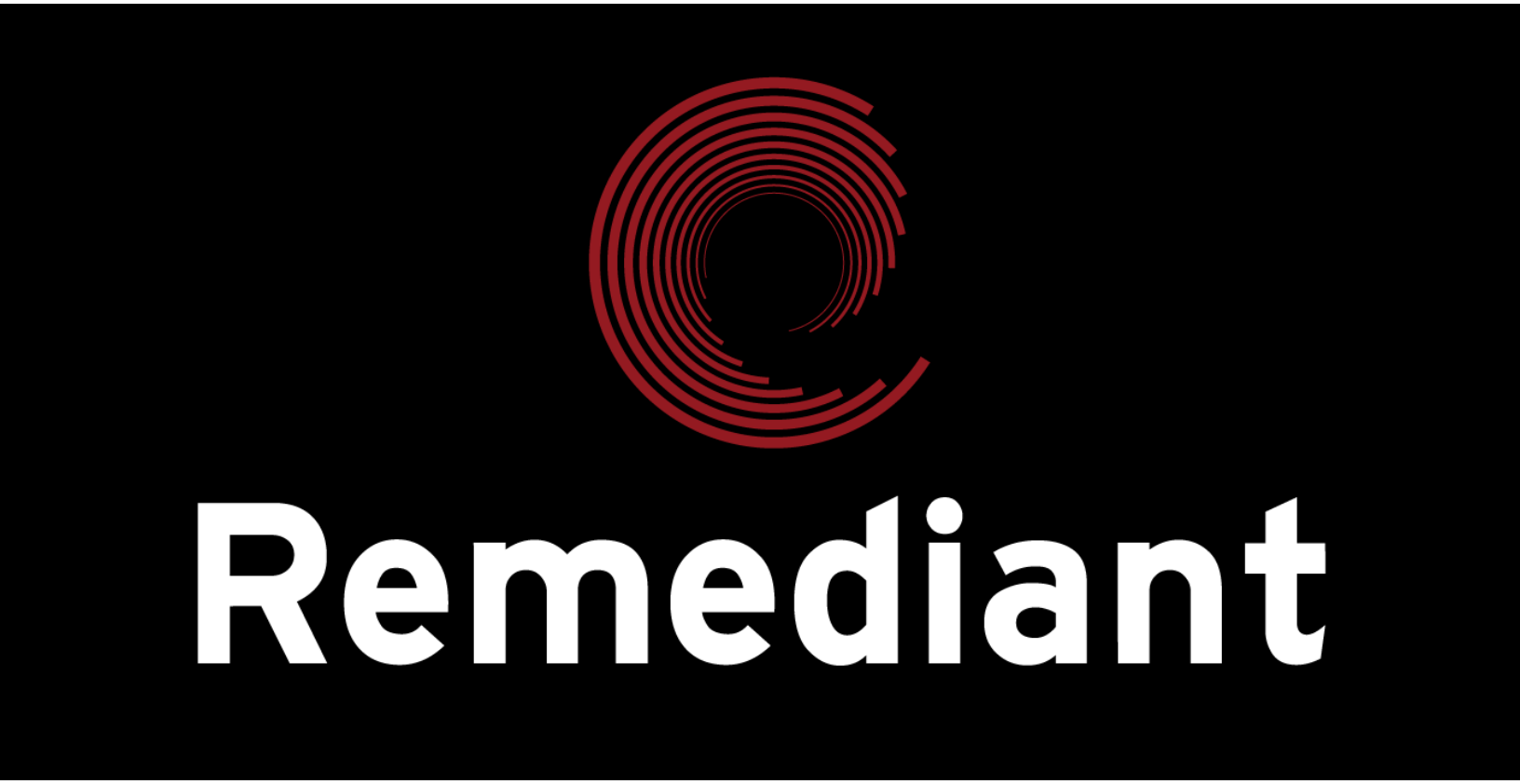


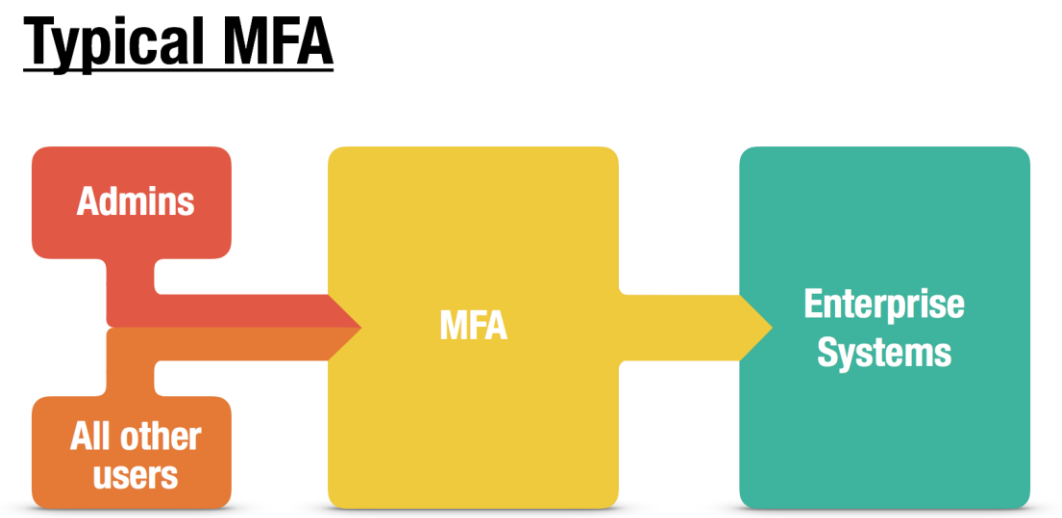
Contents

Multifactor Authentication Challenges

Late to the game: Multifactor Authentication is hard even if you're Amazon

It's not often that Amazon is late to any game. Consistently cited as the leader -- quite often defining the cutting edge -- of supply chain and delivery logistics, e-reading technology, DRM-free digital music distribution and countless other technologies, there is one crucial technology that Amazon was late to adopting: **multi-factor authentication**. You've been able to protect your Google Account with MFA since February 2011 (Enterprise customers **got the feature in September 2010** -- more than 5 years ago!). Apple launched the feature in March 2013, not long after **Mat Honan, Senior Staff Writer for WIRED experienced an "epic hack"** that disabled his computer and mobile device hardware, and compromised his Google, Twitter, Amazon and Apple accounts in the matter of a few minutes. A key part of that attack chain? Amazon. Just a few weeks ago, in November 2015,**Amazon finally announced the availability of two-factor authentication** to protect your Amazon account.

Why did it take Amazon 5 years longer than Google to enable multi-factor authentication? Why do dozens of other cloud services still not offer it? Most critically, why do **32.4% of Enterprise survey respondents** say that <10% of their user population is using any kind of multi-factor authentication?



There are three main reasons why the adoption of multi-factor authentication has been so slow -- in both the consumer and Enterprise spaces. **Cost** and **technical complexity** to implement multi-factor

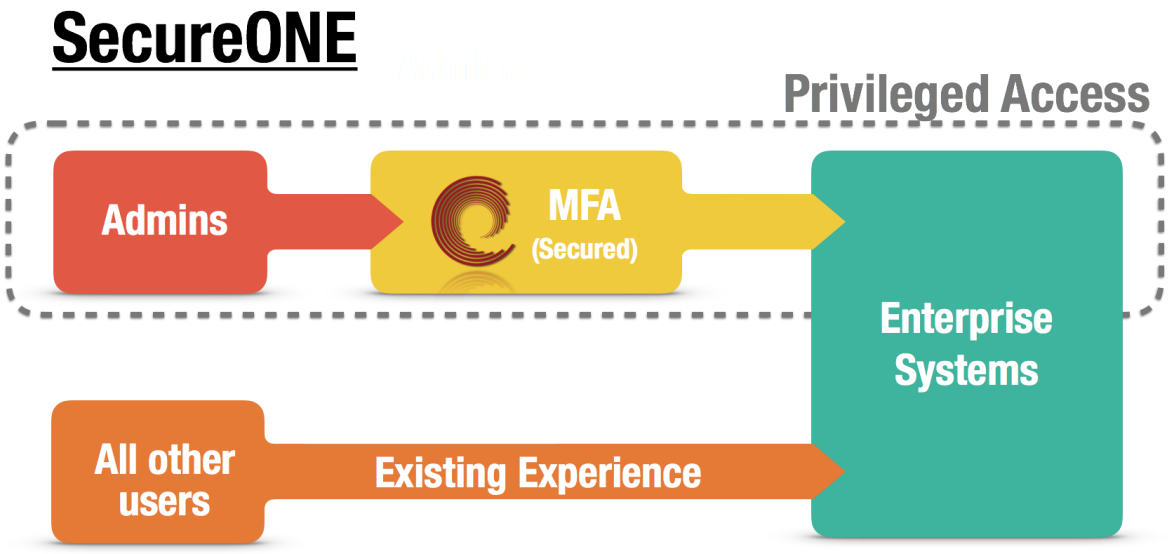
authentication are often cited as top reasons -- and with IT budgets and staff time already pulled in many different directions, these are significant concerns. Multi-factor authentication schemes can break compatibility with older solutions, be difficult to install and maintain and sap resource time and budget dollars from other initiatives.

However, there is one reason that stands above all others: **User Experience**. In a multi-logon, multi-device world, users don't want to be inconvenienced to enable and then authenticate with multiple factors on all of their devices. In the Enterprise, this is made even more difficult by the lack of native multi-factor authentication in off-the-shelf applications and in Windows, the primary OS used in Enterprise environments. IT departments seek to offer their users friction-less computing, and multi-factor authentication, despite the protection it can offer, feels like a move in the wrong direction. This challenging User Experience is one reason why adoption of Google's 2SV (multi-factor authentication) technology limited to **something approximating 6.5%** of their user population -- despite news articles, nag screens and other inducements to enable it.

So, in a world where:

- We need multi-factor authentication to protect our accounts against unauthorized use
- Cost, technical complexity and -- most of all -- a desire to offer an excellent User Experience prevent IT departments from rolling out multi-factor authentication
- Even industry titans like Amazon have difficulty enabling multi-factor authentication

What can we do?



Typical multi-factor authentication solutions require that ALL users utilize the MFA technology… but what if there was a way for Enterprises to enable multi-factor authentication for just the most sensitive user accounts? When we look at **recent hacks**, there is one thing in common across all of them: abuse of administrator credentials in the attack chain. With Remediant's SecureONE product, you can quickly and easily enable multi-factor authentication for your highly privileged administrator accounts -- without making a single change to the user experience for the rest of your users. Audit findings, security standards adherence and best practice adoption all drive IT Security teams toward adopting multi-factor authentication -- now you can bring the power of multi-factor authentication to your Enterprise systems with a hardware appliance that installs in minutes and protects your Enterprise 24/7.

More of the same: LANDESK joins Target, OPM, Sony in the Hacked Club

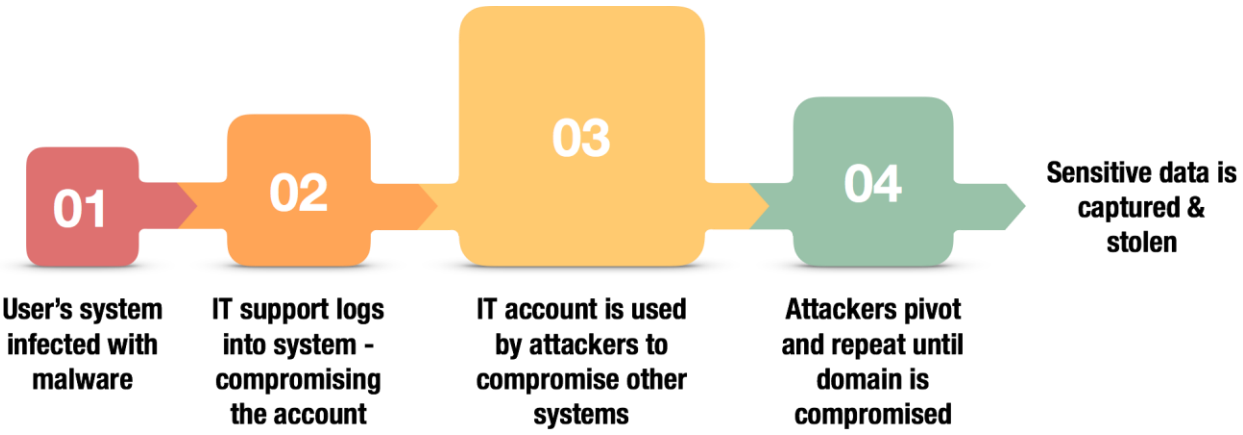
Early in 2016, LANDESK became the latest company to join the ever-growing list of enterprises breached. As one of the titans of IT Asset Management, this breach is particularly painful - LANDESK's core product set is focused on protecting IT assets. As reports indicate that LANDESK's source code / build servers have been compromised, the attack not only jeopardizes employee and LANDESK corporate data -- but potentially the data on all endpoints running LANDESK's client software.

The hack against LANDESK, as reported by Krebs is straight out of the hacker playbook. Despite security being a **core product focus at LANDESK**, they join the ranks of Target[1], Anthem[2], Sony[3], and even the Office of Personnel Management[4] as victims of highly targeted hack attacks. One thing in common across these diverse organizations: all of them had their most critical systems breached using compromised administrator credentials.

> *John said further investigation showed that the attackers were able to compromise the passwords of the global IT director in Utah and another domain administrator from China.*

Compromising Administrator credentials is the most widely used attack method to successfully breach large organizations. Managing privileged access - which admin gets what level access to what systems is a **major** challenge for every enterprise.

The Attack Chain



Pass-the-hash, pass-the-ticket, access tokens, cached credentials, LSA secrets, etc - there are countless number of technical capabilities for hackers to get a hold of administrator credentials. The stark reality is that infrastructures rely on integrated underlying technologies that make it impossible to eliminate these attack channels. You can implement technical strategies to reduce part of the attack, but hackers are always figuring out new and sophisticated methods to compromise your credentials.

> *A LANDESK software developer later found that someone in the IT department had been logging into his build server, so he asked them about it. The IT department said it knew nothing of the issue.*

The biggest challenge security teams face is the ability to differentiate between legitimate and illegitimate use of credentials. Security teams need to perform the bare minimum, in real-time:

1. Know **what** systems your admins can access
2. Know **when** systems are accessed by your admins
3. **Restrict** access to your privileged systems

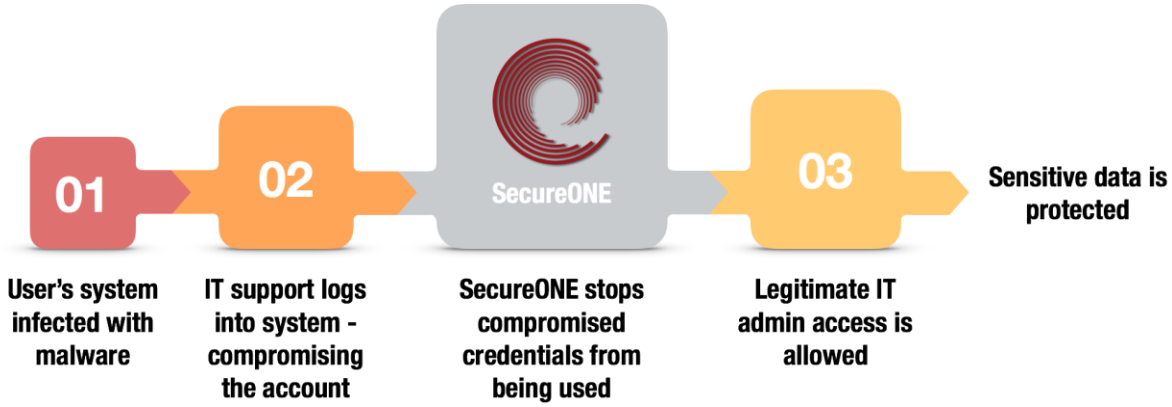
In reality, this isn't feasible (or possible) for most organizations. Even if you have centralized logging of every account activity, security experts need to scour endless logs to find the needle in the haystack.

This is exactly why companies likes LANDESK, Target, Anthem, Sony, & OPM are breached.

Breaking the Attack Chain

After years of security consulting at large enterprises, we've realized it's impossible to funnel every event through your security team. Humans performing remedial tasks are prone to error. Intrusion detection systems won't differentiate between good & bad logins. Implementing a strict and diligent security process will only clog your business flow.

In order to successfully stop this attack chain, you need to continually enforce restricted access to systems **AND** actively monitor changes to access. You need this process automated and streamlined so you aren't impacting important business functions.
Which is why we developed **SecureONE**.



SecureONE solves the problem of compromised credentials by providing administrators time-based, on-demand access to sensitive systems using 2-factor authentication. So when (not if) your administrator credentials are compromised, hackers can't use it to access any system.

IT Administrators are a key part of ensuring 100% uptime of your systems, but not even admins need 24x7 access to the entire infrastructure. Having this level of access only increases your attack vectors & risk. Admins only need to access individual servers for a particular task (to troubleshoot, update, configure). SecureONE automates this workflow seamlessly by providing admins a secure & dead simple interface to access all of your endpoints.

If any of the above companies were using SecureONE, they simply would not have been vulnerable to this type of attack.

Analysis of the Mandiant M-Trends 2016 Report

Mandiant, the breach remediation and forensics company purchased by **FireEye** in 2014 and a leader in the cybersecurity technology world, released their "**M-Trends 2016**" report on their observations from 2015. Even at 48 pages in length, it is well worth a read -- these are some smart folks who are deeply passionate about cybersecurity. The report highlights some unsurprising facts - there are more disruptive attacks than ever, and state-sponsored attacks are driving a lot of them. But it's not all bad news: there are solutions to many of the problems that Mandiant highlighted in this report.

Mandiant Consulting M-Trends 2016 Report:
https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

Breach Detection and Persistence

Let's start off with the good news. In 2012, the median number of days between breach and discovery of the breach was 416 days (that's not a typo -- more than a year!). 2014 saw that drop to 205 days, and the latest info for 2015 shows that has dropped to 146 days. Mandiant doesn't propose any theories as to how this improvement has been achieved, but it's reasonable to guess that an increased focus (at all management levels) on cybersecurity has brought more resources to the fight, and improved awareness of the likelihood, impact and need to prevent breaches. More focus and more resources mean greater detection capabilities are being deployed across enterprises. Existing software and hardware solutions have also gotten smarter -- more able to report suspicious activity on their own -- and those reports are flowing together into SIEM solutions with greater speed and in greater quantities.

It's not all good news, though. Mandiant's Red Team, on average, "is able to obtain access to domain administrator credentials within three days of gaining initial access to an environment". There are so many vectors to obtain highly-privileged accounts that protecting them is an increasingly tough job. Also, you're still more likely to have the FBI notify you than to have your Security Operations Center notify you of a breach: 53% of breaches in Mandiant's 2015 study data were discovered through external notification.

Failure Trends

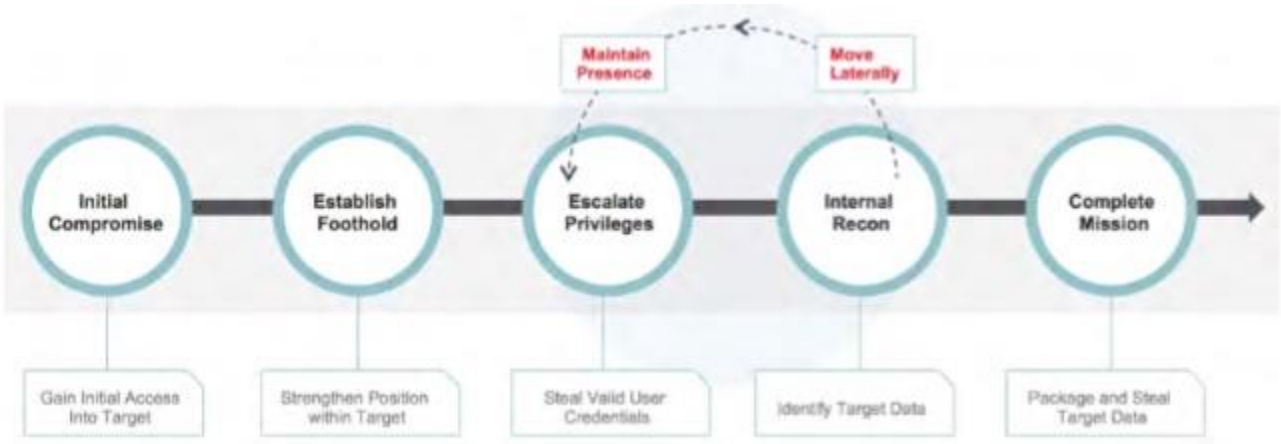
> *Observation #1 – Credentials, in general Captured credentials remain the most efficient and undetected technique for compromising an enterprise.*
> *- Mandiant M-Trends 2016 Report*

It is no surprise that the first observation of security failure trends in the M-Trends report is credentials. Due to the sheer number of attacks available, compromising administrator credentials is still the number one choice for attackers successfully penetrating networks.

> *These tools are fast, almost impossible to detect by AV, publicly- available, and widely supported. Even with detailed guidance from Microsoft regarding the protection of credentials and the built-in safeguards in modern Windows operating systems, our Red Teams continue to have extraordinary success retrieving credentials from memory and reusing those credentials to move laterally throughout a network.*
> *- Mandiant M-Trends 2016 Report*

As reported by FireEye, defending against these attacks has been extremely difficult. It's easy to bypass AV and once credentials are pulled out of memory you can laterally move from system to system without being detected by modern day IDS solutions. FireEye also noted Mandiant is able to compromise domain administrator credentials within three days of gaining initial network access to an environment.

When we take a look at the Targeted Attack Lifecycle, stealing valid user credentials and privilege escalation are at the core of the attack chain.



(figure courtesy of Mandiant)

Stealth and persistence are key to targeted attacks. A compromised administrator account allows an attacker to silently pivot across multiple systems, perform internal reconnaissance, and ultimately steal targeted data. Shockingly, companies informed of a breach from an external agency (the majority) have been compromised, on average, for 320 days.

To protect against these attacks, FireEye has 2 key recommendations:

- Monitor Use of Privileged Accounts
- Implement Multi-Factor Authentication & Jump Servers

Conclusions and Solutions

2016 promises to be another year of innovation -- on the dark side and the light side -- in the cybersecurity world. Remediant is here to help -- our Privileged Access Management solution, SecureONE, helps you to deliver many of Mandiant's recommendations.

- **Breach detectio**n: SecureONE integrates with your SIEM solution to feed in information about privilege escalation -- successful and unsuccessful, authorized and unauthorized. Correlating these events with other security events across your ecosystem can massively improve your ability to detect breach situations and zero in on vulnerable endpoints.
- **Monitor use of Privileged Accounts**: It's 2am -- do you know where the credentials for your highly privileged account are? As Mandiant states in the report, "If you are on an IT or security team, know this: The bad guys are coming for you and they want your credentials".

SecureONE gives you the ability to see exactly when a privileged account is used, by whom. SecureONE can even stop the utilization of a privileged account if the utilization falls outside of established user behavior norms.

- **Multifactor Authentication**: SecureONE is a minimally disruptive way to implement Multifactor Authentication for your highly-privileged administrator accounts. Average users without privileged accounts see no change at all -- and we designed SecureONE with usability as the first principle. We integrate with nearly any existing second factor solution, or you can use the built-in second factor management solution that comes with SecureONE.
- **Credential Protection**: Instead of relying on Password Vaulting or other shared account approaches, SecureONE reduces your attack surface by reducing the quantity of highly privileged accounts in your ecosystem. This not only makes auditing systems easier, but also protects the credentials of your privileged and non-privileged accounts because they are never shared, nor stored.

About Remediant

Remediant delivers on our promise of Securing Innovation through market-leading Cybersecurity products. Our flagship product, SecureONE, brings CISOs, Data Center Managers and IT Security professionals the control and insight they need over privileged access -- the #1 attack vector in security breaches. Built by IT Security professionals for IT Security professionals, SecureONE eliminates critical attack vectors while providing deep audit logging and unparalleled usability.

SecureONE takes a completely new approach to securing privileged accounts. Attackers can compromise credentials in a number of ways -- man-in-the-middle attacks, pass-the-hash, key loggers and more. Once the credentials for a privileged account are compromised, hackers use that privileged account to pivot to increasingly more sensitive systems and infrastructure. SecureONE breaks the chain before it starts -- SecureONE eliminates the risk by eliminating your privileged accounts, while still making it easy for system administrators, help desk personnel, application administrators and other authorized users to perform administrative functions on the endpoints they maintain.

Remediant

www.remediant.com