SOLUTION BRIEF

REDUCE THE ATTACK SURFACE AND STOP RANSOMWARE EARLY WITH **CROWDSTRIKE** AND **REMEDIANT**

Remediant

CROWDSTRIKE

THE CHALLENGE

Your infrastructure is getting more complex as there is a need to secure the ever-increasing volume of data that flows through your endpoints and systems. In addition, the increase in devices such as Windows, Mac and Linux laptops, workstations and servers being added to your network, substantially increase the attack surface for threat actors. The sprawl of undetected and standing 24X7 admin user access presents a large attack surface for the "bad guys" to wreak havoc using compromised accounts to launch identity-based attacks from your endpoints and move laterally through your environment. In fact, recent surveys and studies show that:

- 74% of breached organizations admitted the breach involved access to a privileged account*
- 41% of surveyed organizations admit to allowing users to retain privileged access indefinitely^
- 76% of organizations experience privileged access policy violations each year ^

As a result, there is an urgent need to discover and remove standing privileged access across platforms and to provision the access just-in-time, only on the endpoints where it's needed, removing it again as soon as possible.

Endpoint Detection and Response (EDR) solutions record and store endpoint system-level activity, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity and provide remediation suggestions including threat hunting services. But threat actors have now resorted to using compromised privileged accounts to launch ransomware and malware since any activity using these accounts is difficult to distinguish from normal activity. Detecting and stopping these types of compromised privileged account-based attacks has proven to be very difficult. Reducing the attack surface requires a combined approach that coordinates detection and investigation of endpoint activity with the rapid reduction of unwanted 24X7 privileged access sprawl that threat actors use to move through environments undetected.

** 2020 Verizon Data Breach Investigations Report*
^ 2020 EMA IT & Data Management Research, Industry Analysis & Consulting

THE SOLUTION

CrowdStrike Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. All endpoint activity is streamed to the CrowdStrike Falcon platform so that security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats. The joint solution combines the power of SecureONE's privileged access management with CrowdStrike Falcon Insight, enabling organizations to implement Zero Trust security — without adding an additional PAM agent. Falcon Insight's speedy investigations with deep, real-time forensics and sophisticated visualizations are complemented by SecureONE's identity-based response to attacks which are hard to detect. Remediant's unique approach exposes and removes 24x7 admin sprawl from endpoints replacing it with "Zero Standing Privilege" (ZSP) and user-friendly Just-In-Time (JIT) access. CrowdStrike Falcon Insight plus Remediant SecureONE enables organizations to:

1. Track and record all endpoint activity (processes, network connections, user activity, etc.) including intervals when privileged access and JIT access are in use
   - This feature is particularly useful for audit, forensics and compliance requirements
2. Block attackers from moving laterally to additional systems by eliminating standing 24x7 admin access and replacing with ZSP
3. Provide JIT access for privileged users that eliminates the motivation to circumvent controls

Now, Remediant SecureONE customers using the CrowdStrike Falcon Insight agent can with Intelligent Session Capture (ISC) investigate session activity in near real time for endpoints located both within and outside their corporate network. Also, with SecureONE customers can minimize the privileged account attack surface across Windows, Linux and Mac endpoints on the network.

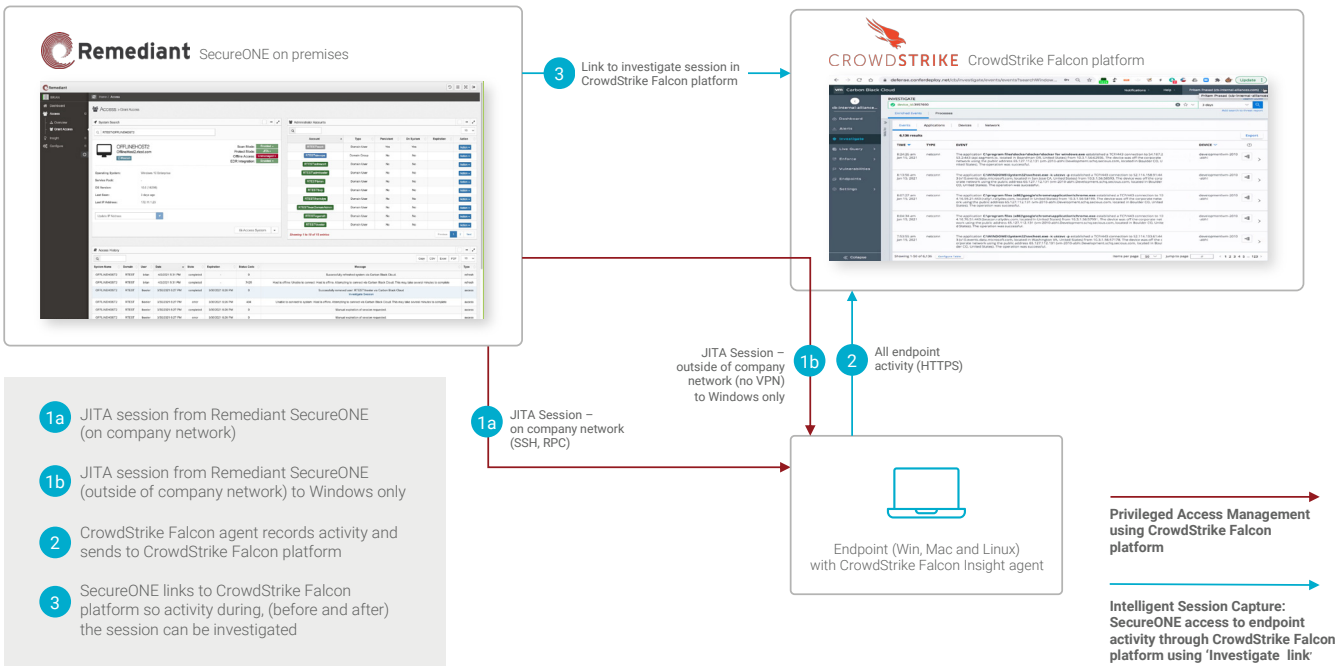

Figure 1. Intelligent Session Capture (ISC) and remote management of Windows sytems with CrowdStrike Falcon

With Remediant SecureONE, customers using CrowdStrike Falcon platform capability may now extend their reach to:

•Maintain ZSP and JIT access for Windows endpoints that are outside the corporate network and VPN.

•Intelligent Session Capture (ISC): Investigate session activity in near real time for endpoints located both within and outside their corporate network.

USE CASES AND BENEFITS OF THE JOINT SOLUTION

The combined solution helps Incidence Response teams quickly determine root cause and stop lateral movement attacks at endpoints.

For example:

• The IR team detects this event using CrowdStrike Falcon Insight

• To investigate, the IR team leverages Remediant's Intelligent Session Capture (ISC) to identify that during a privileged session (JIT) the malware activates on the Windows endpoint to send sensitive information to a C&C site (provides context during the privileged session)

• ISC helps the IR team pivot to the EDR console from Remediant to view all other systems the user has admin rights to during this JIT session and also easily search and find all other systems the malware has moved laterally to

• At this stage, the IR team may either isolate or quarantine the malware infected endpoints using CrowdStrike Falcon Insight

• The IR team can realize the principle of least privilege by implementing JIT and enabling ZSP on all the malware infected endpoints to eliminate lateral movement

The user benefits are:

1. Obtain contextual data into privileged account activity while eliminating the need for additional infrastructure for recording and PAM agents
2. Correlate privileged account activity by accessing the recordings of all end point activity from CrowdStrike Falcon to expedite incident response and remediation in real time
3. Prevent lateral movement attacks by removing excess standing privilege and replacing with JIT access
4. EDR data recordings are easy to access, search and analyze for auditing, forensics and compliance purposes
5. Helpdesk staff can enable their privileged access to support the systems outside the network
6. Security Operations can determine privileged access and enforce the desired JIT privileged access on a system
7. Remote users such as software developers (DevOps) can install software and make system config changes using privileged access

Remediant
Two Embarcadero Center, 8th Floor
San Francisco, CA 94111
(415) 854-8771

ABOUT REMEDIANT

San Francisco-based Remediant is bringing Zero Trust to the Privileged Access Management (PAM) market by taking a focused approach to removing the biggest undiscovered security risk: (24x7/always on/persistent) administrator (rights/privileges/access). Built upon the principle of Zero Standing Privilege, Remediant's award-winning SecureONE PAM software delivers Just Enough, Just-in-Time privileged access and continuous discovery with agentless simplicity. SecureONE protects millions of endpoints worldwide and has been adopted by major enterprises across a number of industries. For more information, please visit: *https://www.remediant.com*.

080921