

January 14, 2021



UPDATE: Microsoft continues to work with partners and customers to expand our knowledge of the threat actor behind the nation-state cyberattacks that compromised the supply chain of SolarWinds and impacted multiple other organizations. Microsoft previously used ‘Solorigate’ as the primary designation for the actor, but moving forward, we want to place appropriate focus on the actors behind the sophisticated attacks, rather than one of the examples of malware used by the actors. Microsoft Threat Intelligence Center (MSTIC) has named the actor behind the attack against SolarWinds, the SUNBURST backdoor, TEARDROP malware, and related components as NOBELIUM. As we release new content and analysis, we will use NOBELIUM to refer to the actor and the campaign of attacks.

Even as investigations into the sophisticated attack known as Solorigate are still underway, details and insights about the tools, patterns, and methods used by the attackers point to steps that organizations can take to improve their defenses against similar attacks. Solorigate is a cross-domain compromise—comprehensive visibility and coordinated defense are critical in responding to the attack. The same unified end-to-end protection is key to increasing resilience and preventing such attacks.

This blog is a guide for security administrators using Microsoft 365 Defender and Azure Defender to identify and implement security configuration and posture improvements that harden enterprise environments against Solorigate’s attack patterns.

This blog will cover:

The recommendations on this blog are based on our current analysis of the Solorigate attack. While this threat continues to evolve and investigations continue to unearth more information, we’re publishing these recommendations to help customers apply improvements today. To get the latest information and guidance from Microsoft, visit <https://aka.ms/solorigate>. Security operations and incident response teams looking for detection coverage and hunting guidance can refer to https://aka.ms/detect_solorigate.

What the Solorigate attack tells us about the state of cyberattacks

Solorigate is a complex, multi-stage attack that involved the use of advanced attacker techniques across multiple environments and multiple domains to compromise high-profile targets. To perpetrate this sophisticated attack, the attackers performed the steps below, which are discussed in detail in this blog:

1. Compromise a legitimate binary belonging to the SolarWinds Orion Platform through a supply-chain attack
2. Deploy a backdoor malware on devices using the compromised binary to allow attackers to remotely control affected devices
3. Use the backdoor access on compromised devices to steal credentials, escalate privileges, and move laterally across on-premises environments to gain the ability to create SAML tokens
4. Access cloud resources to search for accounts of interest and exfiltrate emails

SOLORIGATE ATTACK
High-level end-to-end attack chain

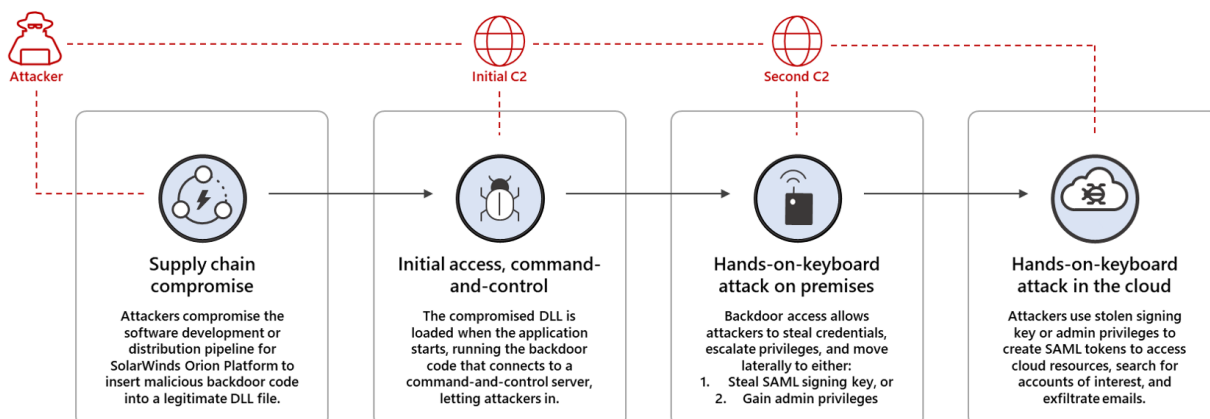


Figure 1. High-level end-to-end Solorigate attack chain

As its intricate attack chain shows, Solorigate represents a modern cyberattack conducted by highly motivated actors who have demonstrated they won't spare resources to get to their goal. The collective intelligence about this attack shows that, while hardening individual security domains is important, defending against today's advanced attacks necessitates a holistic understanding of the relationship between these domains and how a compromise in one environment can be a jump-off point to another.

The Microsoft Defender for Endpoint threat analytics reports published in Microsoft 365 security center enable customers to trace such cross-domain threats by providing end-to-end analysis of critical threats. In the case of Solorigate, Microsoft researchers have so far published two threat analytics reports, which continue to be updated as additional information becomes available:

- [Sophisticated actor attacks FireEye](#), which provides information about the FireEye breach and compromised red-team tools
- [Solorigate supply chain attack](#), which provides a detailed analysis of the SolarWinds supply chain compromise

In addition to providing detailed descriptions of the attack, TTPs, indicators of compromise (IoCs), and the all-up impact of the threat to the organization, the threat analytics reports empower security administrators to review organizational resilience against the attack and apply recommended mitigations. These mitigations and other recommended best practices are discussed in the succeeding sections. Customers who don't have access to threat analytics can refer to a publicly available [customer guidance](#).

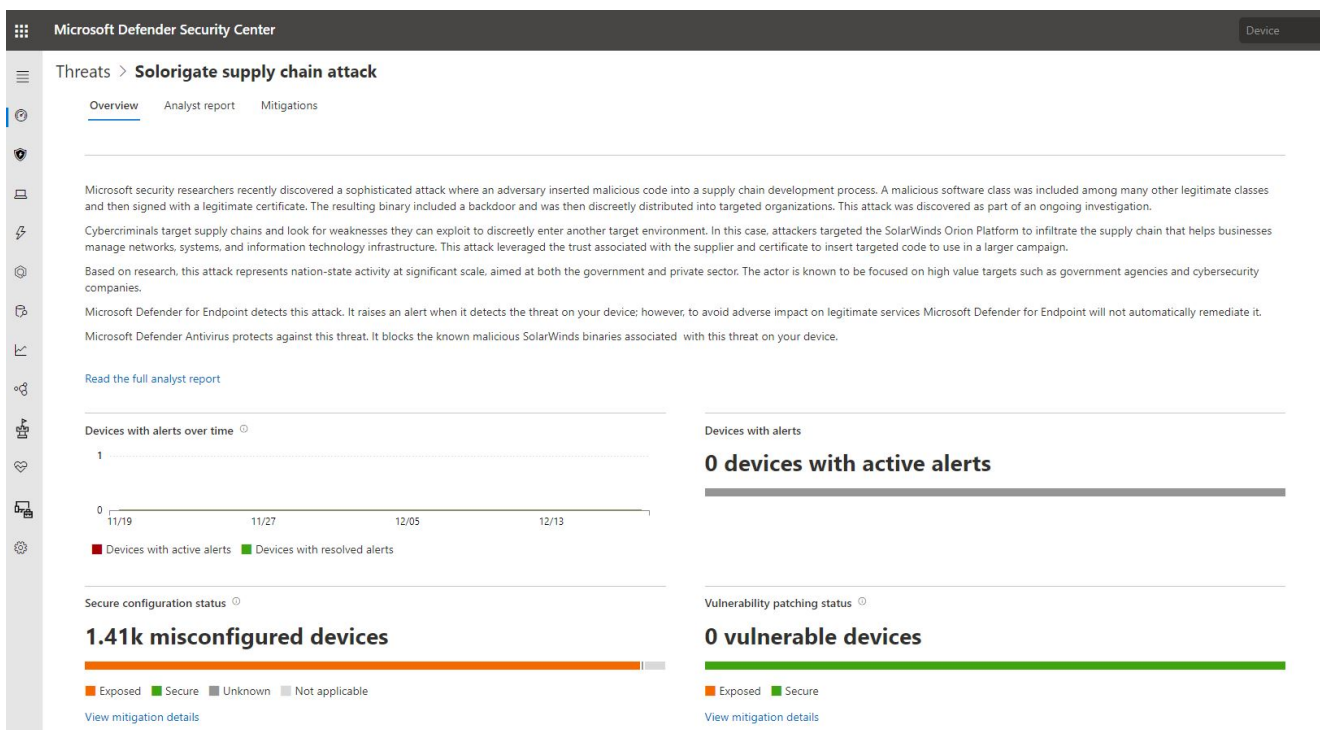


Figure 2. Microsoft Defender for Endpoint threat analytics report on Solorigate attack

Protecting devices and servers

The attackers behind Solorigate gain initial access to target networks by activating backdoor codes inserted into the compromised SolarWinds binary. Protecting devices against this stage of the attack can help prevent the more damaging impact of the latter stages.

Ensure full visibility into your device estate by onboarding them to Microsoft Defender for Endpoint

In the ongoing comprehensive research into the complex Solorigate attack, one thing remains certain: full in-depth visibility into your devices is key to gaining insights on security posture, risk, and potential attack activity. Make sure all your devices are protected and monitored by Microsoft Defender for Endpoint.



Figure 3. Status tile in the Device configuration management tab of Microsoft Defender for Endpoint, showing onboarded devices compared to the total number of devices managed via Endpoint Manager

Identify and patch vulnerable SolarWinds Orion applications

The Solorigate attack uses vulnerable versions of the SolarWinds Orion application so we recommend that you identify devices running vulnerable versions of the application and ensure they are updated to the latest version. The threat analytics report uses insights from threat and vulnerability management to identify such devices. On the Mitigations page in Threat analytics, you can view the number of devices exposed to vulnerability ID TVM-2020-0002, which we added specifically to help with Solorigate investigations:

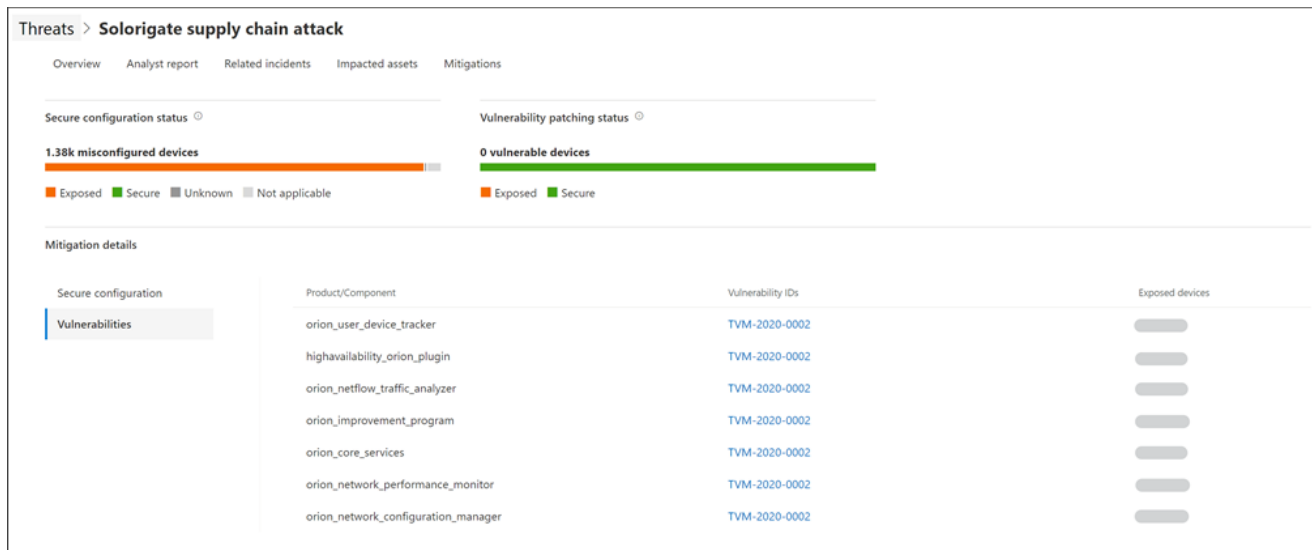





Figure 4. The Threat analytics Mitigations page shows information on exposed devices

The new vulnerability ID TVM-2020-0002 was added to the threat and vulnerability management Weaknesses page in Microsoft Defender for Endpoint so you can easily find exposed devices that have vulnerable SolarWinds software components installed. Additional details are available in the vulnerability details pane.

TVM-2020-0002



 Report inaccuracy

 Legal Notice 

Vulnerability description

Compromised legitimate SolarWinds Orion Platform binaries have been used in supply chain attacks. Attackers can deploy malicious code and control the system when these files are deployed and installed in target environments.

Vulnerability details

Vulnerability name 	Severity
TVM-2020-0002	 Critical
CVSS	Published on
9.4	12/16/20
Updated on	Age
12/16/20	a month

Related Software

Orion Improvement Program (+6 more)

Figure 5. Threat and vulnerability management vulnerability details pane for TVM-2020-0002

Customers can also use the [software inventory page](#) in threat and vulnerability management to view the SolarWinds Orion versions present on endpoints in your environment and whether the vulnerable versions are present. Links to the threat analytics reports are provided under the *Threats* column. You can then assess the footprint of a specific software in your organization and identify the impacted devices without the need to run scans across the install base.

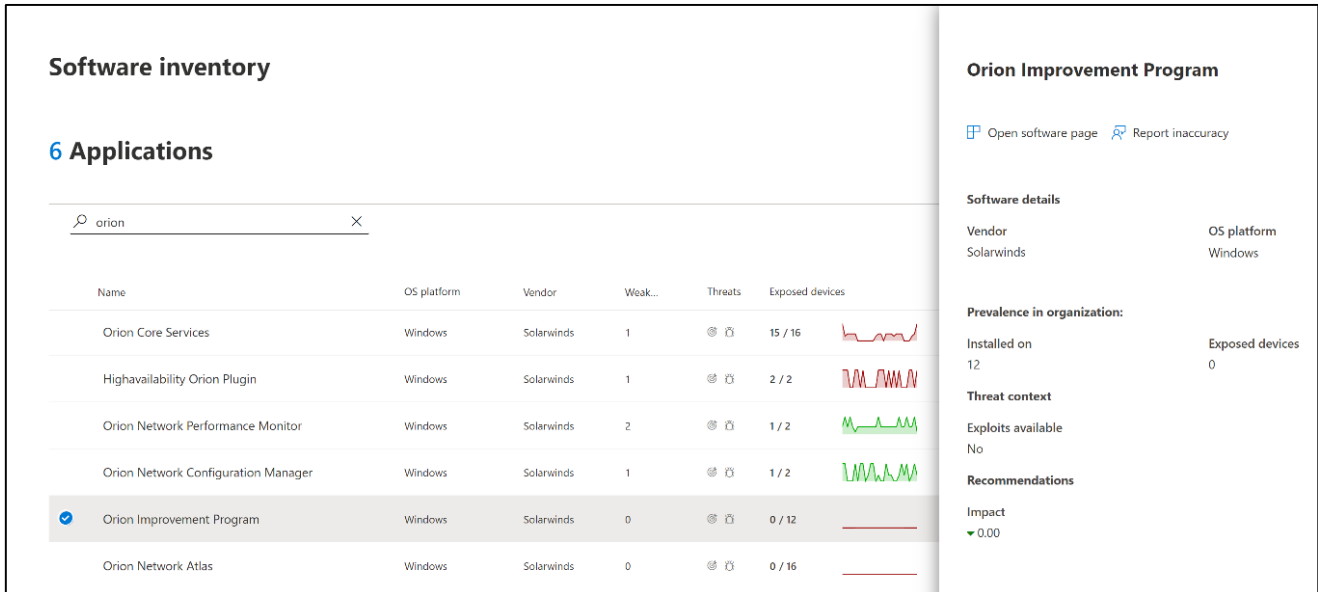


Figure 6. Threat and Vulnerability Management software inventory page displaying installed SolarWinds Orion software

Security recommendations are provided to update devices running vulnerable software versions.

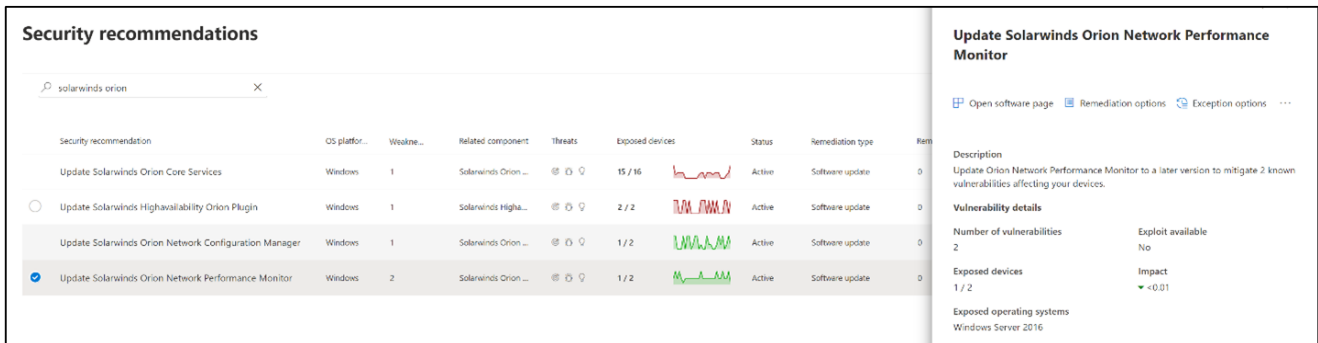


Figure 7. Threat and Vulnerability Management security recommendations page

Security admins can also use advanced hunting to query, refine, and export data. The following `query` retrieves an inventory of the SolarWinds Orion software in your organization, organized by product name and sorted by the number of devices that have software installed:

`DeviceTvmSoftwareInventoryVulnerabilities`

| where SoftwareVendor == 'solarwinds'

| where SoftwareName startswith 'orion'

| summarize dcount(DeviceName) by SoftwareName

| sort by dcount_DeviceName desc

The following query searches threat and vulnerability management data for SolarWinds Orion software known to be affected by Solorigate:

```
DeviceTvmSoftwareInventoryVulnerabilities
```

```
| where Cveld == 'TVM-2020-0002'
```

```
| project DeviceId, DeviceName, SoftwareVendor, SoftwareName, SoftwareVersion
```

For each security recommendation you can submit a request to the IT administrator to remediate vulnerable devices. Doing this creates a security task in Microsoft Endpoint Manager (formerly Intune) that can be continuously tracked in the threat and vulnerability management Remediation page. To use this capability, you need to enable a Microsoft Endpoint Manager connection.

Request remediation for:
Update Solarwinds Orion Network Configuration Manager

Submitting a remediation request creates an activity item, which can be used to monitor the remediation progress of this recommendation. It will not apply any changes to devices. Monitor remediation progress in the [remediation](#) page.

Exposed devices
3 / 6

Remediation
Select the device groups you plan to create a remediation request for.

Device groups
All (9) ▾

Remediation request ⓘ
Update ▾

IT services request
IT service and device management tools
 Open a ticket in Microsoft Endpoint Manager (for AAD joined devices)

Figure 8. Threat and vulnerability management 'Remediation options' for security recommendations and 'Remediation activities' tracking

Implement recommended security configurations

In addition to providing vulnerability assessments, Threat and Vulnerability Management also provides security recommendation guidance and device posture assessment that help mitigate this attack. These recommendations use vulnerability data that is also present in the Solorigate threat analytics report.



Figure 9. Threat analytics Mitigation page shows secure configuration recommendations for devices exposed to Solorigate

The following security recommendations are provided in response to Solorigate:

Component	Secure configuration recommendations	Attack stage
Security controls (Antivirus)	Turn on real-time protection	Stage 1
Security controls (Antivirus)	Update Microsoft Defender Antivirus definitions to version 1.329.427.0 or later	Stage 1
Security controls (Attack surface reduction)	Block execution of potentially obfuscated scripts	Stage 2
Security controls (Attack surface reduction)	Block executable files from running unless they meet a prevalence, age, or trusted list criterion	Stage 2
Security controls (Microsoft Defender SmartScreen)	Set Microsoft Defender SmartScreen Microsoft Edge site and download checking to block or warn	Stage 2

Applying these security controls can be accomplished using Microsoft Endpoint Manager (Intune and Configuration Manager). Refer to the following documentation for guidance on deploying and managing policies with Endpoint Manager:

- [Manage endpoint security policies in Microsoft Intune](#)
- [Windows 10 Antivirus policy settings for Microsoft Defender Antivirus in Intune](#)
- [Intune endpoint security Attack surface reduction settings](#)

Protecting on-premises and cloud infrastructure

In addition to compromising client endpoints, attackers can also activate backdoor code via the compromised SolarWinds binary installed on cloud or on-premises servers, allowing them to gain a stronger foothold in the environment.

Protect your on-premises and cloud servers

A large part of many customers' infrastructure are virtual machines. [Azure Defender](#) helps security professionals protect cloud workloads spanning virtual machines, SQL, storage, containers, IoT, Azure network layer, Azure Key Vault, and more.

As mentioned earlier, one of the key actions that should be taken to help prevent Solorigate and similar attacks is to ensure that all devices are protected and monitored by Microsoft Defender for Endpoint. Deploying Azure Defender for Servers enables Defender for Endpoint for your virtual machines to provide [comprehensive detection coverage](#) across the Solorigate attack chain. [Azure Defender's integrated vulnerability assessment solution for Azure and hybrid machines](#) can also help address the Solorigate attack by providing visibility into [vulnerability assessment findings](#) in Azure Security Center.

Enable additional infrastructure protection and monitoring

To help provide additional in-depth defenses against Solorigate, Azure Defender recently introduced new protection modules for Azure resources. Enabling these protections can improve your visibility into malicious activities and increase the number of Azure resources protected by Azure Defender.

[Azure Defender for Resource Manager](#) allows you to continuously monitor all Azure resource management operations and breadth in protection, which includes the ability to detect attempts to exclude known malicious files by the VM Antimalware extension and other suspicious activities that could [limit antimalware protection](#) on Azure VMs.

In addition, [Azure Defender for DNS](#) ensures that all DNS queries from Azure resources using Azure DNS, including communication with malicious domains used in the Solorigate attack, are monitored, and helps identify Solorigate activity across any of your Azure cloud resources. This helps prevent the malicious Solorigate DLL from being able to connect to a remote network infrastructure to prepare for possible second-stage payloads.

Protect your Active Directory and AD FS infrastructure

After gaining access, attackers may attempt to steal credentials, escalate privileges, and move laterally in the environment. Having complete visibility into your Active Directory, either completely on-premises or hosted in IaaS machines, is key in detecting these attacks and identifying opportunities to harden security posture to prevent them.

In hybrid environments, make sure that Microsoft Defender for Identity sensor components are deployed on all your Domain Controllers and Active Directory Federation Services (AD FS) servers. Microsoft Defender for Identity not only detects malicious attempts to compromise your environment but also builds profiles of your on-premises identities for proactive investigations and provides you with built-in security assessments. We recommend prioritizing the deployment of Microsoft Defender for Identity sensors and using the “Unmonitored domain controllers” security assessment, which lists any detected domain controllers in your environment that are unmonitored. (Note: this capability can monitor your environment only after deploying at least one sensor on a domain controller.)

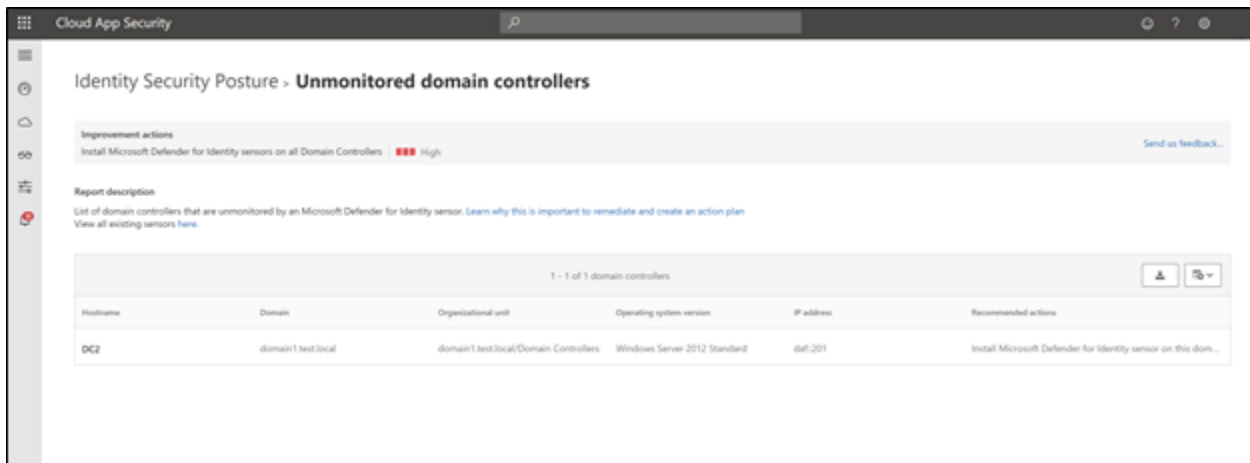


Figure 10. Unmonitored domain controllers' security assessment in the Microsoft Cloud App Security portal

Protecting Microsoft 365 cloud from on-premises attacks

The end goal of the attackers behind Solorigate is to gain access to a target organization's cloud environment, search for accounts of interest, and exfiltrate emails. From a compromised device, they move laterally across the on-premises environment, stealing credentials and escalating privileges until they can gain the ability to create SAML tokens that they then use to access the cloud environment. Protecting cloud resources from on-premises attack can prevent the attackers from successfully achieving their long game.

Implement recommended security configurations to harden cloud posture

Further best practices and recommendations to reduce the attack surface and protect the cloud from on-premise compromise can be found in our protecting Microsoft 365 cloud from on-premises attacks blog.

Implement conditional access and session control to secure access to cloud resources

In addition to hardening the individual surfaces to disrupt and prevent the attack, extending policies to implement zero trust and access controls is key in preventing compromised or unhealthy devices from accessing corporate assets, as well as governing cloud access from compliant devices.

Enable conditional access policies

Conditional access helps you better protect your users and enterprise information by making sure that only secure users and devices have access. We recommend implementing the [common recommended policies](#) for securing access to Microsoft 365 cloud services, including on-premises applications published with Azure Active Directory (Azure AD) Application Proxy.

Additionally, you can configure [user risk](#) and [device risk](#) conditional access policies to enable access to enterprise information based on the risk level of a user or device, helping keep trusted users on trusted devices using trusted applications.

Enable real-time monitoring and session control

Directly integrated with conditional access, session controls in Microsoft Cloud App Security enable extending access decisions into the session, with real-time monitoring and control over user actions in your sanctioned apps. Implement policies to prevent data exfiltration in risky situations, including [blocking or protecting downloads to risky or unmanaged devices](#), as well as for [partner users](#).

Additional recommendations and best practices

Strengthen your security posture even further by reviewing all improvement actions available via [Microsoft Secure Score](#). Secure Score helps operationalize security posture management and improve your organizational security hygiene for your production tenant. Below are some of the Secure Score improvement actions for Azure Active Directory that have a direct impact against Solorigate attack patterns:

- Do not allow users to grant consent to unmanaged applications
- Enable Password Hash Sync if hybrid
- Enable policy to block legacy authentication
- Enable self-service password reset
- Ensure all users can complete multi-factor authentication for secure access
- Require MFA for administrative roles
- Turn on sign-in risk policy
- Turn on user risk policy
- Use limited administrative roles

In addition, you can use the identity security posture assessment feature in Microsoft Defender for Identity to identify common protection gaps that might exist in your environment. Addressing detection gaps such as the following improves your Microsoft Secure Score and improves your overall resilience to a wide range of credential theft attacks:

Stop entities that are exposing credentials in cleartext, including ones that are tagged as sensitive. Attackers listen to cleartext credentials being sent over the network to harvest credentials and escalate privileges. While we have no indication that this technique was used in Solorigate, this is a general attack trend that organizations must be aware of and prevent.

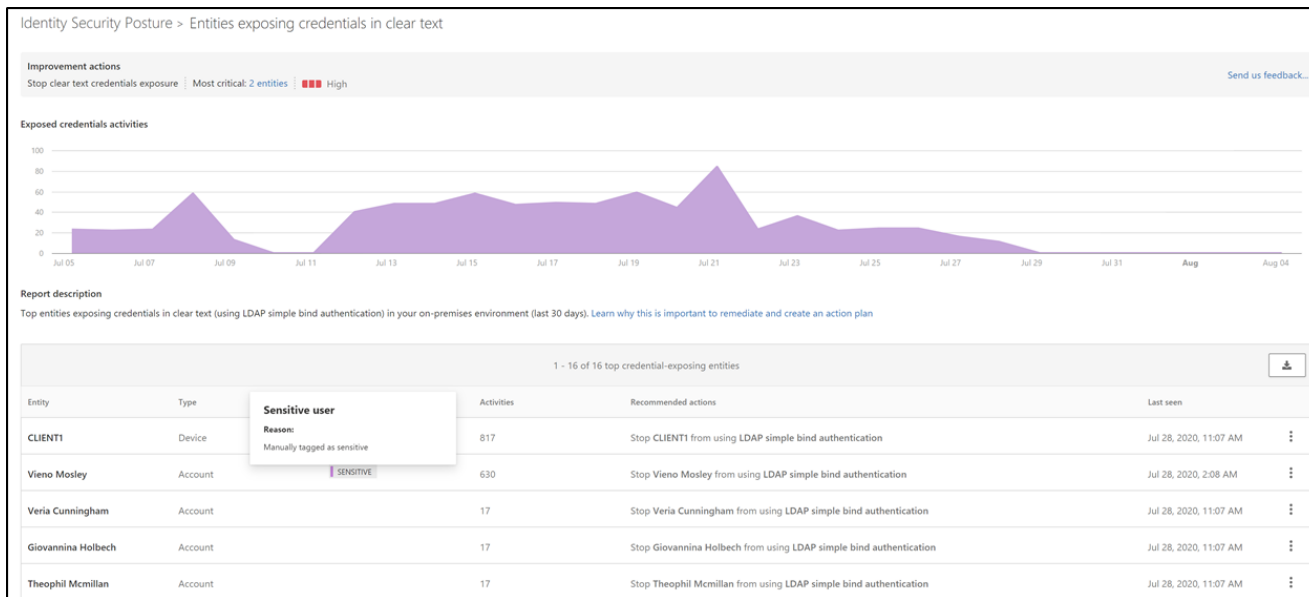


Figure 11. Entities exposing credentials in clear text security assessment in the Microsoft Cloud App Security portal

Remediate accounts with unsecure attributes that could allow attackers to compromise them once an initial foothold in the environment is established.

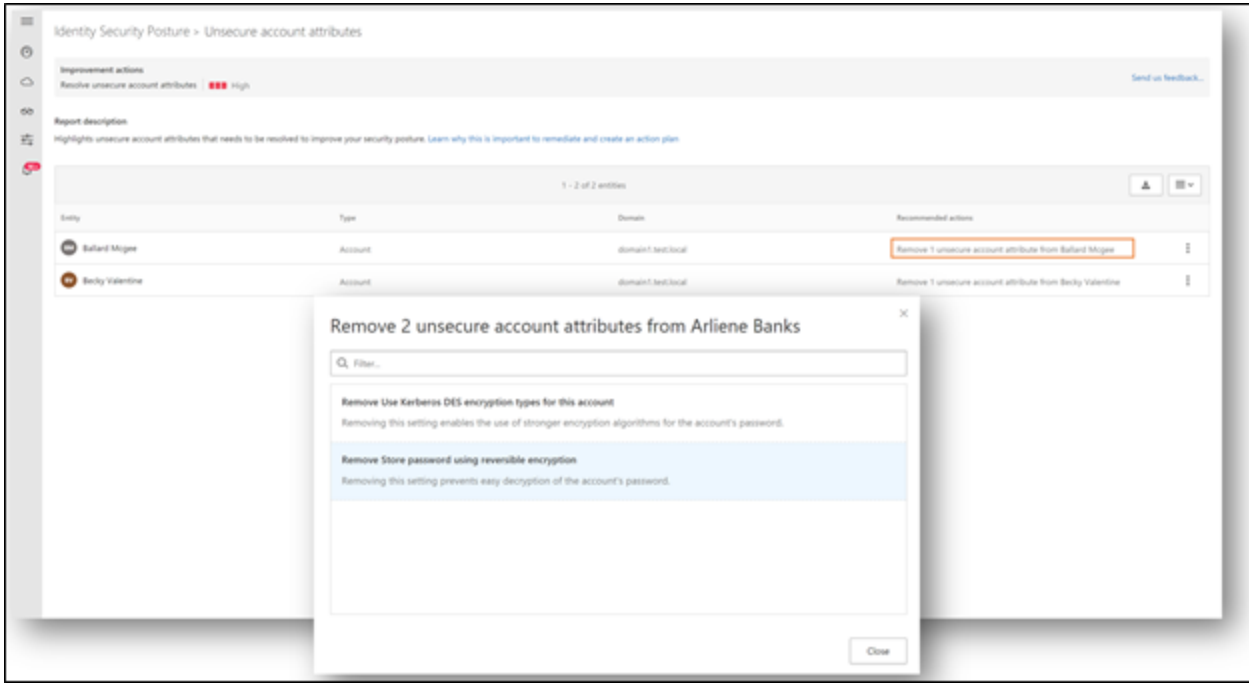


Figure 12. Unsecure account attributes security assessment in the Microsoft Cloud App Security portal

Reduce risky lateral movement paths to sensitive users. An attacker could move across devices to elevate to a more privileged role and operate deeper in your organization's environment, as we've witnessed in the Solorigate attack.

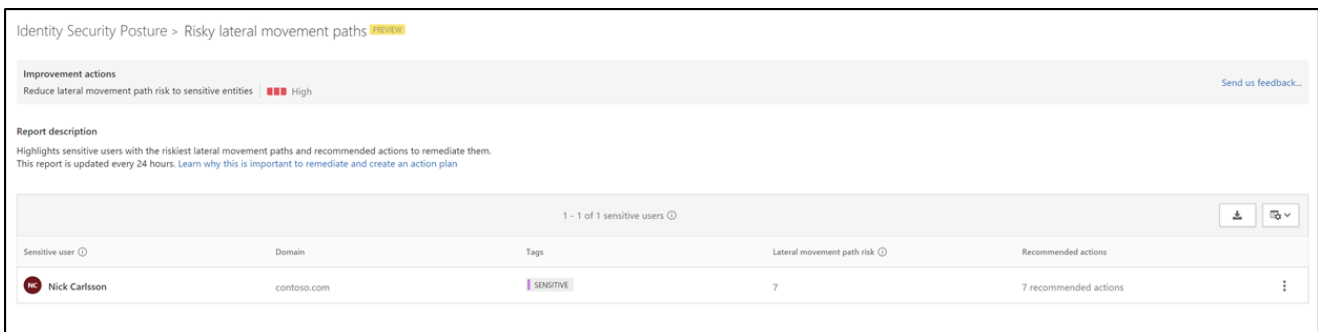


Figure 13. Risky lateral movement paths security assessment in the Microsoft Cloud App Security portal

Multiple layers of coordinated defense against advanced cross-domain attacks

Microsoft 365 Defender and Azure Defender deliver unified, intelligent, and automated security across domains to empower organizations to gain end-to-end threat visibility, which as the Solorigate attack has shown, is a critical security capability for all organizations to have. In addition to providing comprehensive visibility and rich investigation tools, Microsoft 365 Defender and Azure Defender help you to continuously improve your security posture as

a direct result of insights from collective industry research or your own investigations into attacks through configurations you can make directly in the product or in-product recommendations you can implement.

For additional information and guidance from Microsoft, refer to the following: