stealthbits

WHITE PAPER

A PRACTITIONER'S GUIDE TO ACTIVE DIRECTORY SECURITY

TABLE OF CONTENTS

Foreword by Gavin Ashton

GAVIN ASHTON

Identity & Security Expert

Author of the viral "Maersk, me, & notPetya"

Over the past twenty years the challenges presented by external and internal threats has changed dramatically. Once, the primary concerns were the people and devices connected directly to our offices or datacenters. Gradually, over time, things have become almost completely reversed.

We used to apply principle of least privilege to control insider threats as the priority. In the past thirteen years we've seen the consumerization of IT, the cloud, and well-funded cybercrime and nation-states performing highly organized and devastating internet-based attacks. So, it is now as much, if not more so, about protecting ourselves from the kinds of extinction level events seen in cases such as WannaCry and notPetya.

As the tools and techniques used become so much more available, these attacks become more and more frequent. Another week, another big name reporting an enterprise-wide outage. And while some organizations may be further ahead than others in the transition to cloud-native architectures, many are still heavily tied to Active Directory. Even organizations that do have a greater footprint in the cloud likely have one or more critical systems that are still connected to Active Directory and which will be for some time.

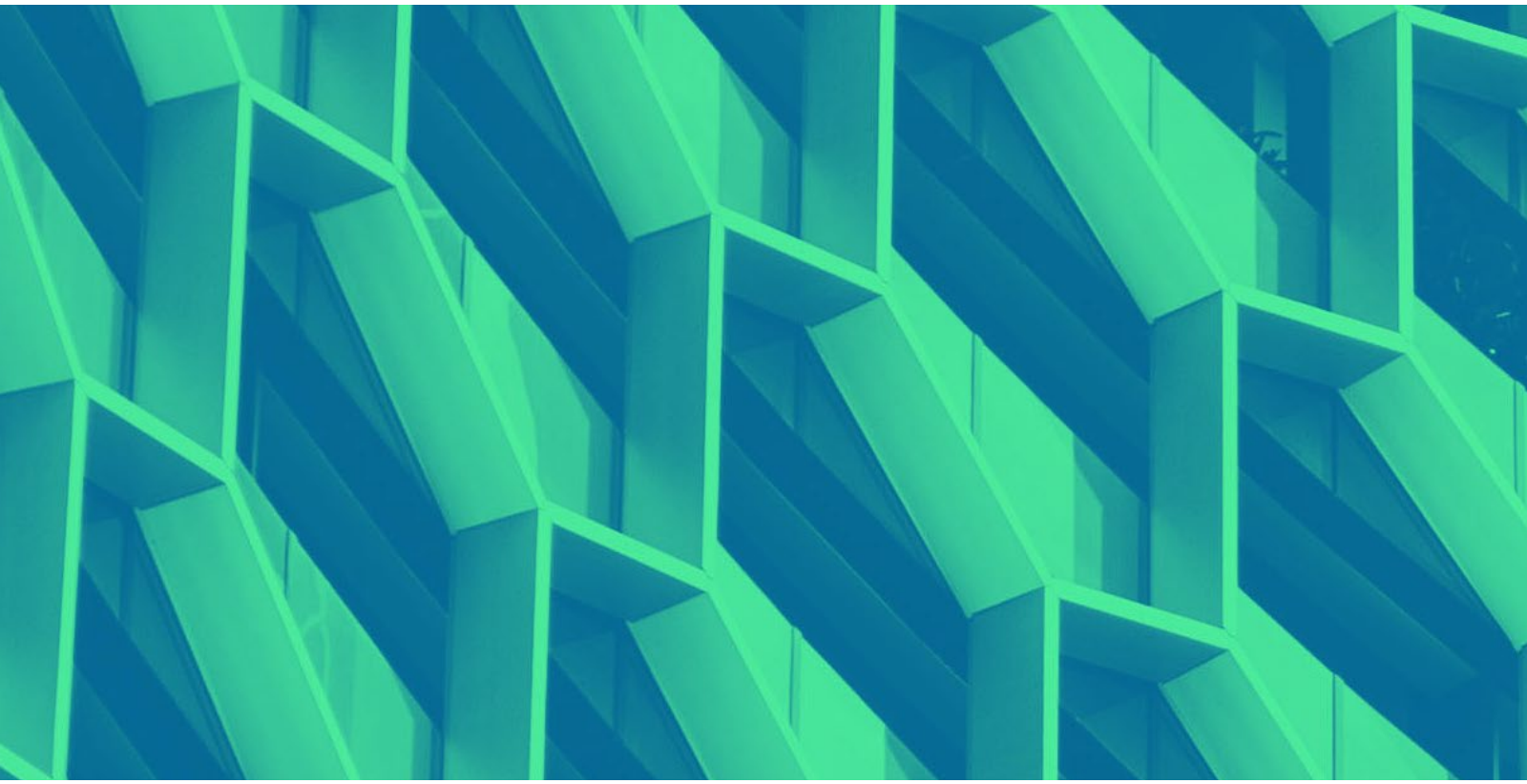
In terms of risks to the organization then, Active Directory remains extremely relevant to the ability of many to operate their business. The pattern is depressingly consistent and frequent: An end user has too many privileges. They click on a link or download some weaponized software update and boom. Malware uses classic methods such as pass-the-hash to traverse from system to system, finding more and more highly privileged credentials with which they can spread across more and more systems, until eventually the organization is owned from top to bottom. And before anybody realizes anything is wrong…

The screens go black. All of them. Laptops, desktops, servers, domain controllers. Applications. Databases. If the system was domain joined, then unless there was some network outage somewhere, it's all gone.

How much confidence do you have in the maturity and effectiveness of your contingency plans?

But even if you know the bad actors are coming, this is no reason to leave the door open. And it is folly to think that some advanced piece of technical wizardry will stop anything. Your best defense is to apply some simple controls consistently. Enforce the principle of least privilege, using the technology you have today. Some will see privileged access controls as a blocker or an inconvenience. The truth is, it is about establishing clarity and setting expectations. If poor access controls are hiding broken processes, then these broken processes are as much a risk as the application service accounts that demand membership of domain admins!

For the sake of not just your bottom line, but also the personal well-being of your customers, your people, partners, and vendors alike please, do not delay. Review and apply these basic processes and controls. It is a duty of care to save them all from the worst impacts of a rapid cyberattack.



INTRODUCTION

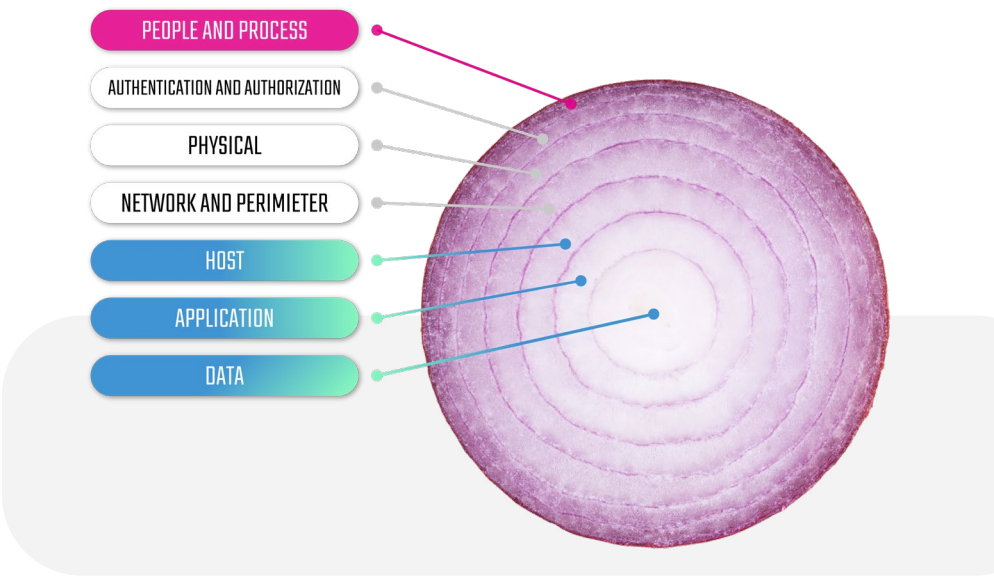
Henry Ford once famously said, "Most people spend more time and energy going around problems than in trying to solve them." This isn't an indictment of today's security practitioners, but rather the reality they're forced to live with. Competing and conflicting business priorities, industry fads, and general misconceptions drive attention and funding to the wrong priorities. As a result, data breach occurrence continues to rise, as does the level of devastation they cause.

Sadly, while attackers continue to improve upon the ease and speed in which they can achieve their objectives, the general techniques or underlying principles they exploit remain very much the same – and it's largely about Active Directory. If you're thinking that's too simple or too narrow, think again. You needn't look too far or search too hard to find that Active Directory is a target – if not the target – of virtually every advanced threat actor, from nation-states to modern ransomware variants and everywhere in between.

So, if Active Directory is the common denominator, why is there so much focus on seemingly everything but AD itself? It's clear that Active Directory needs to be prioritized, but what are the clear priorities for protecting AD and thus everything connected to it?

Priority #1: Create a strong foundation

The concept of defense-in-depth, represented by the "security onion," is a core tenet of a successful approach to information security. Yet, our strategy of defense-in-depth needs a strong foundation and while defending Active Directory is part of that foundation, there are several other crucial cornerstones.



Understand the business and align security processes with business incentives.

As security practitioners, it's vital to understand the business you're protecting. Seek opportunities to talk to folks in the business and understand how the company works from their perspective. Developing security processes that don't match business processes is wasteful, ineffective, and creates friction. These challenges are amongst the hardest for security practitioners to solve. But bridging this gulf to create a culture of security is everyone's responsibility.

Create and keep up-to-date inventories of business-critical or sensitive assets and applications.

Asset inventories may sound boring, but accurate inventories and complete risk assessments are vital to prioritizing your security investments. They're also important for understanding what depth of control is required for each asset. These datasets are not the sole domain of the business continuity and disaster recovery planners; they're vital inputs to security decision-making, and the middle of a major incident is not the time to be figuring this out.

Continuously inventory and validate the assets on your network.

With many devices (smartphones, laptops, etc.) coming and going, it's important to dynamically track their ownership and profile. Many organizations have also expanded bring-your-own-device (BYOD) policies to allow individuals to use personal computers for business purposes, whether out of necessity or desire to reduce costs. The volume and churn make them difficult to track manually, yet they expose the organization to significant risk.

Before allowing these devices to connect to the corporate network or access corporate resources, their security posture should be assured. Systems with unpatched or obsolete operating systems or insecure settings should not be allowed access. The same goes for the organization's servers and corporate-managed computers – continuous patching processes and current operating system versions are essential to closing common vulnerabilities and introducing better security controls.

Priority #2: Adopt strong authentication practices

Two factors drive strong authentication as a key priority. First, adversaries of all kinds have demonstrated success attacking credentials and that continued success only increases focus. Second, the nature of business has changed, and as a result, created a large internet-facing attack surface. Without traditional network perimeters to aide in the defense, credentials take center stage.

Discover and eliminate weak and shared passwords.

Finding and eliminating weak, common, and shared passwords is critical. Whether they're short or common, stored with reversible encryption, shared with multiple accounts, or have been previously compromised in a breach, weak passwords create significant risk for organizations. Through password spraying or credential stuffing attacks, they are often the vector of initial infiltration. Once an adversary has gained a foothold in an environment, shared or weak passwords for privileged accounts create opportunities for privilege escalation.

Deploy multi-factor authentication and use strong authentication factors.

Many organizations have yet to adopt multi-factor authentication (MFA) for externally facing or sensitive systems and applications. This untenable position exposes organizations to a drastically increased risk of credential compromise, and MFA must be a top priority. Organizations should avoid using text message (SMS) or voice call factors, as adversaries have demonstrated simple ways to compromise these mechanisms.

Additionally, biometric authentication factors like Windows Hello or Apple FaceID provide effective security and improved user experience over the traditional password-and-passcode approach. For highly sensitive or privileged users, use hardware security keys (like the YubiKey) to provide increased assurance. These keys can support both traditional smartcard and the more modern FIDO2/WebAuthn standards.

Federate to centrally control identities, consistently implement authentication, and detect anomalies.

Many organizations try to manage identities in multiple places (e.g. on-premises Active Directory, Amazon Web Services IAM, each cloud application, etc.), which yields inconsistent and unmanageable results for the security team and end users. Identity federation with solutions like Azure AD SSO, Okta, or Ping provide a centralized identity clearing house, enabling organizations to centrally deploy strong authentication, evaluate conditional access policies, and detect password attacks. Furthermore, they require end users to only learn one authentication process, reducing complexity and increasing the chances that an end user identifies a fraudulent login page.

NIST SP 800-63B is the new password sheriff in town.

In June of 2017, NIST published Special Publication 800-63B providing updated guidance for securing user passwords. The guidance established two core rules: 1) password length, not complexity, matters the most; 2) passwords don't need to be changed frequently, unless there is evidence that they've been compromised. Use sources like the HaveIBeenPwned compromised password database and internal detection of password spraying and anomalous authentications to establish the evidence of compromise. Provided they are not the sole authentication factor, passwords can be kept short and simple, encouraging users to use and remember unique passwords across the board.

An exception to these rules is non-human identities (e.g. service accounts), which should have as long and complex a password as supported by the platform. These passwords must also be changed frequently.

Priority #3: Embrace Active Directory privilege security

A motivated adversary will almost always find a way to breach a company's perimeter defenses, and they frequently rely on an old favorite: tricking an unsuspecting person to open a malicious email attachment or click a link leading to a malicious website. Once those defenses have been breached, adversaries often find an open playing field. Whether within the corporate network or applied to cloud services, the identity-defined perimeter is essential to limiting an adversary's options.

Continuously map and eliminate paths for lateral movement and privilege escalation.

Most breaches still measure an adversary's dwell time in the tens of days. With that amount of time, they're able to untangle complex webs of privileges that may allow them to fully compromise Active Directory. For example, the logged-on credential of the workstation an adversary compromised is also able to log on to servers. Once on the server, the adversary discovers a logged-on credential with Account Operators permissions and uses that to reset the password for a Domain Admins member. With those privileges, the adversary has compromised the directory. Understanding and eliminating these vectors is essential to preventing privilege escalation and prioritizing your defenses.

Restrict host-to-host communication.

In many organizations, all hosts in the environment are able to communicate (and perhaps authenticate) with each other. This creates a situation in which an adversary or malware only needs to compromise one host to compromise all others. Lateral movement can be constrained by ensuring hosts cannot authenticate to each other unless the services they provide require it. Lateral movement restrictions include: 1) eliminating domain accounts with broad Administrators membership on member computers; 2) using solutions like LAPS to randomize and frequently change the built-in local Administrator's password; 3) using the host-based firewall to permit network connectivity from only a list of approved hosts; 4) use Windows Defender Credential Guard to prevent credential theft.

Establish credential boundaries.

The identity perimeter is established with credential boundaries. Put simply: a policy that denies the use of the same credentials across security classifications. The objective is to prevent privilege escalation from one security classification to another using a set of credentials. At a minimum, draw boundaries around your workstations, servers, and domain controllers (and any system that has administrative access to domain controllers). In many organizations, users with Domain Admin privileges log on to workstations creating a pathway to domain dominance that is trivial to exploit. Establishing this straightforward control would deny an adversary that opportunity. It is worth noting that this approach should also be extended to additional security boundaries – not all member computers are equal. Drawing boundaries around sensitive applications (your security solutions!) and delivery zones (e.g. cloud vs. on-premises) is valuable.

Eliminate privilege, with prejudice.

Simply put – why should an account have its privileges all the time, when it is only used a small amount of time? These standing (or "always on") privileges are what enable adversaries to complete their mission. There should only be one "always on" member of your default privileged groups: the built-in domain Administrator user, which is configured with strong authentication factors and only used in emergency situations.

The same is true for member servers and workstations. Standing Administrator privileges to member workstations and servers should not exist, and solutions like Microsoft's LAPS should be used to protect the built-in local Administrator account for use in emergency situations.

JIT to the future.

After removing the "always on" privileges, administration should be conducted with just-in-time (JIT) accounts: short-lived identities that confer the necessary privileges to complete an activity and then are destroyed when the activity is complete. This approach ensures that privileges can only be obtained following approved workflows, and no artifacts of those privileges remain for an adversary to steal.

While using JIT accounts at the domain level is predominantly about constraining an adversary's ability to escalate privilege. Using them at the member computer level is about reducing the opportunity for lateral movement (which itself may lead to privilege escalation). JIT accounts on servers can grant access to one or more servers and greatly restrict both the scope and duration of lateral movement risk.

Priority #4: Increase visibility into Active Directory threats

Despite this investment in preventative controls, we must instrument our environments to find the correct threats. Network forensics, malware detection, etc. are all important parts of our onion, but too many organizations miss instrumentation of the directory to detect attacks on privilege.

Monitoring Activity Directory changes are as vital as network forensics.

Many organizations make significant investments in network forensic capabilities, but far fewer make investments in deeply understanding and controlling changes in Active Directory. As the arbiter of authentication and authorization, changes in Active Directory have the capability of affecting any system utilizing it for those purposes.

Enabling additional Windows event log types – particularly those providing deeper insight into Kerberos – or adopting technologies providing granular directory auditing are important to producing a clear picture of the authentication flow and changes that may compromise the security of the directory or systems and applications consuming its data.

Detecting attacks on credentials early is essential.

Detecting advanced-stage Active Directory attacks (like a Golden Ticket) is an important verification of your controls, or that you're commencing improvements in a healthy environment. However, detecting signs and symptoms of lateral movement and privilege escalation early is critical to preventing adversaries from being able to execute those late stage attacks or complete their mission. Improved monitoring of Active Directory and endpoints can elucidate evidence of attacks like password spraying or Pass-the-Ticket, which frequently happen during the early stages of an attack.

About Stealthbits

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.

Over nearly two decades, Stealthbits' solution and product portfolio has grown to provide comprehensive offerings focused on:

- DATA ACCESS GOVERNANCE & DATA PRIVACY
- ACTIVE DIRECTORY MANAGEMENT & SECURITY
- PRIVILEGED ACCESS MANAGEMENT

With five product platforms spanning...

Reporting & Governance
stealthAUDIT

Real-Time Threat Detection & Response
stealthDEFEND

Privileged Access Management
stealthbits PAM

Real-Time Policy Enforcement
stealthINTERCEPT

Rollback & Recovery
stealthRECOVER

...Stealthbits provides the breadth of coverage and depth of capability needed to effectively and efficiently secure the two common denominators in every breach scenario: credentials and data.

To learn more about Stealthbits, visit https://www.stealthbits.com/company.