WHITE PAPER

Remediant

REDUCING **PRIVILEGED ATTACK SURFACE**

REDUCING **PRIVILEGED ATTACK SURFACE**

HOW DO YOU MANAGE AND CONTROL YOUR ATTACK SURFACE?

This is the question that keeps IT security professionals up late at night. As soon as we begin to grapple with what our attack surface is, it grows and shifts. Those elusive edges of your attack surface become hard to define and even harder to protect.

Digital transformation, the Internet of Things, and our burgeoning WFH workforces have all grown our attack surfaces. This growth has accelerated even faster as we created environments during the pandemic where we could still do work while society's tethers to sanity, safety, and health threatened to come loose.

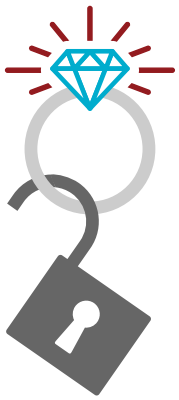
To seize control of the attack surface, you need to first grasp what (and how big) your attack surface is. You cannot defend an attack surface if you can't first define it—including its components. Reducing your privileged attack surface—a key component of your overall attack surface—also requires a continuous, comprehensive approach to managing your privileged access and implementing a just-in-time privileged access provisioning model.

Remediant SecureONE's v2.12 platform update makes reducing your privileged attack surface easier than ever before.

WHAT IS AN ATTACK SURFACE?

Perhaps ***NIST*** defines an attack surface best:

> *"The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment."*



Think of a table in your living room. Now, put something small on top of that table—like a diamond ring. The room around that table represents all the points of access (the attack pathways) someone can use to get to that asset, and steal it. There are lots of doors that grant access into this living room, but they are all locked. It seems like the ring is safe, but all attackers have to do to get into the living room is find a master key (privileged access). That master key will open all the doors, allowing attackers to enter and find the ring on the table.

As you check all the locks on those doors leading into that living room, the diamond ring becomes easier to protect. You know who has the keys to the doors, they're your privileged keyholders—and not unlike the privileged users in your network.

The size and security of your privileged attack surface very much depend on how well your control those keys. The size and security of your overall attack surface depend on your controls protecting all the points of access into that living room.

In your IT ecosystem, your attack surface contains all the places where cybercriminals can access your system and all the points where they can extract your data. An attack surface includes:

- The pathways for data and commands leading in and out of your system
- Your controls protecting these attack pathways
- Your valuable and sensitive data
- Your controls protecting that data
- Your privileged access management controls

That means that your attack surface includes software, your operating systems, and your web apps. But, it also includes web servers and data centers, laptops, workstations, mobile devices, and IoT devices. Physical controls like biometric access systems, employee access cards, even metal keys become part of your attack surface.

Consider that, and then consider the people in your system.

There are the people you don't know:

Anonymous users who aren't authenticated

And there are the people you trust with the life of your company:

The people with highly privileged access

Maybe you trust these helpdesk personnel, database administrators, and system administrators, but what happens if someone steals and assumes their identities in your system?

What happens if a savvy (or just lucky) cybercriminal employs a social engineering attack to get at your employees? What if they spoof a website and phish the log-in credentials of your employee?

Your attack surface reflects the vulnerabilities of your ecosystem. You can find vulnerabilities that affect your attack surface not just in your people, but also in your network and environments—even in your physical environment.

Before you can manage the attack surface, you need to know where it is, where you can be attacked, and how much digital real estate you need to protect.

HOW DO YOU MEASURE ATTACK SURFACE

Today's ubiquitous connectivity and always-available communications come at a cost: vulnerabilities and attack pathways. They're everywhere in today's IT ecosystems. And attack surfaces have never been larger.

So, where do you start when you want to measure and understand your attack surface?

The answer is Attack Surface Analysis or Insights.

STEP 1 MAP THE UNKNOWN

Thinking back to the example of the diamond ring on the table, how do you translate that to your systems, your network, your IT ecosystem?

First, map out your system. Show your devices, pathways, and networks. Break your internal attack surface into its components:

- Network Attack Surface: Hardware and software vulnerabilities
- Software Attack Surface: Vulnerabilities in code
- Physical Attack Surface: Security vulnerabilities in a physical location
- Privileged Attack Surface: Vulnerabilities inherent in the granting of privileged access

Remember to consider your external attack surfaces too, like your social engineering attack surface.

Completing an attack surface analysis will help you clarify your own perception of your architecture. The true value of mapping your attack surface is that it allows you to work with other SMEs, compare knowledge, and record more complete perceptions of your current-state IT security environment.

Build your attack surface analysis iteratively. If you haven't done this before, your first attempt at mapping your attack surface will be incomplete. Review the first drafts with subject matter experts and other stakeholders in your organization.

STEP 2 DETERMINE WHERE YOU'RE MOST VULNERABLE

What parts of your IT ecosystem face outward? How do people access your systems from outside your network?

Any pathway can become an attacker's entryway into your systems. Those vulnerabilities lie throughout your ecosystem. Here are some examples:

- An employee portal
- Your website
- VPN
- A stolen privileged log-in credential
- Excess standing privilege or 24X7 admin access
- An expired security certificate

You're most vulnerable where you offer remote access to the system.

Include these vulnerabilities in your map from Step 1. Don't just look for vulnerabilities, but also look for missing controls that could evolve into vulnerabilities in the future.

STEP 3 KNOW YOUR ASSETS

You also need to understand where your company's 'diamond rings' are. Where does your company keep the data it needs to protect? Consider confidential data, strategic data, regulated data, and data that is sensitive.

Companies can break down the assets in their IT ecosystem into three categories:

- The assets you know
- The assets you don't know
- The assets that aren't actually yours

Obviously, the assets you know will be the easiest to inventory. These will include your company's website, the servers, and everything that needs them to run.

Next come the unknown assets. Remember the website that the marketing team set up for that big campaign in 2018? No? That's because they didn't tell your security team. However, the website still exists even though it's been forgotten by the marketing team, which has turned over completely since 2018. Add to this list software that employees loaded on their own.

The scariest (and hardest) list to generate is the one that has the assets you don't control. These could include:

- a typosquatted domain,
- malware that cyberattackers loaded into your network,
- an app that impersonates your company

Even though you don't control these assets, they still play a role in your attack surface.

STEP 4 ACT

When you set out to reduce your attack surface, you can reduce the amount of code you have running, the entry points and attack pathways in your network, and infrequent services, to name a few. But, with 74% of breached organizations ***attributing their breach*** to a privileged account, doesn't it make sense to start with a deep dive into the privileged access lying dormant, but active across your network?

Start with your privileged attack surface. Excess standing privilege, a key—and often overlooked—component of attack surfaces, vastly enlarges your attack surface. When those credentials allow privileged access into your system, suddenly, your most valuable, strategic, proprietary information can be at risk.

It's your company's diamond ring.

That's when data breaches enter the conversation.

ATTACK SURFACE: MEASURE YOURS BEFORE SOMEONE ELSE DOES

You invest time, effort, and resources to measure your attack surface and to learn what vulnerabilities attackers can exploit in your network. So do attackers.

Attackers measure your attack surface when they're sizing you up for an attack. They find your attack vectors. They pick one and launch their attack.

ATTACK SURFACE: REAL-WORLD EXAMPLES

Remediant offers ***free demonstrations*** of SecureONE. We use them to spread the word on how we stop lateral movement by removing 24x7 admin access, a major result of growing attack surfaces. In fact, the v2.12 SecureONE platform update ***introduces*** privileged access risk dashboards that help users visualize and reduce their attack surface.

Two recent demos took us to Fortune 500 healthcare companies where we presented our proof-of-concept of Remediant SecureONE. Both companies asked us to help quantify their privileged attack surface. Both had a lot going for them:

- Heavy investments in Infosec and their IT control environment
- Significant capabilities in IAM and PAM
- Cultures that value and pursue security

So, what happened when we quantified their privileged attack surface?

The first company vaulted the privilege of just over 10% of their administrator accounts.

The second had vaulted 3%.

Both companies relied on their PAM solutions to vault their privileged access and protect them.

Both had vast quantities of unknown privileged access outside their vaults. Despite their sizeable investments in security, their privileged attack surfaces remained huge.

They were at risk because they had a vault that protected their credentials, but not the access to their resources.

PRIVILEGED ATTACK SURFACE MANAGEMENT

How do you manage that unknown access that's outside your vault? How do you find excess standing privilege so you can control it and reduce your privileged attack surface?

The answer comes down to getting continuous visibility into all your systems through SecureONE.

With SecureONE, you get dynamic visibility into your privileged access sprawl across your entire network. You see what you can't see right now.

Looking into the dark void of the unknown is big and scary. We know because we've been there.

It's big because defining your attack surface and then addressing it—seems like a big project. (And it can be without the right tools.)

It's scary because you learn about all the known and unknown admin access and that you're vulnerable to a breach. (But, wouldn't you rather know now than after it happens?)

Managing your privileged attack surface comes down to implementing some core strategies to reduce the standing privilege in your IT ecosystem. After you have followed the steps above and mapped, assessed, and inventoried your current privileged attack surface, how do you go about reducing your current standing privilege?

Reducing your standing privilege may not be a one-day job, or something that can be accomplished during a working weekend. The best approach may be to resolve your excess standing privilege over time by setting some time-based goals that ultimately lead to Zero Standing Privilege.

HOW CAN REMEDIANT HELP YOU GET TO ZERO STANDING PRIVILEGE?

1 Find your excess standing privilege

With Remediant's **Privileged Access Dashboard**, executives get a point-in-time view into total instances of users who have privileged access via group access and direct access.

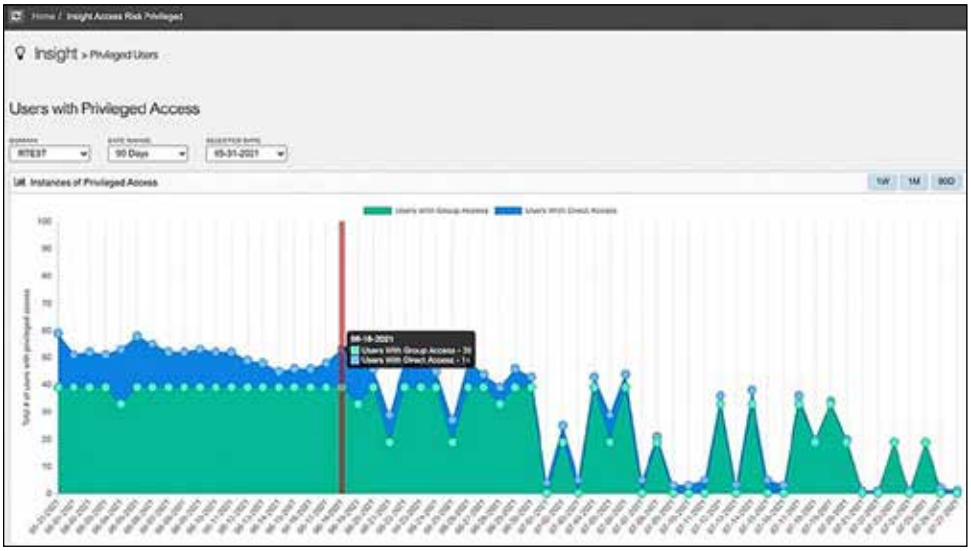


CHART 1: *Privileged Users Access Dashboard for Executives*

2 Fix your excess standing privilege & implement a *Zero Trust* model with MFA

Using Remediant's **Privileged Access Dashboard**, security practitioners can analyze and prioritize efforts to reduce the standing privileged access among the riskiest groups and users most likely to be compromised. You can enable Just-in-Time (JIT) administration.

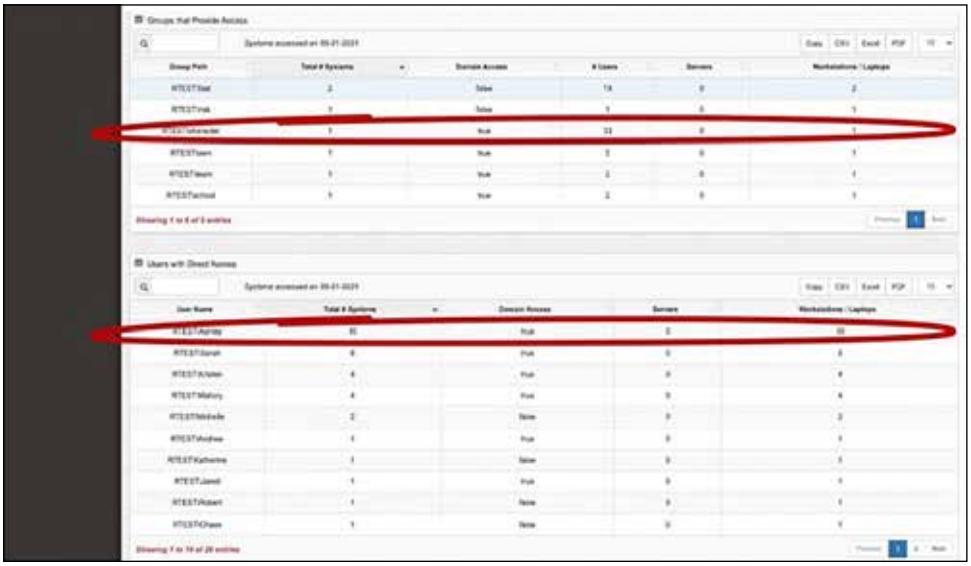


CHART 2: *Privileged Users Access Dashboard for Security Practitioners*

With Remediant's **Segregation Access Dashboard**, you can:

- Empower executives to see their organization's privileged access across tiers, e.g., workstations, servers, and domains to identify the users and groups that are most likely to be compromised.
- Enable security practitioners to see the users and groups with the most risk—by tier—(workstations, servers, and domains) so they can establish a plan to shrink the privileged attack surface.
- Stop lateral movement between tiers by removing excessive admin access and replacing it with JIT access as needed to achieve Zero Standing Privilege (ZSP).

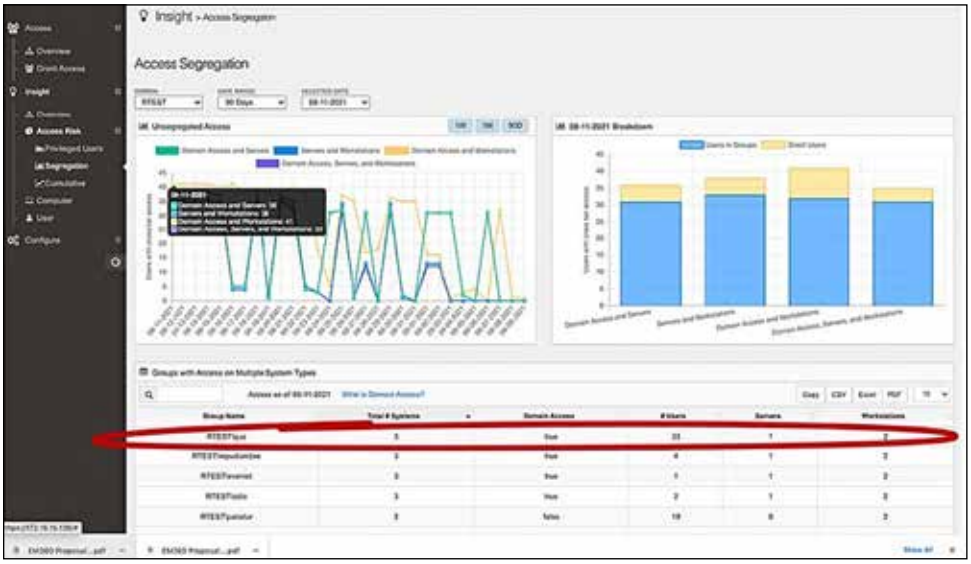


CHART 3: *Privileged Access Dashboard for Executives and Security Practitioners*

With Remediant's **Cumulative Access Dashboard**, you can provide executives with the total instances of privileged users based on the combination of workstations and servers at any point in time.

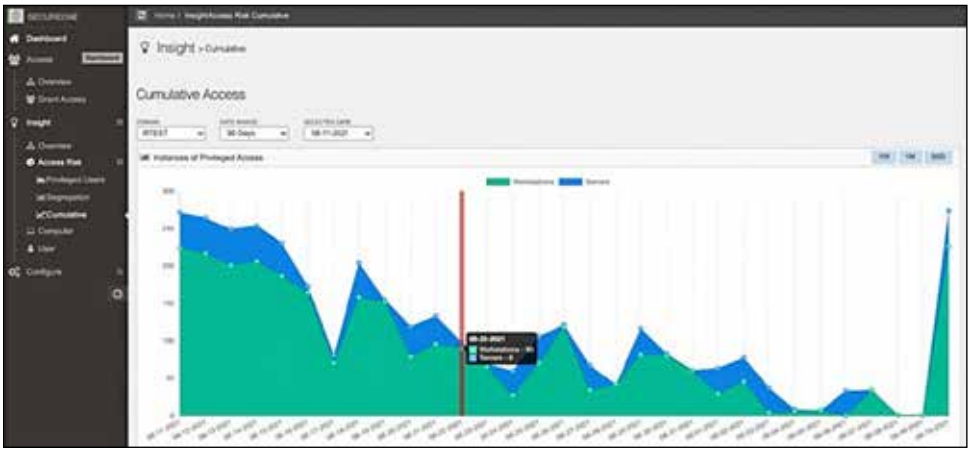


CHART 4: *Cumulative Access Dashboard for Executives*

The **Cumulative Access Dashboard** also allows security practitioners to obtain the average number of standing privileged access accounts per system which enables them to prioritize the removal of excess privileged access from the riskiest systems and then enable JIT admin access as needed with Remediant SecureONE.

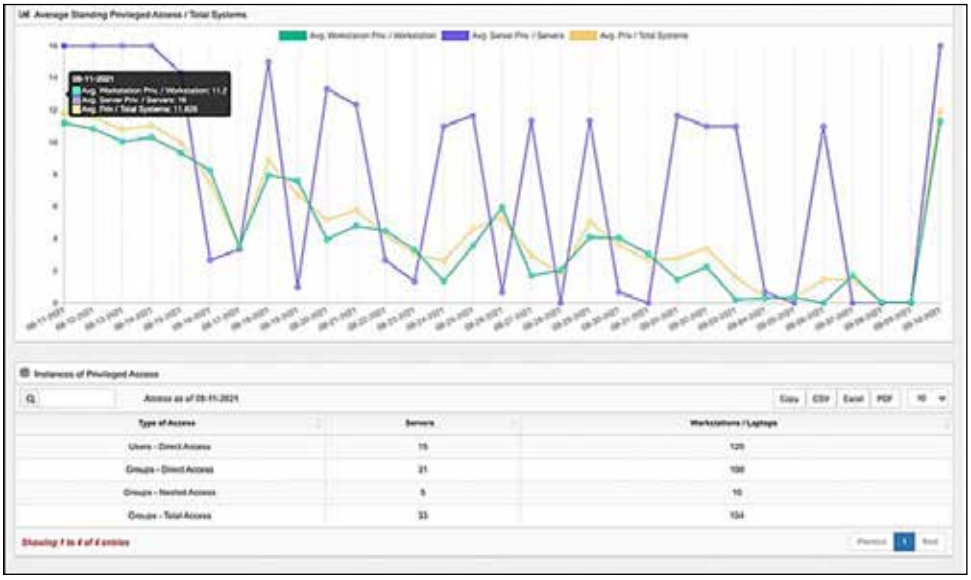


CHART 5: *Cumulative Access Dashboard for Security Practitioners*

AN ATTACK SURFACE STRATEGY FOR THE FUTURE

A true strategy for privileged attack surface analysis and attack surface management doesn't overlook a go-forward plan. How will you identify changes to your attack surface in the future? How will you evaluate and address these new risks?

You can compare your baseline understanding of your privileged attack surface with future versions of your attack surface once you begin to reduce your vulnerabilities. Just as important, though, is understanding how your attack surface has changed while you've been working to reduce it. When you evaluate the changes in your attack surface over time, ask:

- What's changed in the business?
- What new technologies, access points, or changes may have opened new vulnerabilities?
- What exposures could your improvements have created?

How to reduce your privileged attack surface: Implement Zero Trust

When employees—and third parties—go remote, your attack surface grows. No longer do employees need to be on your company's campus or even on your Wi-Fi to access your network and its assets. They don't even have to be on the same continent.

Each one of those accounts, and the privileges you assign to them, adds to your privileged attack surface, and the likelihood that the access you assign will be used against you.

Eliminating excess standing privilege on your network doesn't just reduce your external privileged attack surface; it reduces your internal privileged attack surface too.

Disgruntled employees can do as much (or even more) damage than an attacker from outside your company.

HOW REMEDIANT CAN HELP

There's no exact science on how to analyze and manage your attack surface. It's an exercise of bringing intuition, knowledge, expertise, and experience to this very important exercise of managing your company's risk of getting breached.

With the right tools and choices, you can manage your breach risk much more effectively, but only if you understand your attack surface and its vulnerabilities. By implementing a Zero Trust privileged access model for your administrators, you remove the 24x7 admin rights that cyberattackers reach for when they're breached your attack surface. Even if they hack into your network, it's much more difficult to wreak havoc if you've removed one of their favorite tools.

With a Zero Trust model, you revoke a credential's access to endpoints so it can't be used for lateral movement. Your privileged user will need that access again, and that's fine. With Remediant SecureONE, you can easily provision that access back on a time-limited, *principle-of-least-privilege* basis.

With SecureONE, you get a Zero Trust approach when you:

- Discover and remove privileged access sprawl
- Implement go-forward just-in-time access with MFA
- Reduce your privileged attack surface
- Protect against lateral movement attacks such as ransomware

When you adopt *Zero Standing Privilege* by using Remediant SecureONE, you can reduce an attacker's chance to exploit lateral movement in your system. They can't use a compromised credential to move laterally from endpoint to endpoint if you've shut off the access.

5.5HRS to enable just-in-time access on all servers

99% reduction in risk with no additional FTE requirements

1.5M human accounts with admin rights exposure discovered

SecureONE is easy to implement. It takes just 5.5 hours to enable across all servers and delivers an improved Total Cost of Ownership with its 99% reduction in risk with no additional FTE requirements. With SecureONE's new dashboards, you get point-in-time views into your privileged access sprawl that allow you to prioritize and address the problem. You can set up time-based goals and track progress toward reducing privileged access risk and your privileged attack surface.

You can move toward implementing Just-in-Time administration.

To date, Remediant's SecureONE has discovered 1.5 million human and 6.2k service accounts with admin rights exposure across our client base.

Remediant SecureONE continues its mission to lead the industry in providing Privileged Access Risk visibility and insights to executives and security practitioners. Through SecureONE's dashboards, organizations can now visualize, analyze, and reduce their privileged attack surface and prevent lateral movement attacks.

Get a *demonstration* of Remediant SecureONE with Privileged Access Risk dashboards today!

Remediant
Two Embarcadero Center, 8th Floor
San Francisco, CA 94111
(415) 854-8771 *www.remediant.com*