WALLIX
CYBERSECURITY SIMPLIFIED

The What, How, and Why of
Zero Trust Cybersecurity

The What, How, and Why of Zero Trust Cybersecurity

TABLE OF CONTENTS

As naming goes, Zero Trust is easily understood. No one is trusted implicitly. In terms of cybersecurity, organizations should trust no one, whether an insider or an outsider, with unverified access to sensitive IT assets. That's not to say, of course, that no actor should ever be *granted* privileged access to network resources, which would obviously be an unworkable state of affairs; rather, it requires a security scheme that constantly requires users to not only prove who they are, but also to prove that they have both the need and the authorization to access said resource before entry is granted.

In other words, many other security paradigms assume, at least somewhat, that activity is legitimate until proven otherwise. Zero Trust, on the other hand, assumes that no activity is by default legitimate -- and therefore requires proof to the contrary before allowing privileged access to sensitive resources. **Zero Trust demands equal opportunity verification of credentials, identity, and permissions.** It's important to note that Zero Trust does not assume that all users are bad actors; rather, it simply requires that "proof positive" be provided that access to a privileged resource is appropriate.

That Zero Trust should be an important facet of cybersecurity is also easily understood when considering the damage that can be done to individuals and to a company's bottom line when valuable resources are accessed without proper verification. Whether such access is on the part of an internal admin or an external hacker is of little consequence, because the damage done can be extreme in either case. Indeed, the goal of every hacker is, in some way, to give themselves internal admin authority -- and that's what makes Zero Trust such an important part of cybersecurity.

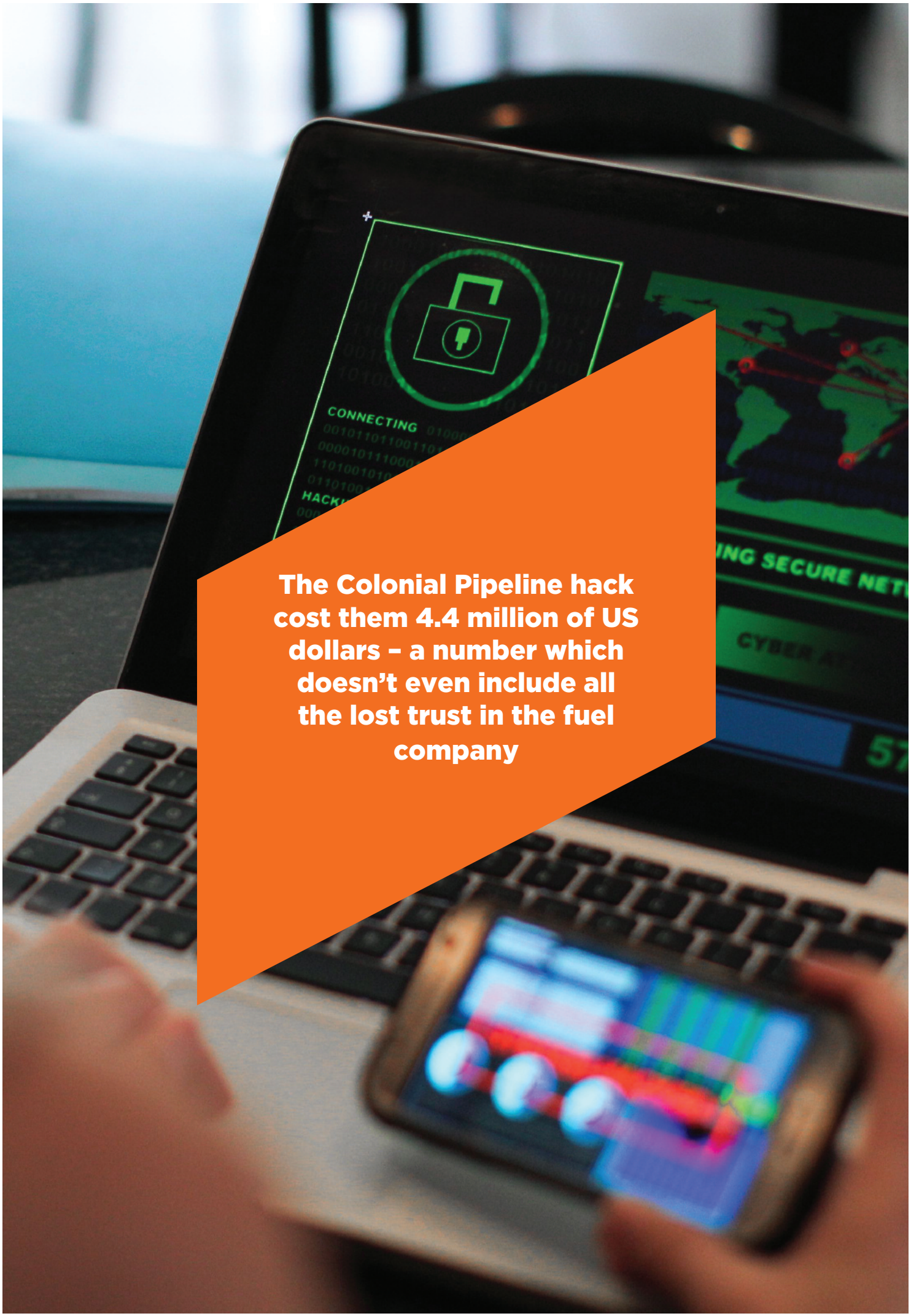
Trust no one with unverified privileged access to sensitive resources

The IBM 2021 Cost of a Data Breach Report provides a particularly illustrative overview of the need for Zero Trust. The report highlights how companies that have suffered a data breach but whose Zero Trust implementation is at a mature stage manage to preserve up to nearly $2 million more than those organizations that have not yet implemented a Zero Trust approach. Because privilege misuse can be mitigated by Zero Trust policies, such findings show how widespread the need is for this kind of approach to security, regardless of vertical.

TOO MUCH TRUST: RECENT CYBER ATTACKS

If the IBM report shows the breadth of the problem, two recent examples are illustrative of the depth of damage that can be done to a company via a breach. In the first incident, the American healthcare administrative-service provider CaptureRx suffered a ransomware attack in February 2021 that affected 2.42 million individuals from different companies. Among these organizations was Walmart, the world's largest retail corporation, which saw its customers' personal health information (PHI) exposed - including their full names, Social Security numbers, account numbers, insurance and private treatment information, etc. The company has paid a high price for this breach: Customers have filled lawsuits against Walmart's negligence. Because CaptureRx is a third-party provider, Zero Trust policies would have meant better control over access to their data and would have gone a long way towards minimizing the amount of personal data that was compromised.

The other enormous hack of 2021 has been the Colonial Pipeline ransomware attack, which also resulted in huge financial costs for the company. In this instance, an inactive VPN account allowed hackers to gain access to this major US fuel pipeline — and since there was no notion of Zero Trust in place, the holders of those privileges were then able to gain access to the private data of nearly 6,000 current and former employees. The compromised data ranged from tax IDs and driver's license numbers to contact and healthcare information, equivalent to 100 gigabytes. Colonial Pipeline finally had to pay 75 bitcoins, which was $4.4 million in May 2021.



The Colonial Pipeline hack cost them 4.4 million of US dollars – a number which doesn't even include all the lost trust in the fuel company

How to Have No Trust

Require proof positive that attempts at privileged access are what they claim to be

Implementing Zero Trust obviously doesn't mean that no user is ever granted privileged access to sensitive resources. What it does mean, however, is that "proof positive" is required that access attempts are not malicious – and thus, a Privileged Access Management (PAM) system should be in place to verify the validity of any and every attempt to access or modify critical resources. In so doing, the PAM system should be validating privileged access attempts according to the following criteria:

1. The user must prove who they are
2. The user must have the necessary privileges to access the resource in question
3. The circumstances of the privileged access must be appropriate
4. Monitor and log everything for assurance, tracing, and audit

Everyone must prove who they are

As evidenced by both recent hacks, a username / password combination alone is not enough to prevent unauthorized privileged access. Usernames and passwords are frequently targets of phising attacks, or else have been stolen in some other way – from an internal

Users inside of a system protected only by a username and password should not be trusted to be who they claim

database, for example, or even from a contractor who happens to have a username and password for the system. Because the ways in which a hacker might gain an otherwise legitimate login are so varied, users inside a system protected only by a username and password cannot be assumed to be who they claim to be.

Because such logins alone cannot be trusted, what is needed is a way to add verification to the login procedure to prove a user is who he or she claims to be

– and that's precisely what **multifactor authentication**, or MFA, provides. MFA requires an second "factor" in addition to something you know, such as a username and password, because something you know can also be learned by someone else. Thus, MFA requires users not just to know something, but also to provide other verifying factors that are unique to an individual. This is commonly something like a phone, to which the system can send a code when the user attempts to login as a secondary layer of verification that the credentials are being used by the authorized person.

The idea behind requiring multiple factors of identification is that it's very unlikely that a hacker will have stolen both a user's credentials as well as physically stolen their phone. It provides additional proof that a user is who they purport to be – and thus, the use of MFA at system entry points is an important part of implementing Zero Trust.

Defining privileges

to sensitive resources

Beyond identity, the right to access specific resources must also be demonstrated

A user proving who they are should only be the first line of defense. The Zero Trust paradigm requires that, even once inside of the system, users should only be granted the least amount of privileges needed in order to accomplish their necessary work tasks. Such granting of privileges is commonly role-based: Database administrators, for example, will have access rights to the databases themselves – but will have no need for administrative access to email servers. Zero Trust requires that every instance of attempted privileged access is validated against the PAM system. Thus, in this example, a database administrator attempting to access an email server they have no business on will be denied: They're an admin, but not one with privileges to that particular system. In this respect, the **Principle of Least Privilege** is a Zero Trust policy with a view to ensuring that no one is granted privileges by default,

but only to the minimum resources necessary, when and where necessary, to eliminate temptation, exposure, and undue trust.

In order to accomplish this, of course, all privileged resources inside of a system should have granular definitions as to which users and roles are allowed which privileged to access them – and the system should also allow for one-off access when it's required, a task which pays off in terms of both flexibility and security. Suppose, for example, that an outside contractor has been hired to apply a patch to one particular server out of many. With a proper PAM solution and a security team following a Zero Trust model, the contractor's login can be granted privileged access for the timeframe needed and restricted to only the machine on which they're performing work.

Privileged access must be monitored for When and How as well as Who

Access under proper circumstances

The Zero Trust principle should also be applied on a level that's more granular than a simple role-based schema. Privileged access rules should encompass not just who is attempting the access, but also define the circumstances under which such privileged access is allowed. This extends to both time periods – contractors are only granted access privileges during a defined maintenance window, for example, or employees only have access during normal work hours – as well as to location and, of course, to specific files and actions within the resource. Certain privileged users will never need the ability to delete an entire file set, or to access a specific sub-folder, and thus these activities can be disallowed.

To extend the contractor example, if he or she will access the system remotely then privileged access can be restricted to known, whitelisted locations or IP addresses, and only during a specified time frame during, say, normal business hours. Having a PAM system capable of such granularity and control is important, because it acts as a filter for privileged access attempts even if logins have been stolen, and even if the stolen logins

otherwise would have appropriate privileges.

Monitor and Log All Activity

To make all of the above protections work (and workable), it's important that all session traffic is monitored in real time. This is another area wherein a strong PAM solution can help put the principles of Zero Trust into action by ensuring that any action taken while in a privileged session is both authorized and legitimate; without this kind of real-time visibility, the entire premise of Zero Trust is undermined.

Because Zero Trust takes a "better safe than sorry" approach to security, any suspicious sessions should be terminated immediately

Numerous repeated attempts to access sensitive resources such as might be seen during a brute-force attack should not be permitted, for example – and therefore, any session that's engaging in such repeated attempts should be automatically terminated. Indeed, the same holds true of any suspicious session activity: even an otherwise innocuous internal user will have their session monitored and flagged for any unusual or unauthorized activity, however innocent. Because Zero Trust takes a "better safe than sorry" approach to suspicious session activity, any such session is automatically (or manually, based on alerts) terminated rather than allowing potentially risky activity to continue.

Real-time monitoring of session activity is critical – but alongside monitoring should also come the recording of all session activity, to include OCR recording of clicks, keystrokes, and CLI commands. This is important from the Zero Trust perspective because, as a last line of defense, it allows for review of sessions that might reveal breaches that, for whatever reason, were able to penetrate all other defenses. Recording of sessions can also facilitate incident recovery by allowing network staff to reverse mistakes like accidental file deletion, or to catch honest mistakes that might have led to network errors. Recording of session activity also allows for robust security

training based on actual network session activity, while also delivering the auditing capabilities and proof of compliance required by critical security regulations and industry standards.

No Privilege? No Visibility

As commonly seen in cyberattacks of all shapes and sizes around the world, once inside a network, ill-intentioned users are able to bounce around from resource to resource. Applying the Zero Trust principle, however, means that the system must approve all privileged access and limit access to only those resources or assets necessary to accomplish a task. Thus, as a result, sensitive resources are hidden from the view of users who do not have privileges to access them. A privileged user, once vetted and admitted through login credentials and multi-factor authentication, still only sees those resources to which he is granted permissions – no more, no less.

For example, our third-party contractor has privileges to the one server on which they need to work – and will not even be able to see other servers, databases, or sensitive assets housed on the network. Applying Zero Trust in this way prevents all users, whether they're employees, contractors, or hackers, from being able to even attempt to access many critical resources in the first place simply because of the fact that they are not aware that they exist. And even if they are aware or can surmise that assets exist, not being able to see them can stop lateral moves across the network.

No one should be able to see sensitive resources to which they are not privileged.

Conclusion

It's common and understandable that companies will have varying levels of trust. Hackers, of course, are never to be trusted, while contractors are typically somewhat trusted and, very often, employees completely trusted. When paired with the assumption that active users inside of a system inherently belong there, this leads to the false conclusion that users can be trusted. **But a user is not inherently trustworthy**, even internal

employees. In fact, the goal of every hacker is to get inside of a system for this very reason – to become an insider threat – and this alone makes trusting internal users by default a dangerous proposition.

Users should only be afforded privileged access when they can demonstrate all of Who, What, Where, When, and How

The astonishing number of data breaches that are accomplished through misuse of privileges means that Zero Trust is a security paradigm that needs to be applied to all users within a system, regardless of their purported identity. Zero Trust makes no assumptions; no activity is considered safe without enacting key steps towards proving identities and privileges are valid. All users, whether internal or external, should only be granted privileged access to critical assets if they can demonstrate all of Who, What, Where, When, and How – and this is exactly what Privileged Access Management, in conjunction with MFA and other security tools, is designed to provide.

about WALLIX

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

WWW.WALLIX.COM

WALLIX
CYBERSECURITY SIMPLIFIED