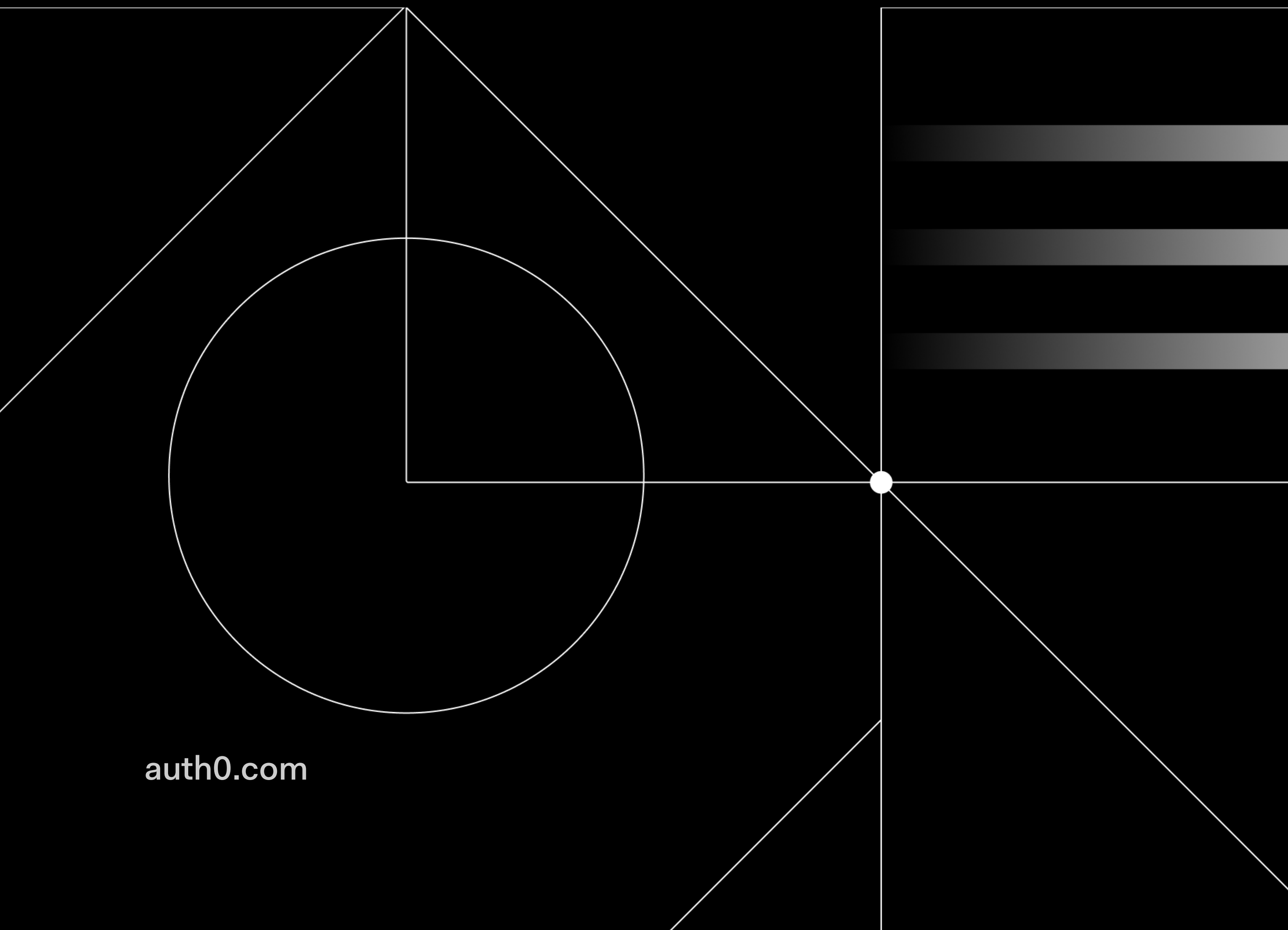
Auth0

Identity is the Perimeter

A Guide to Securing Identity



auth0.com

The idea of identity as the new perimeter for cybersecurity has been part of the conversation for a couple of years. The truth is that identity has **always** been a perimeter.

Historically, cybersecurity experts did not apply multiple security controls like firewalls or encryption to the identity perimeter because we could protect it by adding additional layers of security to our outer defenses. We didn't need to protect identity at its source because we could safely rely on our outer defenses, like a castle reliant on its moat.

Now, however, we can no longer depend on those outer defenses. Because identity is disseminated across so many platforms, devices, and applications, the identity perimeter is exposed, and we need new and better ways to protect it. Traditional perimeter protections are simply inadequate to defend identity against today's increasingly sophisticated and effective attacks.

Ongoing digital transformation has created a convergence of users, devices, and applications that demands an identity-based security approach. To meet the security challenges of this new ecosystem, companies are developing new ways to authenticate identity and authorize users accordingly. In this sense, identity is the gatekeeper, determining who gets what kind of access based on what data.

In this guide, you'll learn more about the relationship between identity and perimeter security, the methods used to attack identity, and new tactics and strategies for securing identity.

Understanding Perimeter Security

Security models, ideas, and configurations have a variety of origins. The National Institute of Standards and Technology (NIST) is a cornerstone whose guidance and institutional knowledge are relied upon throughout the cybersecurity community. Within their vast institutional knowledge is a definition worth sharing:

> Enclave: "A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter."

An enclave in simple (and very common) form is a network inside a building, or perhaps a network on a campus of buildings. The enclave has a perimeter, and perimeter security in this sense is defined as "the protection of the outer boundary of your facility" (Michael Arata, *Perimeter Security*, 2006). While the traditional perimeter was the outer boundary of a brick-and-mortar property, cybersecurity experts have extended this concept to apply perimeter-security concepts digitally.

These perimeters consist of standard network security controls and devices such as firewalls, intrusion detection systems, web application firewalls, and more. This layer of defense is used to protect the interior of the perimeter where an organization's identity information lives.

These strategies are part of what is known as defense in depth, a security concept that calls for layered defenses to protect sensitive data, assets, and information. (We'll delve deeper into the defense in depth concept soon.) This approach is valid and still used today, but traditional, perimeter-focused defense in depth is irrelevant if the assets you're trying to protect leave the building.

Firewalls were once the first line of defense for shielding our network perimeters from outside intrusion. But as more data access came from beyond the boundaries of the internal network, the perimeter moved to the endpoints. And now, digital transformation has moved the perimeter again — this time to identity.

Identity

Identity is a system resource. Systems, applications, and organizations use identity to authenticate users to their services and authorize them to perform specific functions. It was one thing to authenticate identity when everyone within an organization was using the same information infrastructure. Now, in an age of cloud-based microservices, the number of devices with network access is multiplying, and the boundaries around identity are increasingly fluid.

Put simply, identity no longer exists in a single enclave surrounded by a single perimeter. Instead, identity itself is the perimeter. No longer are we relying on defenses of our outer perimeter, because that perimeter is gone. Our castle has lost its moat, but we still need something to defend ourselves against attackers. That means our notion of what those defenses should look like must evolve to suit the ever-changing cybersecurity landscape.

Defense in Depth

Defense in depth is a common cybersecurity strategy sometimes said to have been developed by the National Security Agency. This approach leverages multiple layers of security controls or defenses to protect sensitive information. Defense in depth was originally conceived as a military strategy, in which multiple layers of defense were deployed to prevent an attack so that even if the attack were successful in breaching a single layer, it would be thwarted at subsequent layers.

Defense in depth is intended to provide redundancy in security controls, bolster security posture, and decrease the likelihood of a successful attack. These security controls can take the form of technical, physical, or administrative controls.

Technical Controls

Examples of technical controls include layered cybersecurity defenses of hardware or software, such as firewalls, antivirus programs, vulnerability scanners, encryption, or virtual private networks.

Physical Controls

Physical controls are just what they sound like: material components of your defense infrastructure. Examples include bollards — concrete barriers in front of buildings to prevent forced access via vehicle-ramming attack — access-controlled doors that require a badge, or measures like fences, dogs, or security guards.

Administrative Controls

Examples of administrative controls include organizational policies, processes, or procedures that provide guidelines or standards around security awareness training, data destruction, or personal device usage.

These concepts and controls are still useful in evaluating new strategies for expanding the perimeter to encircle identity. Before we dive into these new strategies, we need to identify what types of attacks we're likely to encounter in our new environment.

Attacks on Identity

Phishing

In 2019, according to the FBI, phishing was one of the most commonly reported cyberattacks, resulting in more than $3.5 million in losses in the United States alone. In a phishing attack, bad actors use emails that appear to be from valid, trustworthy sources (like your bank, university, or employer) to encourage you to perform some action that will allow an attacker unauthorized access to your accounts, credentials, or other sensitive information.

To deceive you into trusting them, phishing emails often feature branding, logos, and wording deceptively similar to the content of legitimate business emails. The wording is calculated to increase your sense of urgency, to manipulate you into clicking on a link or opening an attachment. These emails may offer enticements such as refunds, free offers, or some other opportunity that sounds too good to pass up.

In a variation of this attack called smishing, attackers use text messaging or SMS as an alternative to email. Another version, known as vishing, uses voice phishing over the phone to convince a user to give up sensitive information.

Spearphishing

Spearphishing is a type of phishing attack that targets users on a personal level. These attacks are tailored to individual targets using details, greetings, and phrasing specific to that person. As with phishing, these attacks often convey a sense of urgency in asking a user to verify account information or examine some fraudulent activity on their account.

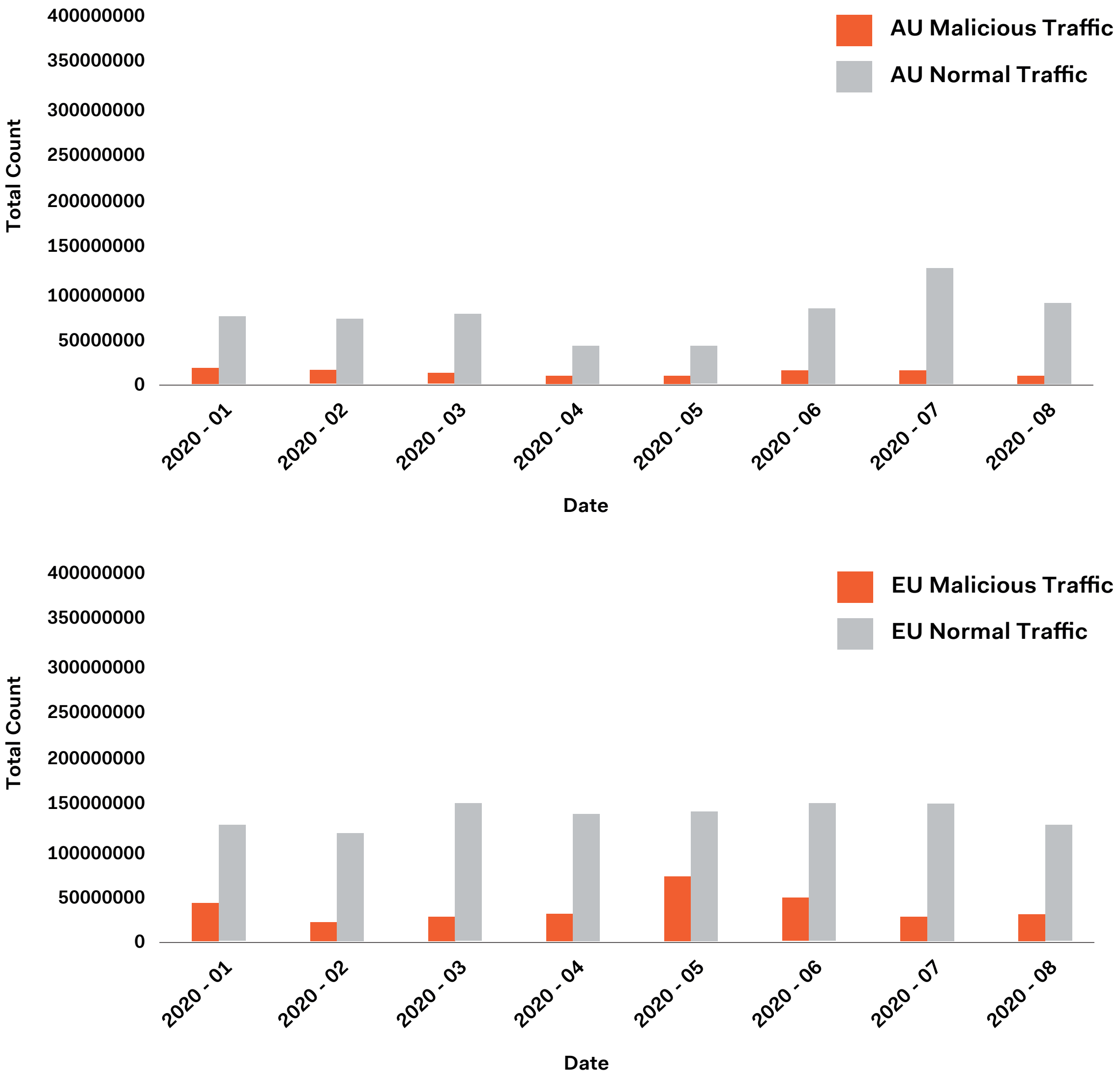
The difference between phishing and spearphishing is the level of personalization, effort, and sophistication required to complete the attack. Attackers often use social media and other public sources of information to harvest details on their targets, in order to make their attacks more effective.

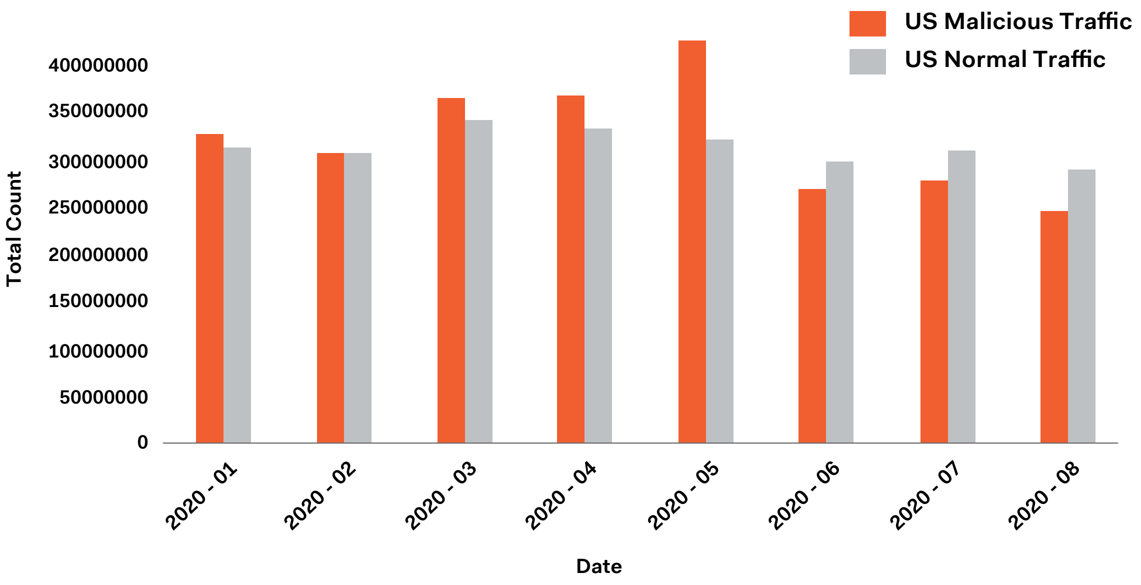
Brute Force Attacks

Brute force attacks involve an attacker trying every possible combination of a single username and multiple passwords in a login sequence until they are successful. These attacks are exhaustive and methodical. Attackers typically try short passwords first, then longer ones as the attack continues.

From the chart below, you can see that over time, brute force attacks increase in volume and do not discriminate when it comes to who can be targeted.

Malicious vs Normal Traffic Per Region Since January 2020





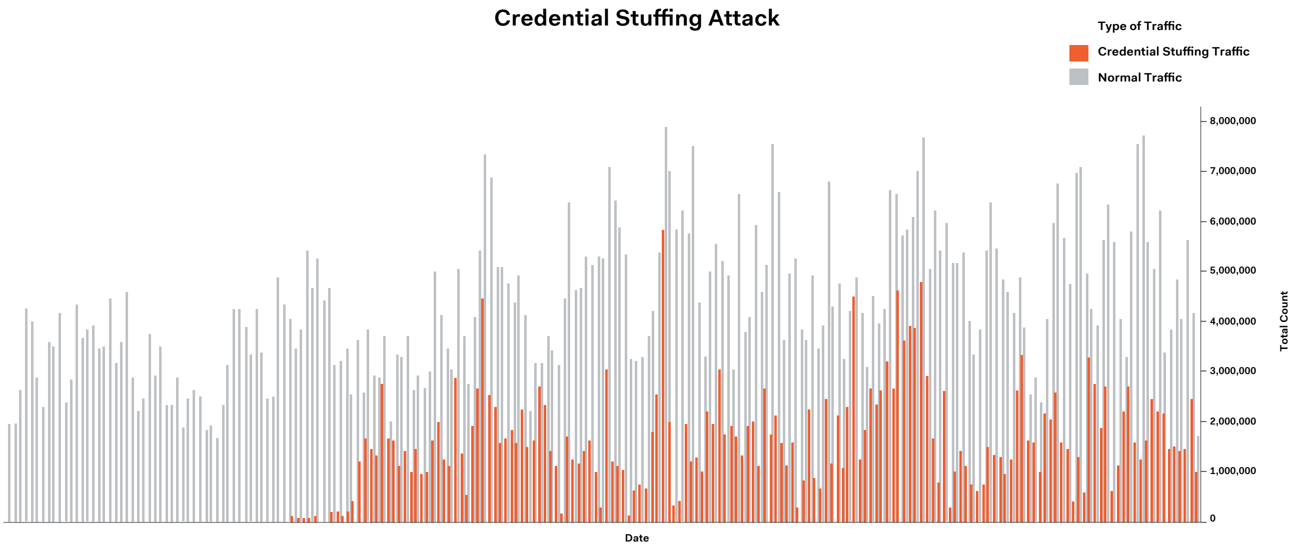
Password Spraying

Sometimes referred to as reverse brute force attacks, password spraying involves attempting combinations of multiple usernames with the same (typically common) password in a login form until the attack is successful.

Credential Stuffing

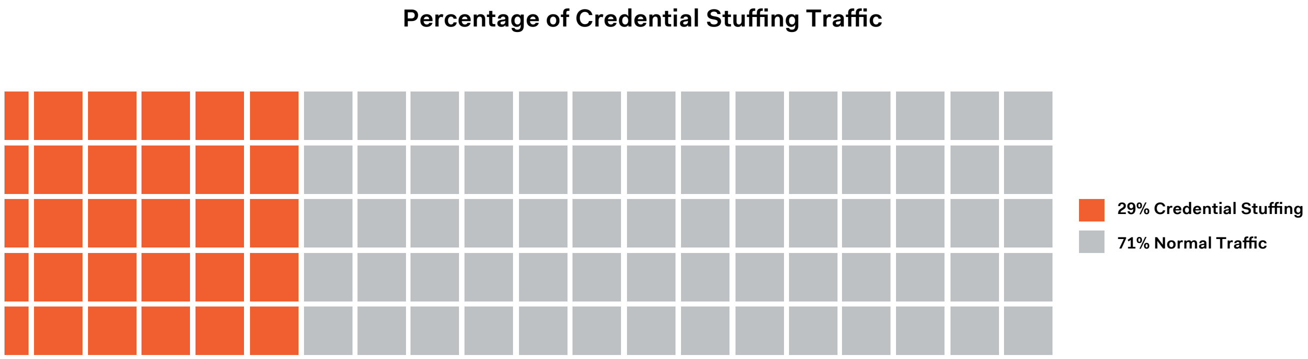
Credential stuffing is another type of brute force attack sometimes referred to as credential recycling. This attack utilizes usernames and passwords obtained in other data breaches or purchased from bad actors who obtained these credentials. Because many people reuse the same credentials across different sites, credential stuffing attacks have a relatively high rate of success. The attacker attempts to log into various services, applications, or websites with an array of stolen credentials until they are successful.

The following visualization shows a credential stuffing attack against a large financial services company:



Over time, credential stuffing can consume a significant volume of an application's resources as well as pose a risk to the identities themselves. In the graph above, the credential stuffing attack is shown in orange, and represents a substantial volume of the total traffic.

Credential stuffing attacks comprise a significant percentage of total attack traffic, and this percentage tends to surge during the worst attacks, resulting in downgraded performance, denial of service, or even a complete outage. Below is an example of one of the worst credential stuffing attacks by volume we've observed at Auth0 in the last year.



Man-in-the-Middle

Another attack that seeks to gain access to credentials is the man-in-the-middle attack (MITM), in which attackers covertly relay and possibly alter the communication between two parties who think they're speaking directly to each other over a private connection — when in fact the whole exchange is being observed, or even controlled, by the attacker. In order to accomplish MITM attacks, bad actors must be able to intercept all messages passing between the involved parties and interject new ones. This type of attack is often called active eavesdropping.

In all of the attacks discussed above, identity is at risk. The good news is that there are security controls that can be applied in each of these scenarios to help mitigate that risk.

Protecting Identity

In order to protect the identity perimeter, organizations must evolve their security strategies, leveraging a layered, defense in depth approach. Now that we've reviewed the most common and effective methods of attacking identity, let's explore the security controls that cybersecurity teams use to combat these attacks.

Multi-Factor Authentication (MFA) and Contextual MFA

Multi-factor authentication (MFA) is a simple but effective means of protecting identity. Because passwords are relatively easy to guess, MFA demands an additional credential from the user, such as a one-time PIN or an additional security question. Implementing MFA increases the likelihood that the user being authenticated is who they say they are — that you can trust them.

Contextual MFA considers not only additional credentials like a one-time PIN, but also contextual clues to the legitimacy of the user's identity. Authenticating based on context involves looking at what time of day a request was made, from what location, and using which device. Historical behavior patterns also come into play. For instance, if you habitually do your online banking from your laptop at home during the week, a login request from a smartphone on the other side of the world could trigger an additional verification step, since the context suggests that the user making the login request is not you.

MFA is used to thwart automated, bot-generated credential stuffing attacks, as well as to reduce the velocity of brute force attacks. MFA is also a critical tool in preventing account takeover, a form of fraud in which an attacker seizes control of a user's accounts.

Behavioral Analysis

Behavioral analysis of system activity is another control that helps defend the identity perimeter. Monitoring and analyzing system behavior can identify anomalies that indicate brute force or credential stuffing attacks, allowing organizations to detect and mitigate these attacks before they do too much damage. Implementing web application firewalls, blocking suspicious IP addresses, requiring users to pass a CAPTCHA, and other controls protect against content-generating bots and bad actors and reduce the impact of their attacks.

Data Protection

Data protection is an essential measure to secure identity. In order to effectively protect identity, any credentials or verification data should be properly protected with access controls and encryption. Data in transit should be encrypted using appropriate cryptographic protocols and ciphers. Passwords in storage should be protected using one-way hashes that are salted, and credentials and verification data should use appropriate encryption with strong key management procedures and protocols. Encryption and strong data protection mechanisms also help prevent man-in-the-middle attacks.

Rate Limiting

Rate limiting is a process by which login attempts are limited to a specified number of times. The intention is to prevent excessive login attempts. If you've ever been temporarily locked out of an account because you couldn't remember your username or password after several tries, you've experienced rate limiting. Rate limiting is a simple concept, but it's an extremely effective first-line defense against password spraying, brute force attacks, and credential stuffing attacks.

Zero Trust

Finally, embracing a Zero Trust model — even incrementally — can improve security posture. A Zero Trust model is built on the idea that nothing should be trusted and everything should be validated before being allowed across your perimeter.

The National Institute of Standards and Technology recently released a Special Publication on Zero Trust, which describes how the security perimeter has moved from the network to the users themselves — that is, to identity. Implementing a Zero Trust strategy allows organizations to prevent unauthorized access to sensitive assets, particularly identity, by consistently and continuously authenticating and authorizing all access.

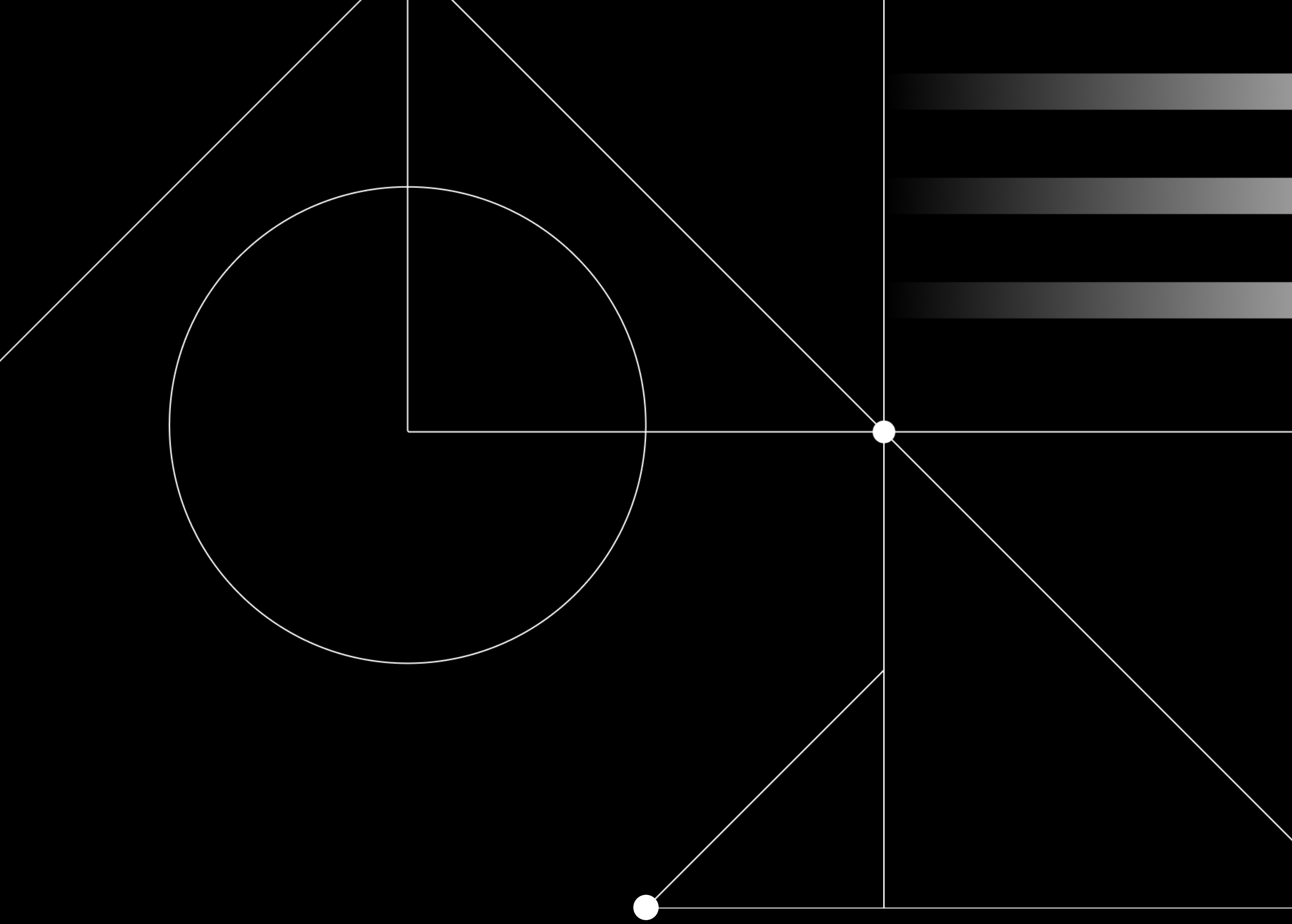
Giacomo Collini, Director of Information Security for King.com (the creators of Candy Crush), has said that Zero Trust is "key to enable companies to transition to a pure-cloud environment." However, layered controls to protect the perimeter are still valuable. While most organizations will live in a hybrid environment of perimeter security and Zero Trust as the transition to Zero Trust occurs, implementing Zero Trust architecture will ultimately improve security posture.

Center Security on Identity

In today's immensely interconnected world, with teams distributed globally and people using a wide variety of devices and applications to perform overlapping functions, the traditional approach to perimeter security has become outdated. Attacks are increasingly effective and sophisticated, and our old understanding of the perimeter as the castle moat no longer serves.

Instead, we must realize that security and identity are coterminous. An identity-centered security approach is the only way to manage the confluence of people, devices, and applications that is our new normal. Using layers of security controls, contextual MFA, data protection measures, rate limiting, and other approaches, organizations can establish a modern defense in depth security strategy to protect identity.

To learn more about the intersection of security and identity, explore Auth0's resource library.



Auth0

About Auth0

Auth0 provides a platform to authenticate, authorize, and secure access for applications, devices, and users. Security and development teams rely on Auth0's simplicity, extensibility, and expertise to make identity work for everyone. Safeguarding more than 4.5 billion login transactions each month, Auth0 secures identities so innovators can innovate, and empowers global enterprises to deliver trusted, superior digital experiences to their customers around the world.

For more information, visit www.auth0.com or follow @auth0 on Twitter.