ONE IDENTITY by Quest

How to Protect Your Expanding Enterprise Attack Surface with IAM

Five ways to limit access to your digital assets through identity-based tools and practices.

Connections are at the heart of your competitive advantage.

But the more connected you are, the bigger your attack surface.

Your employees, customers, prospects and business partners can find and collaborate with you in more ways every year. Unfortunately, with all that growth in business opportunity comes growth in your enterprise attack surface: the potential entry points that cybercriminals can exploit for unauthorized access to your digital assets.

In most enterprises, a few technology imperatives are contributing to the rapid growth of that attack surface:

The shift to cloud

One of the most notable changes in attack surfaces has been the shift to cloud. Cloud-based services offer scalability, cost-effectiveness and agility, but they also represent another point of username-and-password authentication – a point over which you exercise only limited control. Cybercriminals who gain access to those services can exploit vulnerabilities in infrastructure and applications that you don't own and cannot defend.

Connected devices and IoT

The Internet of Things (IoT) and its landscape of connected devices are designed with convenience as a selling point and with security as an afterthought.

Defend your enterprise attack surface by making IAM the center of your security strategy.

- **Deploy access management** with multi-factor authentication.
- **Adopt and enforce** the principle of least privilege.
- **Implement** privileged access management (PAM).
- **Lock down** your Active Directory.
- **Manage identities** with identity governance and administration (IGA).

Cybercriminals look for IoT vulnerabilities, including in routers and networking gear, to launch intrusions such as botnet exploits and distributed denial-of-service (DDoS) attacks. Add to the mix the work-from-home initiatives with consumer-grade endpoints, peripherals and networking solutions.

Third-party vendors and supply chain

Besides its connections to your employees and your customers, your enterprise relies heavily on connections to third parties and vendors for basic services like payment processing, data storage, secure file transfer and customer support. How much do you know about the security controls those third parties have in place? If threat actors

manage to get unauthorized access to your vendor's network, can they jump from there to your network as well? Or, if your software supply chain depends on updates and security patches from your vendor – and it does – can you be certain of the source before installing them?

Identity – The common thread

You might think that defending your attack surface means revisiting those technology imperatives and cutting back on the ways you connect with your marketplace. And that makes sense if you still think of network security in the traditional context of establishing and defending a network perimeter.

But not so fast.

What do all of those technology imperatives have in common? Identity. What if you regarded identity as the new perimeter? You could then apply modern identity and access management (IAM) tools to reduce your attack surface by limiting access to your digital assets.

IAM helps prevent unauthorized access by ensuring that users authenticate themselves properly. With identity-based tools and practices you can defend your enterprise attack surface while confidently connecting to cloud infrastructure and applications, adopting IoT, embracing more types of devices and relying on third-party vendors.

Making IAM the center of your security strategy

One Identity recommends five identity-based practices and corresponding tools for limiting access to your network and assets.

1. **You can defend your company against most credential theft** by implementing enterprise-grade access management that incorporates advanced password management and multi-factor authentication.
2. **Enumerate and audit your companies' identities**, paying special attention to your privileged users. Smart administrators delete any dormant accounts they find. They also apply the principle of least privilege to overprivileged accounts to ensure that users have access to only the resources they need to perform their duties.
3. **Implement privileged access management.** With PAM you stay in control of privileged accounts and align them to your preferred risk posture.
4. **Lock down your Active Directory.** Microsoft AD is often the first port of call for any cybercriminal. Improve the security posture of your AD with zero trust and delegated permissions.
5. **Manage identities with identity governance and administration.** Identities should conform to your organization's standards, policies and risk posture. With IGA you can define and manage identities in the context of those policies.

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management (AD Mgmt) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 500 million identities for more than 11,000 organizations worldwide. For more information, visit www.oneidentity.com.

ONE IDENTITY by Quest