WHAT IS ZERO TRUST?
WHAT IS ZERO TRUST?

IN ITS SIMPLEST TERMS, ZERO TRUST MEANS GRANTING USERS JUST WHAT THEY NEED, WHEN THEY NEED IT, AND NOTHING MORE.

As a cybersecurity strategy, Zero Trust has evolved to protect today’s increasingly digital business environments against a rapidly changing threatscape. It owes its beginnings and its existence to its founder, Forrester alum John Kindervag who succinctly boiled down its tenets and practices to one concise mantra: “never trust, always verify.”

As the tech universe expands to increasingly embrace new technologies like cloud-based solutions, SaaS applications, virtualization, AI, and robotic process automation, Zero Trust has emerged as a key model in protecting companies beyond the perimeter safeguards they have turned to in the past. Those ‘fences’ no longer work against today’s cyberthreats.

In a threatscape where cyberattackers can launch their attacks over the fences of perimeter-based security or even attack from inside the fence by hijacking trusted accounts, Zero Trust offers measures that can protect against these attacks and mitigate the damage done by the attacks that do get through. Castles and moats no longer protected villagers in a world of flight. Perimeter-based control environments no longer protect companies against today’s cybercriminals. The time for Zero Trust is here.

3 WHERE DID ZERO TRUST COME FROM?
3 HOW DOES ZERO TRUST WORK?
4 THE MISCONCEPTIONS OF ZERO TRUST, EXAMINED
5 THE CASE FOR JUST-IN-TIME ACCESS
6 CONFRONTING ZERO TRUST INERTIA
6 RISKS OF IGNORING ZERO TRUST
7 IMPLEMENTING ZERO TRUST
8 LESSONS WE’VE LEARNED IN ZERO TRUST IMPLEMENTATIONS
9 HOW REMEDIANT CAN HELP
WHAT IS ZERO TRUST?

Where did Zero Trust come from?

When Zero Trust first emerged as a cybersecurity strategy, it had to compete with tried-and-true control methodologies like legacy PAM (Privileged Access Management). While it’s hard to stare up at the walls you’ve built over the years and decades and realize that they’re no longer protecting you, PAM’s effectiveness relied on a time when all privileged access resided within a company’s network. That’s simply not the case today with the proliferation of cloud environments, big data projects, and savvy cybercriminals, as well as established markets overseas that thrive on the profits of these crimes.

If perimeter-based security and legacy PAM built a system around vetting your visitors based on who they said they were, cloud technology and advanced persistent threats (APTs) made it possible for bad actors to steal the identities of your most trusted users and attack from within, using the privileges that companies reserved for the select few.

Zero Trust emerged from a security environment that needed more. Zero Trust scrutinizes standing privilege. It’s just-in-time (JIT) administrator access delivered when your administrators need it—not when cybercriminals find it.

Zero Trust embraces the principle of least privilege by granting authorized users the access they need, when they need it, and nothing more. With Zero Trust, you no longer leave the ladders along the castle walls at night, hoping that attackers won’t find them.

How does Zero Trust work?

Zero Trust was built on a series of four core concepts:

1. **Zero Trust means Just-in-Time Administration, not Just-in-Case Administration**

   When you adopt the Zero Trust model, all default access—all standing privilege—gets reevaluated. If that access can’t be justified—or if you’re leaving it active ‘just-in-case,’ it gets terminated. Just-in-case administration leads to excessive amounts of “standing privilege,” which opens your ecosystem up to big risk when there’s a breach.

   According to a 2020 Remediant study, 480 admins have 24x7 access to the average employee laptop in an organization with 10,000 endpoints. Without Zero Trust, just-in-case access can spread like a contagion.

   With Zero Trust and Zero Standing Privilege, you assume that the attackers have already breached your network and your perimeter-based security. The Zero Trust model implements just-in-time access, and works to ensure that all requests to access your system pass-through authentication, authorization, and encryption.

2. **Zero Trust means Recognizing the Value of Real-Time Monitoring**

   Breaches happen—even with the best controls in place and functioning as intended. Zero Trust integrates both preventive and detective controls. When a breach occurs, real-time monitoring helps minimize the damage an attacker does because your company becomes aware of the breach sooner. With real-time monitoring, your Zero Trust strategy is more able to identify, investigate, mitigate, and contain breaches because you’re actively watching for them.
WHAT IS ZERO TRUST?

3 ZERO TRUST COMBINES SEVERAL PREVENTIVE CONTROLS

Zero Trust builds on preventive controls that many organizations have already implemented, but combines them for a control environment that's stronger than the sum of its parts. Zero Trust incorporates:

**Micro-segmentation:** Zero Trust establishes smaller, more contained perimeters that mitigate attacks when they occur. When your perimeter sets up smaller zones, attackers can't move beyond their micro-segment if they've been walled in by a sound micro-segmentation strategy.

**Principle of Least Privilege:** Zero Trust means giving users what they need, when they need it, and no more. If an attacker hijacks one of your trusted accounts, the principle of least privilege will constrain their access and limit the damage they can do.

**Multi-factor Authentication (MFA):** Zero Trust means investing time and effort into your organization's authentication mechanisms. MFA strengthens controls around verifying a user's authorizations by relying on not one, but two or more identity verifications that can include: verification by email or text and/or token-based authentication, for example. Contextual authentication mechanisms are also gaining traction in the market writ large.

4 ZERO TRUST COMPLEMENTS YOUR OVERALL SECURITY STRATEGY

Any component of your security strategy has to align with your overall technology and business strategies. Zero Trust is no different. Zero Trust, when implemented properly, forms a core part of your security strategy, complementing and improving your existing control environment. If your Zero Trust model doesn’t align with other security components like endpoint detection and response (EDR), your enterprise and its assets remain at risk.

THE MISCONCEPTIONS OF ZERO TRUST, EXAMINED

**MYTH #1 ZERO TRUST ≠ ZERO TRUST IN YOUR EMPLOYEES**

Cybercriminals using hijacked security credentials don't care if you trust your employees to do the right thing. In fact, they're counting on the fact that they won't. Zero Trust assumes that criminals have already stolen the identities of your most trusted employees and that you have to minimize the damage that they'll do. Consider examples like:

- That access you granted your admin users for that weekend project in 2019
- That access you granted to Help Desk employees so they could meet their SLAs and resolve issues ASAP
- The access the Information Security VP needed just in case his directors got sick during COVID

Zero Trust roots out standing privileges that have gone stale and blasts them into the terminated column before rogue actors can seize and exploit them during a breach.

**MYTH #2 ZERO TRUST IS JUST FOR BIG COMPANIES**

Any text following the headlines about the 2020 SolarWinds attack begins to speculate about the depths to which it infiltrated the US Government and/or the nation's Fortune 500 companies. But, the whole truth doesn’t always get captured by the headlines.

All companies—not just the largest ones—face the threat of credential-based cyberattacks. With the average cost of a data breach in the US averaging $8 million, according to 2020 IBM/Ponemon Institute research, data breaches may be an even bigger risk for smaller companies since they may not have the resources to sustain the attack.

Many small businesses can't sustain the costs of a breach even though 43% of attacks are aimed specifically at them, according to Verizon. In fact, sixty percent of small businesses go out of business within six months of being attacked by cybercriminals.

Zero Trust costs time and resources, but it's time and resources invested into your business, not spent mitigating the damage and expenses caused by bad actors.
MYTH #3  ZERO TRUST MEANS GOING ALL OUT, ALL AT ONCE

To get Zero Trust implemented right and working as intended, you need to start small, with 40 to 50 users/workloads and take the time you need to grow with the model. As you successfully implement Zero Trust, piece by piece, across your organization, the model can be evolved out to successively larger groups.

Too often, companies often go too big, too fast, rolling out Zero Trust to thousands of users at once. That temptation to “go large” will always exist for larger companies with thousands of users, but Zero Trust implementations on a large scale require resources and timeframes on a large scale too. Patience stretches thin and decisions loom large. Many of those Zero Trust implementations fail before the companies even get to see the model’s true value.

MYTH #4  ZERO TRUST MEANS STARTING FROM SCRATCH

Zero Trust doesn’t mean a brand new network architecture. Zero Trust is a journey; it builds on the network architecture you already have, not one that has been ported in from some best-practice company or ivory castle academic. Zero Trust works in the real world because it is real world.

Zero Trust works with your existing architecture and enhances it, relying on principles like MFA, SSO, and risk-based access and then builds in measures to limit lateral movement and enforce zero standing privilege through Just In Time Administration. Lastly, Zero Trust teaches organizations to proactively monitor everything. Zero Trust prepares you for the worst: when cyber-attackers succeed in breaching your network, your response can be both swift and effective if you’ve done the work to prepare for it. Assume compromise and plan accordingly for it.

THE CASE FOR JUST-IN-TIME ACCESS

When many organizations first commit to implementing the Zero Trust model, IT groups find that they have a system based on complete trust for their most powerful users and a model of just-in-case administration that helps these users meet the SLAs the company needs from their technology to keep operations going. Indeed, many risks in an IT security environment rise up despite the best intentions and incomplete confidence in methodologies like PAM.

The risks of solely relying on Privileged Access Management and just-in-case administration are just too great in today’s expanding threatscape. With ransomware on the rise and increasing numbers of workers going remote, leaving privileged access ready and waiting for attackers who breach your perimeters is just too dangerous. The Verizon Data Breach Investigations Report found that 29% of all attacks relied on the use of a stolen credential. Those stolen credentials, especially when they provide the always-on privileged access of a trusted user, render perimeter-based controls useless as cybercriminals speed across your breached network, stealing data, and deploying ransomware.

Zero Trust delivers just-in-time access when it’s needed, not when attackers find it during a breach. Implementing the Zero Trust model integrates many best-practice preventative control methodologies into a company’s control environment.

Some core components of a complete Zero Trust model include:

| Identity verification | Micro-segmentation | Endpoint Detection & Response (EDR) | Least privilege | Multi-factor Authentication (MFA) |

Initially, Zero Trust requires a considerable investment of time and resources to implement—and implement right—but the time it saves downstream, when it minimizes damage and provides ransomware protection during a breach proves its worth.
Confronting Zero Trust Inertia

Even ten years on, the Zero Trust model isn’t always a quick sell to IT groups. Bring up Zero Trust in any meeting on IT security controls and someone at the table might give you an eye roll and will likely start pointing out:

- The skills it takes to implement Zero Trust
- The costs to support the model, and
- The time requirements to get Zero Trust up and running

And the naysayers are not completely wrong. Implementing a Zero Trust model takes time, money, and SME effort. After all, in implementing Zero Trust, you’ll have to:

- Assess your attack surfaces
- Create and prioritize an inventory of your IT assets
- Assemble the controls that will form your IT control environment, and
- Establish a system of continuous monitoring

All of these measures take time. But, few people will argue that any of these efforts aren’t worth that time or the money it will take to get them right.

When you suggest Zero Trust as an initiative that makes all of that happen right now, with a properly resourced plan encompassing all the right control activities, executive eyeballs grow big and executive budgets get nervous. This is when it’s time to consider that:

- Many IT groups have already implemented components of Zero Trust, sometimes without even realizing that micro-segmentation, the principle of least privilege, or MFA are all steps on the road to a complete Zero Trust implementation.
- The costs of installing Zero Trust are often must less than the costs of remediating a breach and repairing the reputational damage your company may sustain in its wake. According to a recent IBM/Ponemon Institute report, the US is the costliest country in the world in which to experience a breach; the average cost of a breach here exceeds $8 million.

When you consider that 78% of attacks on web applications use a stolen credential, the case for spending time, money, and people on a Zero Trust implementation right now gets a lot stronger.

Risks of Ignoring Zero Trust

The cost of an average breach—$8 million—can go a long way, especially when you’re not using it to recover from a breach. But, beyond the pure costs that companies incur in remediating the effects of a breach, there are other costs, more difficult to quantify, that should also be considered like:

- Ransomware, and its insidious harm to your network as it lurks before it’s identified
- Reputational risk, and the loss of your clients’ trust following the breach

Consider the press that the 2020 SolarWinds attack received.

According to a 2020 Remediant study, 480 admins have access to the average employee laptop in an organization with 10,000 endpoints. That same research went on to find that 1,291 admin accounts had access to more than 2,000 systems in that same representative organization.

Indeed, the SolarWinds attack appears to have weaponized stolen privileged accounts with 24x7 access to move laterally across systems, infecting customer endpoints with infected updates.

While $8 million is the cost of the average breach, the costs of many breaches far exceed that amount. For example, the total cost of the NotPetya breach at Merck approximated some $1.3 billion, and other high-visibility attacks at companies like Maersk ($300 million) and Nuance ($92 million) show that the risks of ignoring today’s best-practice controls and models like Zero Trust may build up to vast sums of money very quickly.
IMPLEMENTING ZERO TRUST

In a world where perimeters no longer stop cyber-attackers, identity becomes the attack surface. In fact, 74% of breached organizations admitted that their breach involved access to a privileged account, according to the Verizon Data Breach Investigations Report (DBIR).

Exploiting the access granted by accounts belonging to your most trusted users is the hallmark of today’s most successful breaches. More than perimeters, identity becomes the new walls an enterprise sets up to prevent and mitigate breaches.

That means ensuring the right person is on the network and right-sizing their access so that resources are not exposed or abused, even if the identity is compromised. That means implementing Zero Standing Privilege (ZSP) as a first and key step toward achieving a true Zero Trust model. Zero Standing Privilege lies at the very core of the Zero Trust Model. Without ZSP, you cannot have Zero Trust.

MEASURING STANDING PRIVILEGE

You can’t protect what you can’t see! To get to Zero Standing Privilege, you have to know which standing privileges you’re starting with, or which administrator credentials already exist. To measure standing privilege, you need to:

1. Discover and identify persistent accounts across workstations and servers
2. Map out admin access on a system-by-system basis
3. Measure changes to access over time (new admin users added, terminated admin users never removed, etc.)

Once you have measured the standing privilege in your organization, you can manage it, protect your enterprise environment, and achieve Zero Standing Privilege when you:

**Freeze systems so net new admin access cannot be created**

Admin access is a slippery slope in many organizations. It’s granted when the help desk needs to resolve issues fast. It’s the grease that keeps the business’ engine running when you’re facing a pressing deadline. But, every admin credential you create provides a potential gateway for a future hacker to exploit during a breach.

Once you’ve measured and inventoried the standing privilege, the next step is to “stop the bleeding” by stopping the creation and/or bifurcation of new administrator accounts. For this to work, companies have to freeze this access across all systems, e.g., Windows, Mac, Linux, and across all access types (local, group, domain).

**Review access and remove access no longer needed**

After you’ve stopped new admin access from being created, it’s time to review the access you have. Which accounts do you need? Which accounts do you need right now (not yesterday, not tomorrow, not just in case)?

For any accounts that land in the “no longer needed” category, their access should be revoked and reprovisioned back only when the need arises again.

**Move to a Just-in-Time (JIT) model for administrator access**

The last step in achieving Zero Standing Privilege is to move to a model where administrators are granted Just-in-Time access when they need it, where they need it, and for the task they’ve been assigned. To avoid Just-in-Case administration, that access should be revoked as soon as the task has been completed. This is fronted by Multi-Factor Authentication (MFA).

**Risk-based approach**

When implementing Zero Trust, take a risk-based approach. Start with the users you trust the most and who have the highest level of access—your administrators, developers and other users with elevated or privileged access.

Scrutinize their access. Zero Trust means that you don’t provide administrators 24x7 access into perpetuity. You move toward just-in-time Zero Trust access. In the long run, despite Zero Trust’s costs, it’s worth the time and effort.
LESSONS WE’VE LEARNED IN ZERO TRUST IMPLEMENTATIONS

After committing to Zero Trust, many companies, especially large companies, often try to accomplish too much, too soon. Large companies have big resources, big pockets, and big initiatives. They become convinced that the Zero Trust Model will help them, and then decide to roll it out to thousands of users.

But, to move toward a successful Zero Trust implementation, there are some core steps we’ve learned along the way that will help you—whether you’re a large company or one with just a few users.

<table>
<thead>
<tr>
<th>Appoint a project champion</th>
<th>Design an informed project plan</th>
<th>Prioritize communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>With a Zero Trust implementation, you need a point person, a person who is both responsible and who can take on responsibility. Your project champion needs to be a key resource within your company, someone who understands both the technical side of the implementation and the logistics of how to make it happen.</td>
<td>After you have your Zero Trust project champion, you need a plan to get the implementation done. Like any effective project plan, a good Zero Trust project plan:</td>
<td>Communicate early, often, and truthfully. We’re all hit with a lot of communication and noise. It comes from internal sources and from outside our companies.</td>
</tr>
<tr>
<td>Your Zero Trust champion probably shouldn’t be a C-level person, because they’ll need time and focus to get into the weeds. But, they’ll need to be high up enough into the org chart to have an understanding of your business, your company, and who needs to be at the table as you design the project plan and determine how to get it done.</td>
<td>1. Sets expectations and requirements clearly</td>
<td>In any company, complaints will surface that this implementation will be too much, too soon.</td>
</tr>
<tr>
<td>Once you’ve picked your project champion, give them the resources they need to get the implementation done right. That means time and people. If your company’s resources allow it, consider making this role their full-time job so that its priorities won’t conflict with their ‘day job.’</td>
<td>2. Makes sense for your business and its realities:</td>
<td>You can help confront these complaints—or even prevent them—by communicating about the project, why you’re undertaking it, and the value it will provide in the future.</td>
</tr>
<tr>
<td></td>
<td>• No project plan is one-size-fits-all across companies and industries</td>
<td>Communicate the Zero Trust project, and the plan for the project. Some of the important points to make are that the Zero Trust implementation:</td>
</tr>
<tr>
<td></td>
<td>3. Lays out how the implementation will proceed</td>
<td>• Confronts a problem like privilege sprawl and works to fix it, and</td>
</tr>
<tr>
<td></td>
<td>• Will the implementation roll out by location, region, or SBU?</td>
<td>• Addresses the huge risk of standing privilege</td>
</tr>
<tr>
<td></td>
<td>• How long will the implementation take?</td>
<td>A Zero Trust model will also shine a light on the massive problem of unchecked service accounts that lurk within many enterprises. Most companies have many more service accounts than they need. Zero Trust can help you address this risk, clean up these accounts, and help you design a better go-forward process for better access control in the future.</td>
</tr>
</tbody>
</table>
HOW REMEDIANT CAN HELP

With Remediant's SecureONE, you can stop ransomware by implementing the Zero Trust model and removing the 24x7 admin rights that cyberattackers seek and exploit during a breach. Without always-on, just-in-case admin access, privileged accounts get revoked when they’re no longer needed, and that access can no longer be weaponized to move from one machine to the next in a breach.

SecureONE helps you get Zero Trust implemented in your organization by:

• Discovering privileged access
• Removing privileged access and shrinking the attack surface
• Providing ransomware protection by preventing lateral movement
• Administering just-in-time access with MFA, going forward

Averaging just 5.5 hours to enable just-in-time access on all servers, Remediant SecureONE offers faster time to value and delivers an improved Total Cost of Ownership with its 99% reduction in risk with no additional FTE requirements.

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