STOP LATERAL MOVEMENT AND RANSOMWARE EARLY WITH **VMWARE CARBON BLACK** AND **REMEDIANT**

THE CHALLENGE

As more and more endpoints such as Windows, Mac and Linux laptops, workstations and servers are added to your network, they substantially increase the attack surface for threat actors. The prevalence of undetected and standing 24X7 admin user access presents a large attack surface for the "bad guys" to wreak havoc using compromised accounts to move laterally through your environment, stealing sensitive information from your endpoints. In fact, 74% of breached organizations admitted the breach involved access to a privileged account*. There is a need for an automated way to remove that standing access across platforms and to provision the appropriate access directly to user accounts just for the time needed.

Endpoint Detection and Response (EDR) solutions record and store endpoint system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to protect and restore affected systems. As EDR continues to increase its effectiveness in detecting malware and unusual activity, threat actors have pivoted to using compromised privileged accounts. Their activity using these accounts is hard to distinguish from normal activity. Protecting a company today requires a comprehensive approach that 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.

** Verizon 2020 Data Breach Investigations Report*

THE SOLUTION

The VMware Carbon Black Cloud is a cloud native platform delivering best-in-class, next-generation antivirus, EDR managed detection, and audit and remediation without compromising system performance. This is achieved by consolidating multiple endpoint and workload security capabilities using one agent and console, helping you operate faster and more effectively. As part of VMware's intrinsic security approach, Carbon Black Cloud spans the system hardening and threat prevention workflow to accelerate responses and defend against a variety of threats.

The joint solution combines the power of SecureONE's privileged access security with Carbon Black Cloud, enabling organizations to implement Zero Trust security — without adding an additional PAM agent. Carbon Black's best-in-class protection is complemented by SecureONE's identity centric response to attacks which are hard to detect. Remediant's unique approach exposes and removes 24x7 "Just-In-Case" admin rights from endpoints replacing it with easy-to-use Just-In-Time (JIT) access and "Zero Standing Privilege" (ZSP). VMware Carbon Black 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. Pinpoint and eliminate unnecessary privileged users, groups and systems attackers rely on to compromise entire organizations
3. Block attackers from moving to additional systems by eliminating standing 24x7 admin access
4. Simple Just-In-Time access for privileged users that eliminates the motivation to circumvent controls

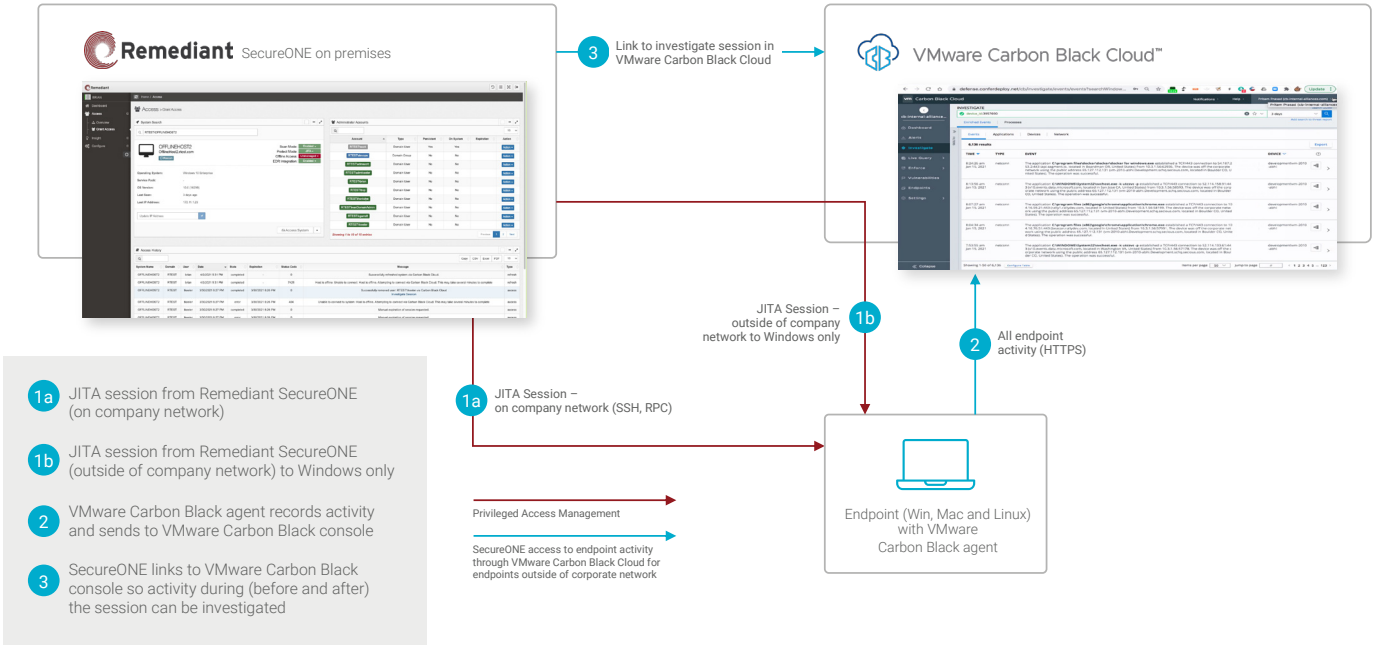

Figure 1. Intelligent Session Capture (ISC) with VMware Carbon Black

With Remediant SecureONE, customers using VMware Carbon Black Cloud's Live Response 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.

The integration of SecureONE with Carbon Black simplifies life for the increasing remote workforce.

USE CASES AND BENEFITS OF THE JOINT SOLUTION

Traditional PAM strategies have left companies ill-prepared for the identity-based attacks on endpoints. The Remediant and VMware Carbon Black integration allows organizations of all sizes to protect their endpoints by discovering and restricting 24X7 privileged account sprawl and enabling Zero Trust security.

The use cases are:

1 Helps Incidence Response teams quickly determine root cause and stop lateral movement attacks at endpoints.

For example:

- A user signed into a Windows endpoint browses a website and accidently downloads malware
- The IR team detects this event using VMware Carbon Black Cloud
- 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 VMware Carbon Black Cloud
- 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

2 Helpdesk staff can enable their privileged access to support the systems outside the network

3 Security Operations can determine privileged access and enforce the desired JIT privileged access on a system

4 Remote users such as software developers (DevOps) can install software and make system config changes using privileged access

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 VMware Carbon Black Cloud 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

""As the threat landscape evolves, security and IT teams must be empowered to detect and stop emerging attacks. Leveraging the VMware Carbon Black Cloud, Remediant can help customers bolster their defenses by deploying Zero Trust privileged access management that helps better detect and prevent lateral movement in compromised accounts."

CHRIS GOODMAN
DIRECTOR OF TECHNICAL ALLIANCES
SECURITY BUSINESS UNIT | VMWARE

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*.

043021