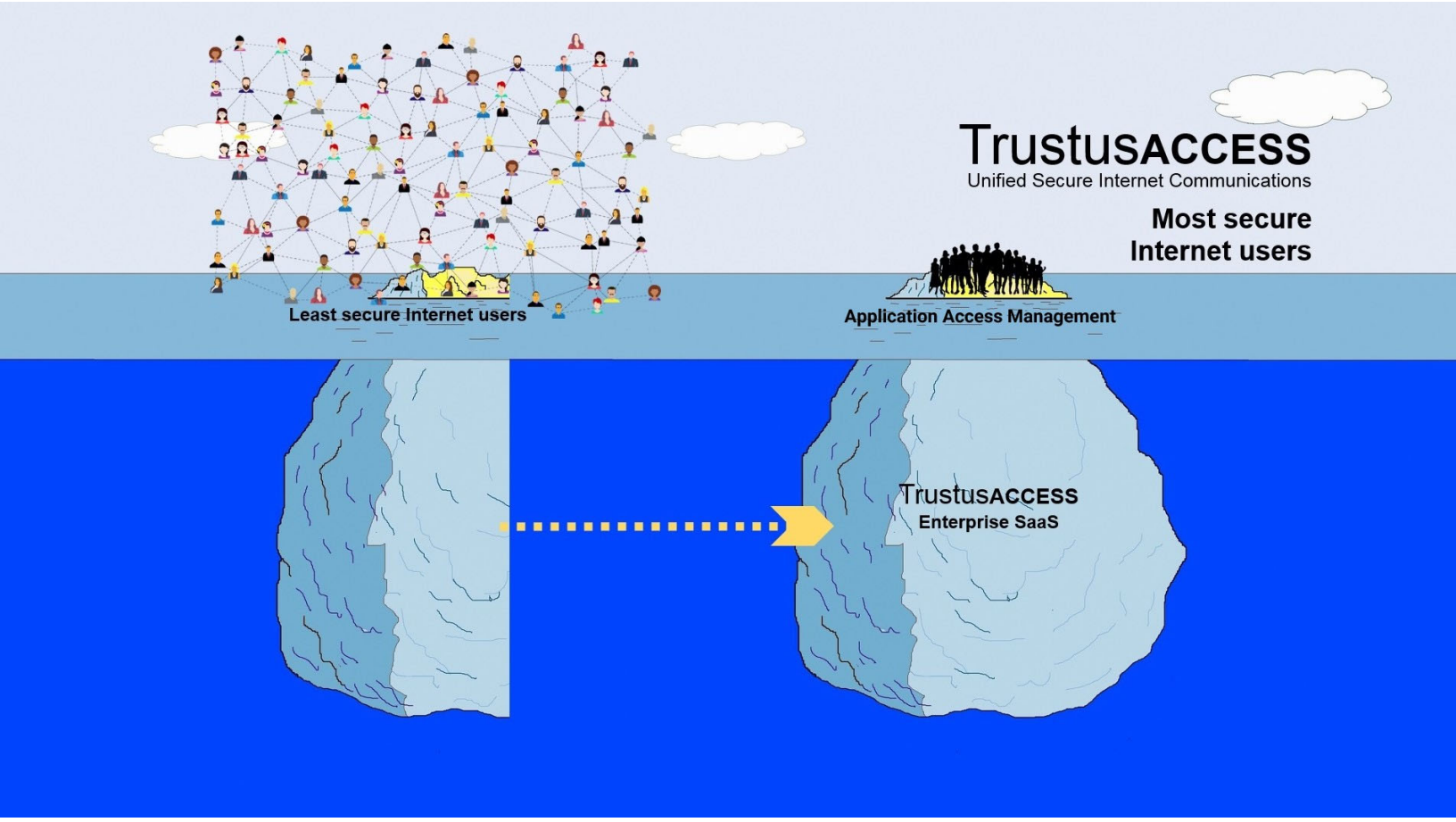

Trustus AAM Unified Secure Internet Communications (USIC)

Attack surface prevention – level up your security awareness | March 2024 Blog

Threat reality is damaging

In 2023, Google Cloud found that over 85% of breaches involve stolen credentials or credential related issues which could be addressed by stronger identity management[1] at the organization level.

Verizon found that 83% of breaches involved external actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches. 74% of breaches involved the human element, which includes social engineering attacks (phishing, etc.), errors or misuse. Web application attacks (brute force, etc.) account for 25% of breaches, by leveraging stolen credentials and vulnerabilities to gain access to organizations' assets.[2]

Integrated identity and application access cyber protection is first line of defence

Proactive approach

Stopping an attack from occurring in the first place is the first line of defence. Trustus AAM Application Access Management with built in digital identity (DI), protecting the application layer, firewalls protecting the network layer, and anti-malware are examples of proactive cyber security.

Reactive approach

AI and monitoring software as a means of prevention, rank second in their ability to prevent an attack. SSL inspection is an example of reactive cyber security.

[1] Threat Horizons Report, Google Cloud, August 2023.
[2] Data Breach Investigations Report, Verizon, 2023.

Trustus AAM is pure X.509, PKI protocol-driven cyber defence proactivity with both identity management and command and control application access and connectivity management for Unified Secure Internet Communications (USIC).

How to prevent data breaches

We will explore Trustus proactive measures that organizations can take to mitigate threats from phishing and malware, to password vulnerabilities.

Compromised credentials (user identifiers, passwords, biometrics), anything that authenticates who you are, is responsible for not stopping the majority of the growing threat landscape. Whether credentials are strong or weak, attackers can steal, alter, expose or simply use them to intentionally cause harm to their victims. Organizations often suffer the most financially with ransomware, brand loyalty attrition and legal costs.

With remote work, customers and suppliers needing access, and cloud deployments, the traditional network perimeter has shifted to the center with identity management at the forefront. IAM (identity and access management) is the common solution used by many, with credentials management taking center stage. But credential management solutions, such as SSO, 2FA and password vaults, are failing in their ability to securely protect application access from harmful attackers. There are reasons for these failures, and this is why credential related breaches are escalating.

A primary cause is that IAM is the authentication of a user, deploying a token to authenticate the end source. Tokens are not digital identifiers and they were never designed to be.

True digital identity (DI), the machine to machine identity relatability is only accomplished with a digital certificate deployed on each user device. So, credential management in their current state are technically incomplete. They cannot deliver the DI piece necessary, nor can they secure the application level perimeter. Only Trustus AAM can.

So, credentials deployed without Trustus AAM, regardless of type and strength, are leading to data breaches because authentication with token based activities do not prevent attackers from getting in.

What is an organization to do to fortify their security posture for access management? Trustus deployed Application Access Management (AAM) delivers the strongest unified approach:

Part A

- The Trustus Privacy Bridge controls and limits access in real time to only those remote users with an approved certificate present.

- Trustus AAM digitally identifies all users (people, devices, things, internet nodes, functional activities) with a Trustus root-signed certificate. The digital certificate pre-approves and establishes user provenance, followed by transactional authorization each time the user attempts to connect to its enterprise application.

AAM supplants IAM credential management systems for SSO (Single Sign On) and 2FA (Two Factor Authentication). Trustus is the first line of defence. IAM can remain as the second, or not.

With Trustus, whether credentials have been compromised or not, the perpetrator could not pass through the Trustus Privacy Bridge without a Trustus certificate present. Even if credentials are compromised, Trustus AAM protects and denies access.

Since organizations may find it difficult to retire their IAM, Trustus AAM comes as a light touch, protecting legacy solutions. It is fully automated, easy to deploy and maintain, and is juxtaposed as a frictionless SaaS in front of any IAM credential management system.

Part B

Trustus "Private" URL

- Trustus delivers private access through its "Private" URL access from user designated devices to their organizations' applications. Access to enterprise applications, API's, EDI, Cloud, etc. is carried out by Trustus AAM connectivity through the "Private" URL, being inaccessible to other public internet users. Enterprise application access is limited to the Trustus user community.

Four layers of computers – why it matters

The layers of computer architecture from bottom up are the hardware, operating system, software, and user layers. Users access applications (software) on the user layer. The internet is the ultimate user level, connecting browsers to domains, users to login pages to reach applications. When the user level is protected with Trustus AAM, networks comprised of many applications are protected too.

This, of course, requires proper mapping of resources to identify all network nodes. An attacker cannot deploy malware through an application portal when it is Trustus protected, only through a network. Blocking network access avoids perimeter exploitation.

The aim is to avoid network perimeter exploitation by properly securing application access. Without Trustus AAM, attackers gain access to an organization's systems and data, often using stolen passwords and login information, credential stuffing, and social engineering to get in. Once the attacker is inside, they will attempt to penetrate unsecure, easy to read, relational and hierarchal repositories, and even change permissions on compromised accounts for future login. With sensitive data in hand, they can sell it, lock it for ransomware, use it for future attacks, or release it on the open market to damage the organization.

Common ways credentials are hacked

Despite best efforts, credentials like passwords face a mounting uphill battle that they single-handedly cannot win against attackers. Traditional practices to avoid compromise are to use strong and unique passwords, implement multi-factor authentication (MFA), enforce the principle of least privilege, (PoLP), and follow system hardening best practices and patch. Daily reporting of breaches prove these methods no longer suffice by themselves. The biggest treats are:

Credential recycling and password recycling

Credential recycling refers to re-using username and password combinations obtained from brute force attacks. Password recycling is using the same password across multiple account logins or amongst multiple team members. The later can significantly increase the risk of breach, the first being the result of successful attacker attempts. Both can result in gaining access to unauthorized user accounts and organizations' applications, systems and networks.

Phishing

Phishing is a technique used by cybercriminals to trick individuals into disclosing their credentials and sensitive data using fake emails, messages, or links to websites. Once revealed, the attacker mounts attacks against their intended victims, and often times, exposing organizations with vulnerable data.

Malware

Malware is short for malicious software, developed by cybercriminals to steal credentials and data, and infiltrate with the intent to damage computer systems and networks. Common examples are ransomware, viruses, worms, Trojans, spyware, and adware. Users who unknowingly download malware, often have their credentials used to gain access to organizations' applications and systems, including, for example, the bank accounts of their users.

Account takeover and identity theft

An account takeover refers to the hijacking of an account that belongs to someone else. Identity theft refers to opening a new account with someone's stolen credentials and personal information. Each involves stolen credentials. Stolen tokens/cookies are used to bypass the authentication process, such as MFA.

Brute force attacks

A brute force attack is a trial and error attack method to crack passwords, login credentials, and encryption keys. It is simple to carry out by bombarding a public facing login or webpage to gain unauthorized access to applications and organizations' systems and networks.

How can organizations best protect themselves

Implement best cyber protection with Trustus AAM at the gateway of your digital transformation.

Trustus AAM enterprise SaaS

Trustus is an advanced unified digital identity cybersecurity and privacy platform delivering innovative internet communications. We partner with businesses of all sizes to provide automated trusted solutions for securing digital identities, and connecting devices, applications and ecosystems, enabling people and things to communicate with each other safely. Our team has delivered some of the most complex web portal and infrastructure solutions to some of the best-in-class international companies. Managing the complexity and risks associated with internet communications is our strength. The Trustus team looks forward to work with you to meet the needs of your growing digital landscape.

Contact us at sales@trustussecurity.com for a demo.

https://trustussecurity.com/