Building an Active Defense Plan From a Pen Test Report

A Guide to Finding Active Defense Opportunities

EBOOK

Table of Contents

Introduction

Penetration test reports tell a story. The story of how the team managed to break into your environment. A critical component often missing from these reports is the rationale behind the choices made by the pen testers who ran the assessment.

- Why did they go after a particular account?
- Why did they target a specific set of servers?
- Why did they choose one lateral movement technique over another?

Asking questions like these allows you to deconstruct choices that real threat actors might make in your environment. Understanding those choices will give you some active defense opportunities.

In this guide, we used a pen test with the objective to access a customer database (DB).

As part of the assessment, the pen testers followed these seven steps:

1. Established a C2 using PowerShell.
2. Enumerated the Active Directory domain for users and groups, specifically privileged groups.
3. Enumerated the domain to find computers.
4. Attempted privilege escalation and compromised the domain admin.
5. Scanned a subset of computers to identify the customer DB.
6. Used the domain admin account to login to the database server.
7. Logged into the Customer DB.

In each of these steps, the pen testers made some choices. Deconstructing these choices can help you build better defenses.

Deconstructing a Pen Test Report To Find Active Defense Plays

The MITRE Engage framework for Adversary Engagement (formerly MITRE Shield Active Defense Matrix) was released by MITRE to provide a framework for identifying opportunities where adversary behavior can be influenced to enable defenders to easily spot threats.

The foundation of the Active Defense approach rests on three principles:

1. Beat the human behind the software.
2. Do simple things that the adversary does not anticipate, to encourage or complicate their operation.
3. Make sure the things that you do allow the corresponding telemetry to stand out (i.e. collect more effective telemetry).

In the following pages, we'll deconstruct each of the 7 steps from the pen test report to identify Active Defense opportunities.

#1 – C2 Using PowerShell

WHY DID THE PEN TESTERS USE POWERSHELL?

- Sophisticated, off the shelf tooling.
- PowerShell logging & blocking not widely implemented.
- Great obfuscation capabilities.

ACTIVE DEFENSE OPPORTUNITY

Block PowerShell to force the adversary to use non–PowerShell options.

ADVANTAGE

Since PowerShell usage for C2 is fairly common, it reduces the risk of being hit with commodity malware that uses PowerShell, even today.

#2 – Enumerated the Domain for Users and Groups

WHY DID THE PEN TESTERS ENUMERATE THE USERS?

- To find privileged group members like Domain Admin (DA) and Enterprise Admin (EA). Successful compromise of a DA/EA will almost certainly result in customer DB access down the line, so it's important to know who they are.
- Run keyword searches across attributes like username, SPN, description, etc. to find accounts that can be used for SQL logins. Example 'SQL', 'DB', 'etc'. This will be useful when it's time to figure out how to login to the database, regardless of whether you have admin credentials or not.

ACTIVE DEFENSE OPPORTUNITY

Deploy attractive decoy accounts, assign high-value privileges, and setup attribute level auditing on description, SPN, etc. to monitor enumeration attempts. This has the added advantage of detecting password spraying regardless of intensity and staggering strategies.

ADVANTAGE

Gain insight into enumeration activities being conducted against the domain from a user perspective. (Note: Don't use these accounts for any operations. There are ways to make this Operations Security (OPSEC) safe)

#3 – Enumerated the Domain for Computers

WHY DID THE PEN TESTERS ENUMERATE THE COMPUTERS?

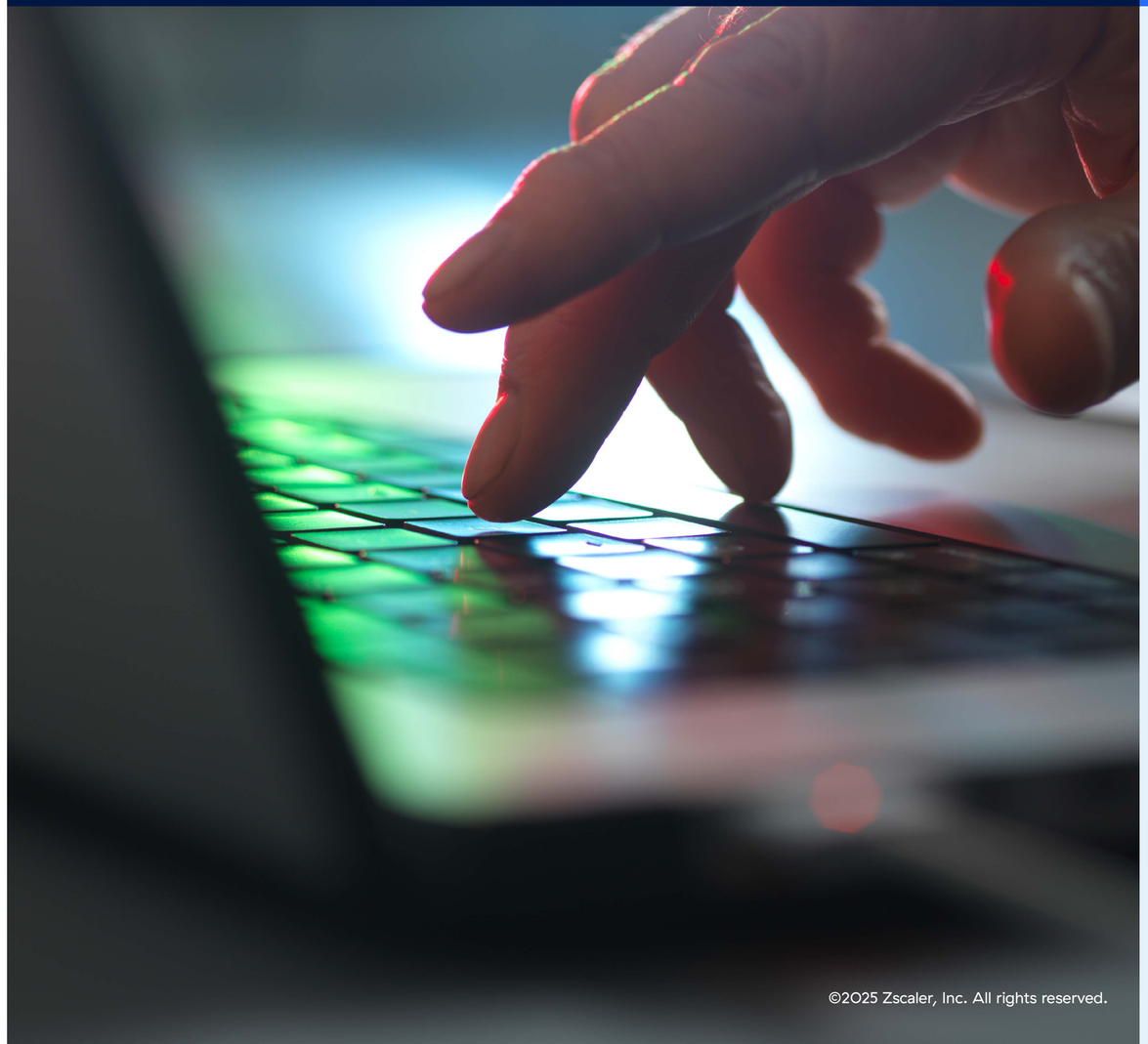
- Run keyword searches across attributes like hostname, SPN, and description to find accounts that could be SQL servers. Example ‘SQL’, ‘DB’, ‘etc’. This will be useful when it’s time to figure out where the DB is located.

ACTIVE DEFENSE OPPORTUNITY

Deploy decoy computers, assign attractive hostnames to databases, and setup attribute level auditing on description and SPN, to monitor enumeration attempts.

ADVANTAGE

Gain insight into enumeration activities being conducted against the domain from a computer perspective.



#4 – Privilege Escalation

WHY DID THE PEN TESTERS ESCALATE PRIVILEGES?

- To get closer to the target privilege level, which in this case is the database/server administrator on the customer database.
- Escalated privileges can allow you admin access to one, few, many, or all systems on the network.
- With high privileges, you can log in to more systems and steal credentials.

Let's assume that Kerberoasting was the privilege escalation technique that worked. In this case, let's also assume that the service account was a domain admin.

WHY KERBEROASTING?

- It targets service accounts such as those that have an SPN attribute configured.
- Service account passwords never expire.
- Sometimes, service accounts often have admin privileges and may be granted domain admin.
- Many service accounts are extremely old and have weak passwords.
- It's really difficult to detect on the wire.
- Logs related to service ticket operations are not logged by default. If they are, it is difficult to tell the difference between legitimate and malicious service ticket operations.

#4 – Privilege Escalation (Cont.)

ACTIVE DEFENSE OPPORTUNITY

1. Setup a decoy kerberoastable account, assign attractive usernames to databases (e.g. SQLAdmin), add a SQL-related SPN (e.g. MSSQLSvc/custdb.domain.com), and write a rule to capture Event ID 4769 for the decoy account.
2. Remove the real domain admin service account from being kerberoastable or downgrade its privileges.

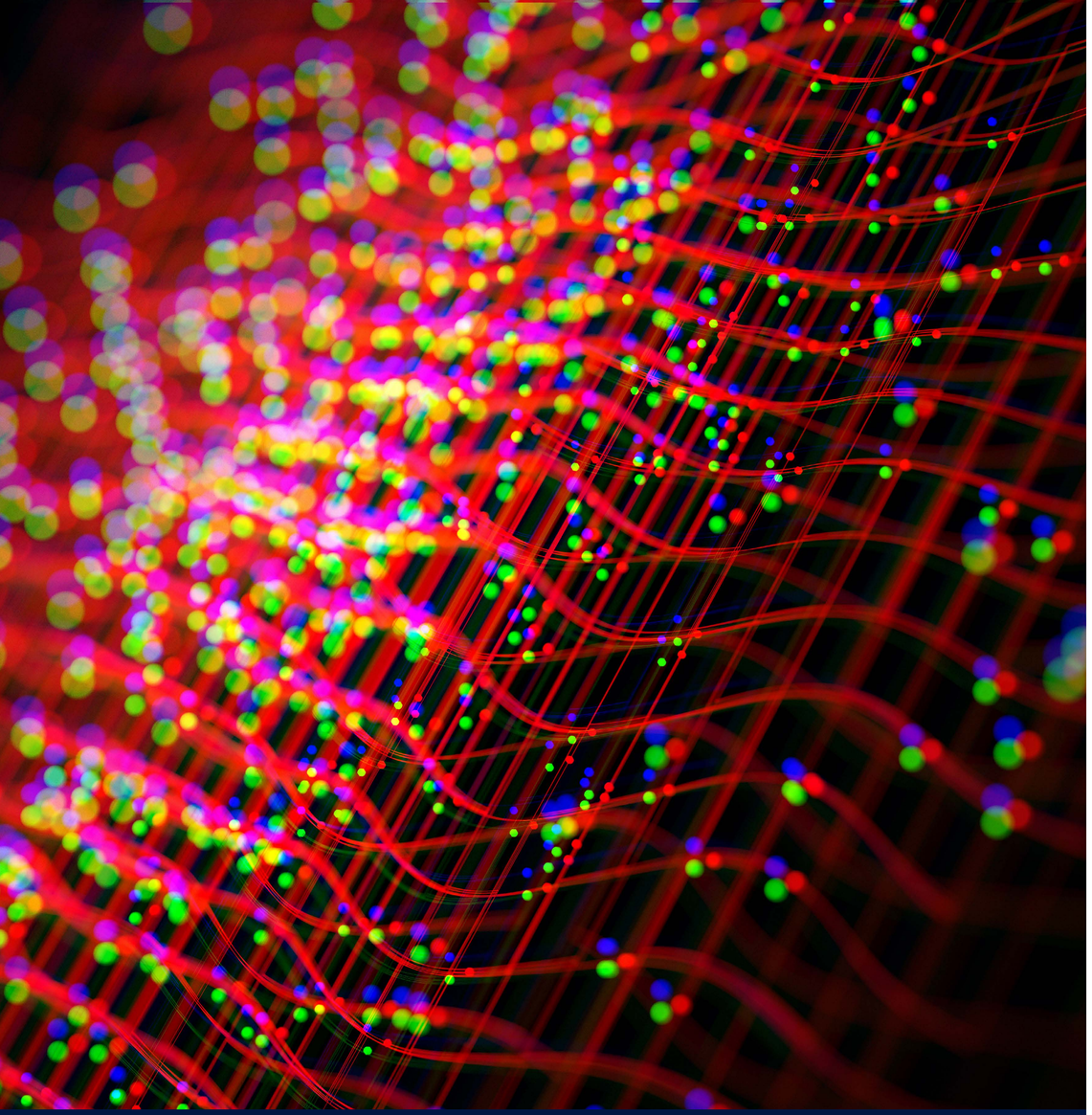
ADVANTAGE

This makes the adversary believe they have obtained hashes to the customer database SQL service account while removing the risk of kerberoasting a real domain admin account.

A similar approach can be used for other popular privilege escalation techniques including:

1. **Tomcat Manager exploit** — Plan a decoy system with Tomcat manager and monitor for connections and interactions towards this system.
2. **LLMNR poisoning** — Use a tool like Conveigh to send decoy broadcasts over the subnet and monitor for responses to these broadcasts.
3. **Credential Dumping** — Use Invoke-runas to plant fake domain admin credentials in memory using the /netonly technique.

There are many techniques available for privilege escalation, and some of them lend themselves well to an Active Defense approach. However, in cases where that doesn't work, focus on what the adversary intends to accomplish with those privileged credentials.



#5 – Scanned a Subset of Computers to Identify the Customer Database

WHY DID THE PEN TESTERS SCAN A SUBSET OF COMPUTERS?

- To check if the database server is reachable from the target list compiled in #3.
- To check if the database port is open.
- To check if any banners reveal which might be the customer database.
- To check for default passwords on SQL servers for the System Administrator account.

ACTIVE DEFENSE OPPORTUNITY

1. Plant a decoy SQL server on the network. Alert when you see port enumeration.
2. Make the real customer database accessible only from certain machines.

ADVANTAGE

Even a single port query against the decoy SQL server system is worth investigating while complicating access to the real customer database.

#6 – Used the Domain Admin Account to Login to the Customer Database Server

WHY DID THE PEN TESTERS LOG IN TO THE CUSTOMER DATABASE SERVER?

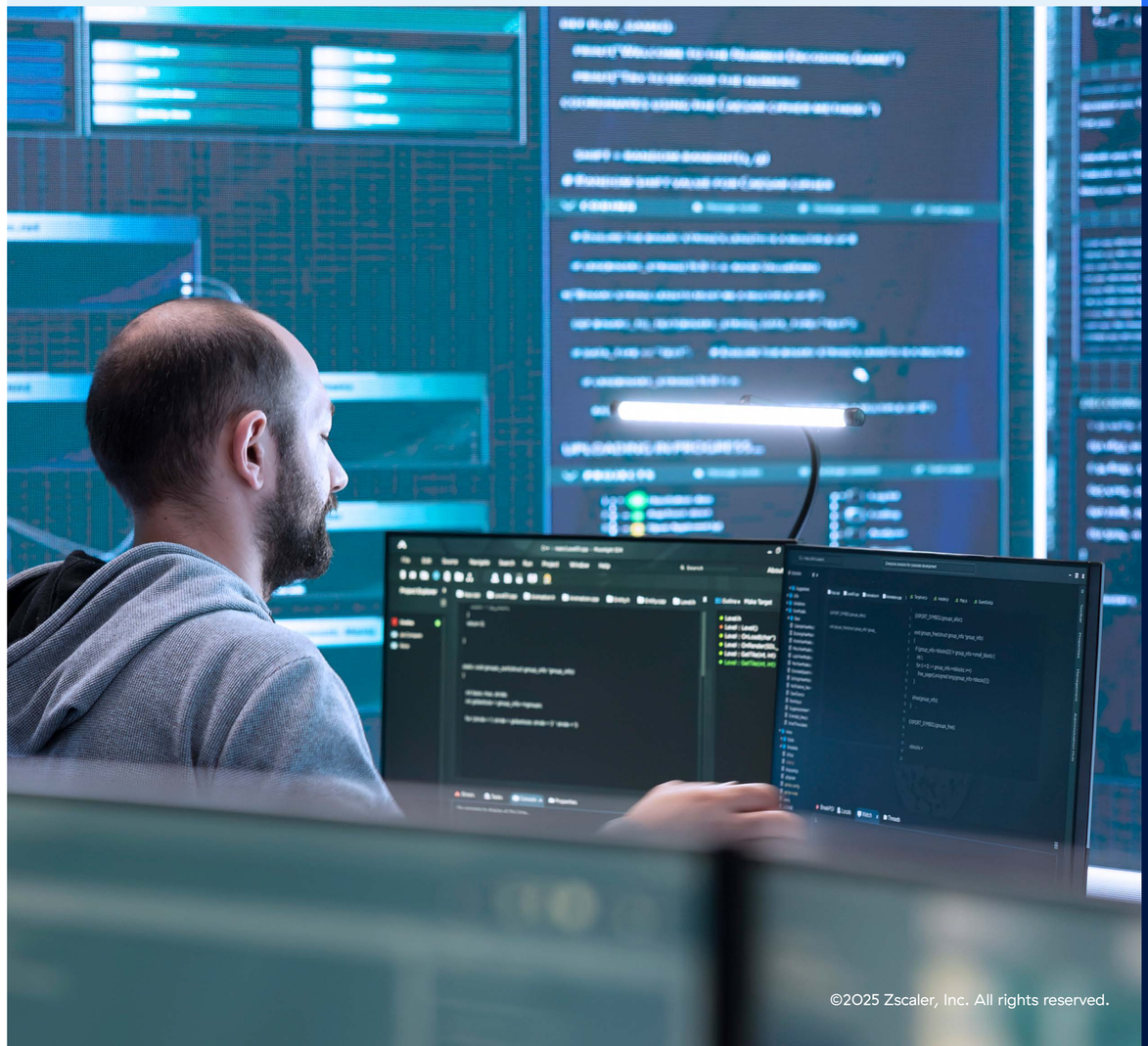
- With domain admin privileges, you can extract credentials from memory from the server hosting the customer database.
- Helps you compromise the logged–on SQL administrator account (whether it's a user or service doesn't matter).

ACTIVE DEFENSE OPPORTUNITY

1. Implement a standard operating procedure to prevent a domain admin from ever logging into the database server. Implement the corresponding rule for this server alone in your SIEM.
2. Plant decoy SQL administrator credentials in memory.

ADVANTAGE

Even a single port query against the decoy SQL server system is worth investigating while complicating access to the real customer database.



#7 – Login to the Database Itself

ACTIVE DEFENSE OPPORTUNITY

Unfortunately, if the adversary has reached this point, detection difficulty increases. This is because, from an analytics perspective, you are looking for a legitimate account, logging into a legitimate database, and running possibly legitimate queries. However, there are still things you can do.

ACTIVE DEFENSE OPPORTUNITIES

1. Setup query auditing on the SQL server for accounts with DB admin rights.
2. Hunt for non-standard queries in the hope of spotting the adversary running ‘select *’ operations and join operations to fully extract the customer database.

Applying the Active Defense Approach to any Use Case

Here's a four-step approach to applying an Active Defense:

1. **Deceive** — Can I do something to trick the adversary en route to/on the system?
2. **Standardize** — Can I define how a particular system must be used/controlled?
3. **Analyze** — Can I bubble-up anomalies against the system I am protecting?
4. **Control** — Can I make it more difficult to reach and compromise the system?

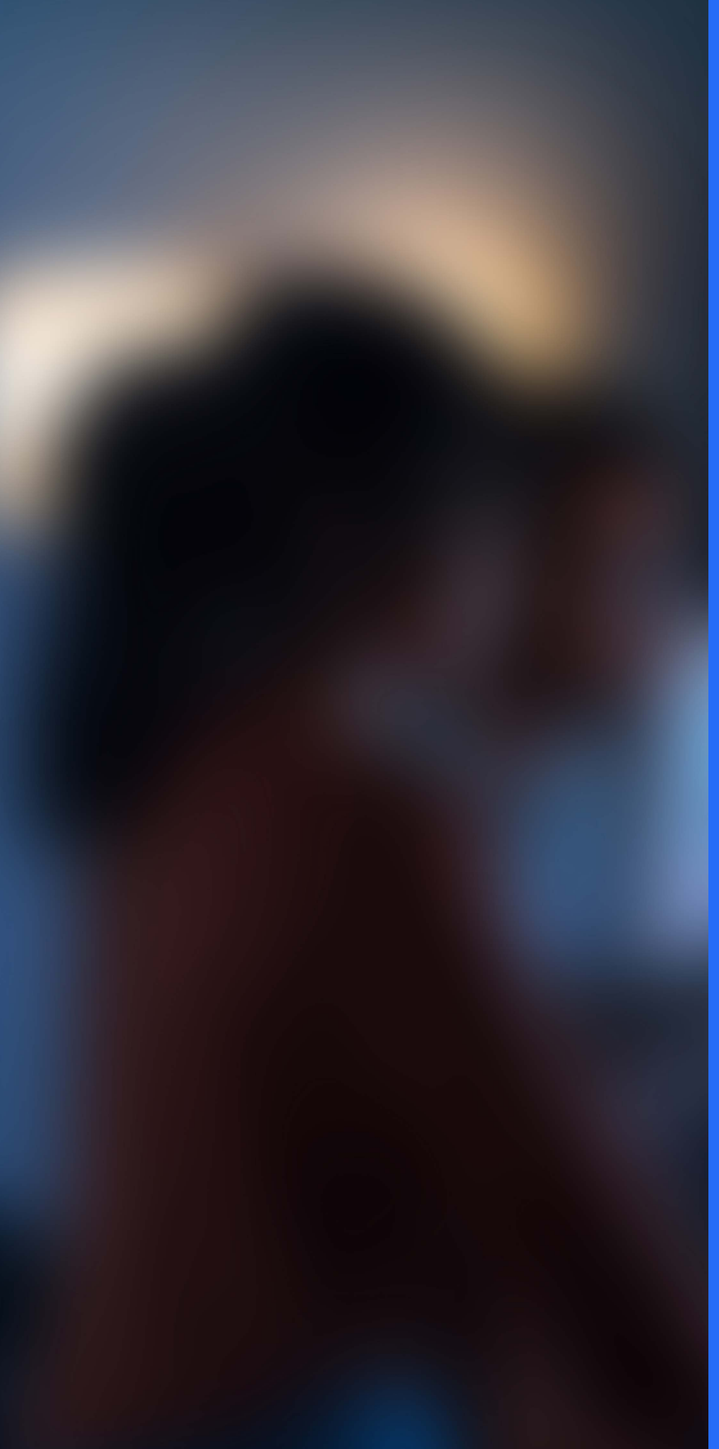
You can use the above as a combination to assess a use case beyond analyzing pen test reports. The pen test report was just a means get you thinking about active defense.

Zscaler Deception enhances the Active Defense approach by leveraging realistic decoy systems—such as databases, servers, and network endpoints—to proactively detect adversarial behaviors. Aligned with the MITRE Engage framework, Zscaler Deception simplifies and standardizes the integration of deception techniques into existing security strategies, ensuring an effective and cohesive active defense posture.

Closing Notes

- Use of the MITRE Engage (formerly Active Defense) approach covers the kill-chain and encourages you to think about the 'why' to build better defenses and how your network, endpoints, and active directory are all interconnected.
- The Active Defense approach is not limited to decoys alone, but it is a significant component.
- You don't have to baseline and standardize all your operating procedures — just the ones that matter most to you. You can also take a targeted approach to apply controls, rather than spread them throughout the network, which costs time and requires effort.
- You can tighten your use cases with Active Defense, making threat hunting a lot more productive.

Ready to see Zscaler Deception in action? **Request a demo today** to discover how it integrates seamlessly into your security strategy and enhances your active defense posture.



zscaler™ | Zero Trust Everywhere

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**