Microsoft IT Showcase

Improving security by protecting elevated-privilege accounts at Microsoft

An ever-evolving digital landscape is forcing organizations to adapt and expand to stay ahead of innovative and complex security risks. Increasingly sophisticated and targeted threats, including phishing campaigns and malware attacks, attempt to harvest credentials or exploit hardware vulnerabilities that allow movement to other parts of the network, where they can do more damage or gain access to unprotected information.

Microsoft Core Services Engineering and Operations (CSEO), like many IT organizations, used to employ a traditional IT approach to securing the enterprise. We now know that effective security calls for a defense-in-depth approach that requires us to look at the whole environment—and everyone that accesses it—to implement policies and standards that better address risks.

To dramatically limit our attack surface and protect our assets, we developed and implemented our own defense-in-depth approach. This includes new company standards, telemetry, monitoring, tools, and processes to protect administrators and other elevated-privilege accounts.

In an environment where there are too many administrators, or elevated-privilege accounts, there is an increased risk of compromise. When elevated access is persistent or elevated-privilege accounts use the same credentials to access multiple resources, a compromised account can become a major breach.

This case study highlights the steps we are taking at Microsoft to protect our environment and administrators, including new programs, tools, and considerations, and the challenges we faced. We will provide some details about the new "Protect the Administrators" program that is positively impacting the Microsoft ecosystem. This program takes security to the next level across the entire enterprise, ultimately changing our digital-landscape security approach.

Understanding defense-in-depth protection

Securing all environments within your organization is a great first step in protecting your company. But there's no silver-bullet solution that will magically counter all threats. At Microsoft, information protection rests on a defense-in-depth approach built on device health, identity management, and data and telemetry—a concept illustrated by the three-legged security stool, in Figure 1. Getting security right is a balancing act. For a security solution to be effective, it must address all three aspects of risk mitigation on a base of risk management and assurance—or the stool topples over and information protection is at risk.

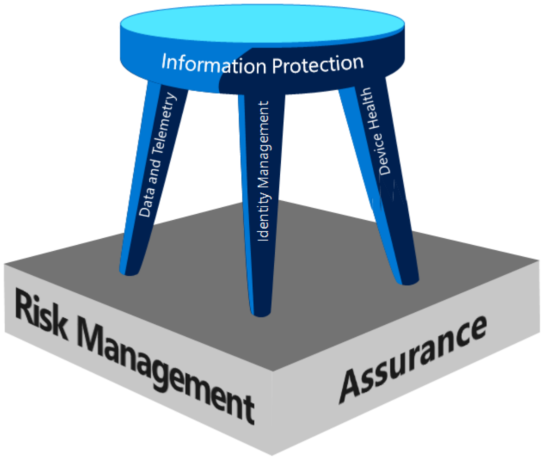

Figure 1. The three-legged-stool approach to information protection.

Risk-based approach

Though we would like to be able to fix everything at once, that simply isn't feasible. We created a risk-based approach to help us prioritize every major initiative. We used a holistic strategy that evaluated all environments, administrative roles, and access points to help us define our most critical roles and resources within the Microsoft ecosystem. Once defined, we could identify the key initiatives that would help protect the areas that represent the highest levels of risk.

As illustrated in Figure 2, the access-level roles that pose a higher risk should have fewer accounts—helping reduce the impact to the organization and control entry.

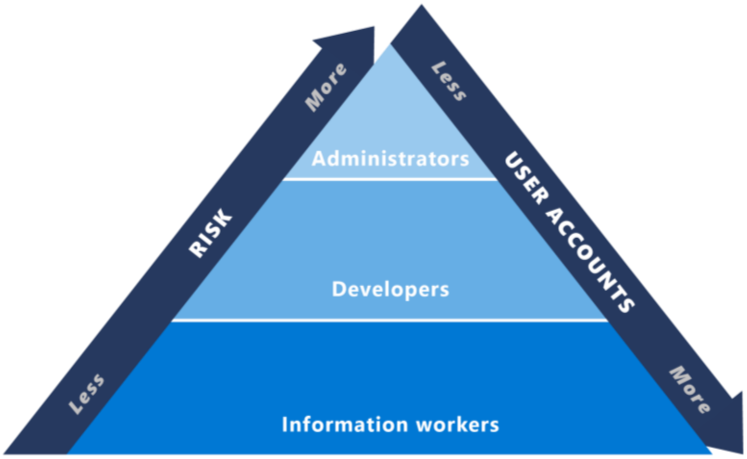

Figure 2. The risk-role pyramid

The next sections focus primarily on protecting elevated user accounts and the "Protect the Administrators" program. We'll also discuss key security initiatives that are relevant to other engineering organizations across Microsoft.

Implementing the Protect the Administrators program

After doing a deeper analysis of our environments, roles, and access points, we developed a multifaceted approach to protecting our administrators and other elevated-privilege accounts. Key solutions include:

- Working to ensure that our standards and processes are current, and that the enterprise is compliant with them.
- Creating a targeted reduction campaign to scale down the number of individuals with elevated-privilege accounts.
- Auditing elevated-privilege accounts and role management to help ensure that only employees who need elevated access retain elevated-access privileges.
- Creating a High Value Asset (HVA)—an isolated, high-risk environment—to host a secure infrastructure and help reduce the attack surface.
- Providing secure devices to administrators. Secure admin workstations (SAWs) provide a "secure keyboard" in a locked-down environment that helps curb credential-theft and credential-reuse scenarios.
- Reporting metrics and data that help us share our story with corporate leadership as well as getting buy-in from administrators and other users who have elevated-privilege accounts across the company.

Defining your corporate landscape

In the past, equipment was primarily on-premises, and it was assumed to be easier to keep development, test, and production environments separate, secure, and well-isolated without a lot of crossover. Users often had access to more than one of these environments but used a *persistent identity*—a unique combination of username and password—to log into all three. After all, it's easier to remember login information for a persistent identity than it is to create separate identities for each environment. But because we had strict network boundaries, this persistent identity wasn't a source of concern.

Today, that's not the case. The advent of the cloud has dissolved the classic network edge. The use of on-premises datacenters, cloud datacenters, and hybrid solutions are common in nearly every company. Using one persistent identity across all environments can increase the attack surface exposed to adversaries. If compromised, it can yield access to all company environments. That's what makes identity today's true new perimeter.

At Microsoft, we reviewed our ecosystem to analyze whether we could keep production and non-production environments separate. We used our Red Team/penetration (PEN) testers to help us validate our holistic approach to security, and they provided great guidance on how to further establish a secure ecosystem.

Figure 3 illustrates the Microsoft ecosystem, past and present. We have three major types of environments in our ecosystem today: our Microsoft and Office 365 tenants, Azure subscriptions, and on-premises datacenters. We now treat them all like a production environment with no division between production and non-production (development and test) environments.

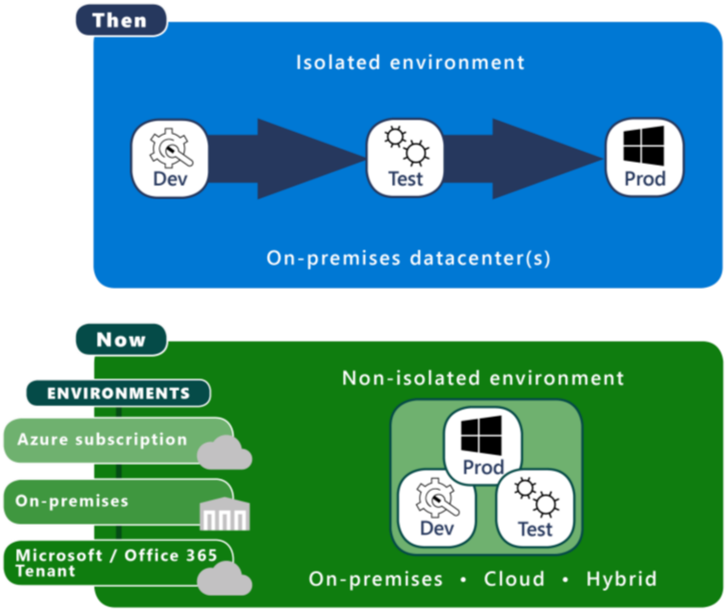

Figure 3. Now, everything is considered a "production" environment. We treat our three major environments in the Microsoft ecosystem like production.

Refining roles to reduce attack surfaces

Prior to embarking on the "Protect the Administrators" program, we felt it was necessary to evaluate every role with elevated privileges to determine their level of access and capability within our landscape. Part of the process was to identify tooling that would also protect company security (identity, security, device, and non-persistent access).

Our goal was to provide administrators the means to perform their necessary duties in support of the technical operations of Microsoft with the necessary security tooling, processes, and access capabilities—but with the lowest level of access possible.

The top security threats that every organization faces stem from too many employees having too much persistent access. Every organization's goal should be to dramatically limit their attack surface and reduce the amount of "traversing" (lateral movement across resources) a breach will allow, should a credential be compromised. This is done by limiting elevated-privilege accounts to employees whose roles require access and by ensuring that the access granted is commensurate with each role. This is known as "least-privileged access." The first step in reaching this goal is understanding and redefining the roles in your company that require elevated privileges.

Defining roles

We started with basic definitions. An information-worker account does not allow elevated privileges, is connected to the corporate network, and has access to productivity tools that let the user do things like log into SharePoint, use applications like Microsoft Excel and Word, read and send email, and browse the web.

We defined an administrator as a person who is responsible for the development, build, configuration, maintenance, support, and reliable operations of applications, networks, systems, and/or environments (cloud or on-premises datacenters). In general terms, an administrator account is one of the elevated-privilege accounts that has more access than an information worker's account.

Using role-based controls to establish elevated-privilege roles

We used a role-based access control (RBAC) model to establish which specific elevated-privilege roles were needed to perform the duties required within each line-of-business application in support of Microsoft operations. From there, we deduced a minimum number of accounts needed for each RBAC role and started the process of eliminating the excess accounts. Using the RBAC model, we went back and identified a variety of roles requiring elevated privileges in each environment.

For the Azure environments, we used RBAC, built on Azure Resource Manager, to manage who has access to Azure resources and to define what they can do with those resources and what areas they have access to. Using RBAC, you can segregate duties within your team and grant to users only the amount of access that they need to perform their jobs. Instead of giving everybody unrestricted permissions in our Azure subscription or resources, we allow only certain actions at a particular scope.

Performing role attestation

We explored role attestation for administrators who moved laterally within the company to make sure their elevated privileges didn't move with them into the new roles. Limited checks and balances were in place to ensure that the right privileges were applied or removed when someone's role changed. We fixed this immediately through a quarterly attestation process that required the individual, the manager, and the role owner to approve continued access to the role.

Implementing least-privileged access

We identified those roles that absolutely required elevated access, but not all elevated-privilege accounts are created equal. Limiting the attack surface visible to potential aggressors depends not only on reducing the number of elevated-privilege accounts. It also relies on only providing elevated-privilege accounts with the least-privileged access needed to get their respective jobs done.

For example, consider the idea of crown jewels kept in the royal family's castle. There are many roles within the operations of the castle, such as the king, the queen, the cook, the cleaning staff, and the royal guard. Not everyone can or should have access everywhere. The king and queen hold the only keys to the crown jewels. The cook needs access only to the kitchen, the larder, and the dining room. The cleaning staff needs limited access everywhere, but only to clean, and the royal guard needs access to areas where the king and queen are. No one other than the king and queen, however, needs access to the crown jewels. This system of restricted access provides two benefits:

- Only those who absolutely require access to a castle area have keys, and only to perform their assigned jobs, nothing more. If the cook tries to access the crown jewels, security alarms notify the royal guard, along with the king and queen.
- Only two people, the king and queen, have access to the crown jewels. Should anything happen to the crown jewels, a targeted evaluation of those two people takes place and doesn't require involvement of the cook, the cleaning staff, or the royal guard because they don't have access.

This is the concept of least-privileged access: We only allow you access to a specific role to perform a specific activity within a specific amount of time from a secure device while logged in from a secure identity.

Creating a secure high-risk environment

We can't truly secure our devices without having a highly secure datacenter to build and house our infrastructure. We used HVA to implement a multitiered and highly secure high-risk environment (HRE) for isolated hosting. We treated our HRE as a private cloud that lives inside a secure datacenter and is isolated from dependencies on external systems, teams, and services. Our secure tools and services are built within the HRE.

Traditional corporate networks were typically walled only at the external perimeters. Once an attacker gained access, it was easier for a breach to move across systems and environments. Production servers often reside on the same segments or on the same levels of access as clients, so you inherently gain access to servers and systems. If you start building some of your systems but you're still dependent on older tools and services that run in your production environment, it's hard to break those dependencies. Each one increases your risk of compromise.

It's important to remember that security awareness requires ongoing hygiene. New tools, resources, portals, and functionality are constantly coming online or being updated. For example, certain web browsers sometimes release updates weekly. We must continually review and approve the new releases, and then repackage and deploy the replacement to approved locations. Many companies don't have a thorough application-review process, which increases their attack surface due to poor hygiene (for example, multiple versions, third-party and malware-infested application challenges, unrestricted URL access, and lack of awareness).

The initial challenge we faced was discovering all the applications and tools that administrators were using so we could review, certify, package, and sign them as approved applications for use in the HRE and on SAWs. We also needed to implement a thorough application-review process, specific to the applications in the HRE.

Our HRE was built as a trust-nothing environment. It's isolated from other less-secure systems within the company and can only be accessed from a SAW—making it harder for adversaries to move laterally through the network looking for the weakest link. We use a combination of automation, identity isolation, and traditional firewall isolation techniques to maintain boundaries between servers, services, and the customers who use them. Admin identities are distinct from standard corporate identities and subject to more restrictive credential- and lifecycle-management practices. Admin access is scoped according to the principle of least privilege, with separate admin identities for each service. This isolation limits the scope that any one account could compromise. Additionally, every setting and configuration in the HRE must be explicitly reviewed and defined. The HRE provides a highly secure foundation that allows us to build protected solutions, services, and systems for our administrators.

Secure devices

Secure admin workstations (SAWs) are limited-use client machines that substantially reduce the risk of compromise. They are an important part of our layered, defense-in-depth approach to security. A SAW doesn't grant rights to any actual resources—it provides a "secure keyboard" in which an administrator can connect to a secure server, which itself connects to the HRE.

A SAW is an administrative-and-productivity-device-in-one, designed and built by Microsoft for one of our most critical resources—our administrators. Each administrator has a single device, a SAW, where they have a hosted virtual machine (VM) to perform their administrative duties and a corporate VM for productivity work like email, Microsoft Office products, and web browsing.

When working, administrators must keep secure devices with them, but they are responsible for them at all times. This requirement mandated that the secure device be portable. As a result, we developed a laptop that's a securely controlled and provisioned workstation. It's designed for managing valuable production systems and performing daily activities like email, document editing, and development work. The administrative partition in the SAW curbs credential-theft and credential-reuse scenarios by locking down the environment. The productivity partition is a VM with access like any other corporate device.

The SAW host is a restricted environment:

- It allows only signed or approved applications to run.
- The user doesn't have local administrative privileges on the device.
- By design, the user can browse only a restricted set of web destinations.
- All automatic updates from external parties and third-party add-ons or plug-ins are disabled.

Again, the SAW controls are only as good as the environment that holds them, which means that the SAW isn't possible without the HRE. Maintaining adherence to SAW and HRE controls requires an ongoing operational investment, similar to any Infrastructure as a Service (IaaS). Our engineers code-review and code-sign all applications, scripts, tools, and any other software that operates or runs on top of the SAW. The administrator user has no ability to download new scripts, coding modules, or software outside of a formal software distribution system. Anything added to the SAW gets reviewed before it's allowed on the device.

As we onboard an internal team onto SAW, we work with them to ensure that their services and endpoints are accessible using a SAW device. We also help them integrate their processes with SAW services.

Provisioning the administrator

Once a team has adopted the new company standard of requiring administrators to use a SAW, we deploy the Azure-based Conditional Access (CA) policy. As part of CA policy enforcement, administrators can't use their elevated privileges without a SAW. Between the time that an administrator places an order and receives the new SAW, we provide temporary access to a SAW device so they can still get their work done.

We ensure security at every step within our supply chain. That includes using a dedicated manufacturing line exclusive to SAWs, ensuring chain of custody from manufacturing to end-user validation. Since SAWs are built and configured for the specific user rather than pulling from existing inventory, the process is much different from how we provision standard corporate devices. The additional security controls in the SAW supply chain add complexity and can make scaling a challenge from the global-procurement perspective.

Supporting the administrator

SAWs come with dedicated, security-aware support services from our Secure Admin Services (SAS) team. The SAS team is responsible for the HRE and the critical SAW devices—providing around-the-clock role-service support to administrators.

The SAS team owns and supports a service portal that facilitates SAW ordering and fulfillment, role management for approved users, application and URL hosting, SAW assignment, and SAW reassignment. They're also available in a development operations (DevOps) model to assist the teams that are adopting SAWs.

As different organizations within Microsoft choose to adopt SAWs, the SAS team works to ensure they understand what they are signing up for. The team provides an overview of their support and service structure and the HRE/SAW solution architecture, as illustrated in Figure 4.

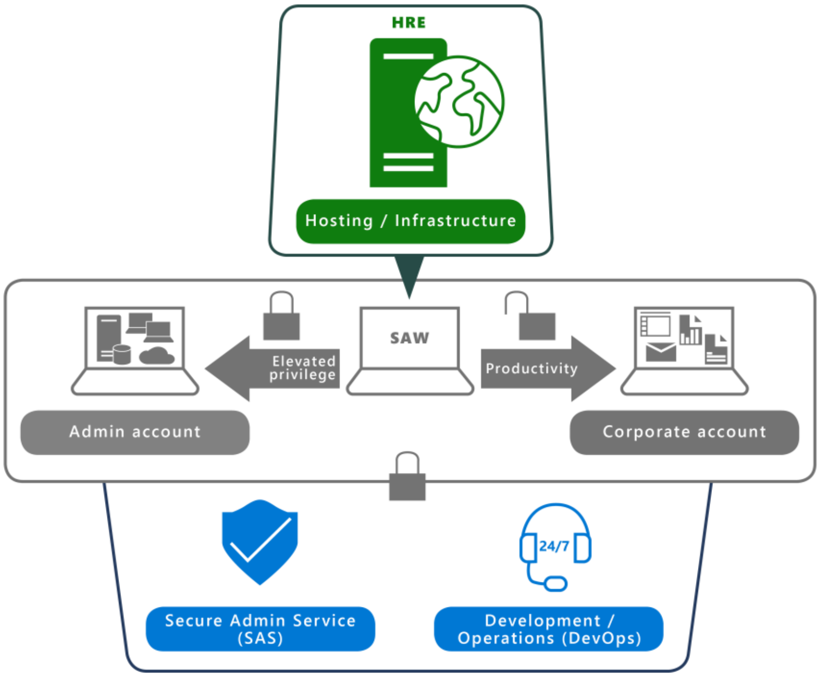

Figure 4. An overview of an isolated HRE, a SAW, and the services that help support administrators.

Today, the SAS team provides support service to more than 40,000 administrators across the company. We have more work to do as we enforce SAW usage across all teams in the company and stretch into different roles and responsibilities.

Password vaulting

The password-vaulting service allows passwords to be securely encrypted and stored for future retrieval. This eliminates the need for administrators to remember passwords, which has often resulted in passwords being written down, shared, and compromised.

SAS Password Vaulting is composed of two internal, custom services currently offered through our SAS team:

- A custom solution to manage domain-based service accounts and shared password lists.
- A local administrator password solution (LAPS) to manage server-local administrator and integrated Lights-Out (iLO) device accounts.

Password management is further enhanced by the service's capability to automatically generate and roll complex random passwords. This ensures that privileged accounts have high-strength passwords that are changed regularly and reduces the risk of credential theft.

Administrative policies

We've put administrative policies in place for privileged-account management. They're designed to protect the enterprise from risks associated with elevated administrative rights. CSEO reduces attack vectors with an assortment of security services, including SAS and Identity and Access Management, that enhance the security posture of the business. Especially important is the implementation of usage metrics for threat and vulnerability management. When a threat or vulnerability is detected, we work with our Cyber Defense Operations Center (CDOC) team. Using a variety of monitoring systems through data and telemetry measures, we ensure that compliance and enforcement teams are notified immediately. Their engagement is key to keeping the ecosystem secure.

Just-in-time entitlement system

Least-privileged access paired with a just-in-time (JIT) entitlement system provides the least amount of access to administrators for the shortest period of time. A JIT entitlement system allows users to elevate their entitlements for limited periods of time to complete elevated-privilege and administrative duties. The elevated privileges normally last between four and eight hours.

JIT allows removal of users' persistent administrative access (via Active Directory Security Groups) and replaces those entitlements with the ability to elevate into roles on-demand and just-in-time. We used proper RBAC approaches with an emphasis on providing access only to what is absolutely required. We also implemented access controls to remove excess access (for example, Global Administrator or Domain Administrator privileges).

An example of how JIT is part of our overarching defense-in-depth strategy is a scenario in which an administrator's smartcard and PIN are stolen. Even with the physical card and the PIN, an attacker would have to successfully navigate a JIT workflow process before the account would have any access rights.

Lessons learned

In the three years this project has been going on, we have learned that an ongoing commitment and investment are critical to providing defense-in-depth protection in an ever-evolving work environment. We have learned a few things that could help other companies as they decide to better protect their administrators and, thus, their company assets:

- **Securing all environments.** We needed to evolve the way we looked at our environments. Through evolving company strategy and our Red Team/PEN testing, it has been proven numerous times that successful system attacks take advantage of weak controls or bad hygiene in a development environment to access and cause havoc in production.
- **Influencing, rather than forcing, cultural change.** Microsoft employees have historically had the flexibility and freedom to do amazing things with the products and technology they had on hand. Efforts to impose any structure, rigor, or limitation on that freedom can be challenging. Taking people's flexibility away from them, even in the name of security, can generate friction. Inherently, employees want to do the right thing when it

comes to security and will adopt new and better processes and tools as long as they understand the need for them. Full support of the leadership team is critical in persuading users to change how they think about security. It was important that we developed compelling narratives for areas of change, and had the data and metrics to reinforce our messaging.

- **Scaling SAW procurement.** We secure every aspect of the end-to-end supply chain for SAWs. This level of diligence does result in more oversight and overhead. While there might be some traction around the concept of providing SAWs to all employees who have elevated-access roles, it would still be very challenging for us to scale to that level of demand. From a global perspective, it is also challenging to ensure the required chain of custody to get SAWs into the hands of administrators in more remote countries and regions. To help us overcome the challenges of scale, we used a phased approach to roll out the Admin SAW policy and provision SAWs.
- **Providing a performant SAW experience for the global workforce.** We aim to provide a performant experience for all users, regardless of their location. We have users around the world, in most major countries and regions. Supporting our global workforce has required us to think through and deal with some interesting issues regarding the geodistribution of services and resources. For instance, locations like China and some places in Europe are challenging because of connectivity requirements and performance limitations. Enforcing SAW in a global company has meant dealing with these issues so that an administrator, no matter where they are located, can effectively complete necessary work.

What’s next

As we stated before, there are no silver-bullet solutions when it comes to security. As part of our defense-in-depth approach to an ever-evolving threat landscape, there will always be new initiatives to drive.

Recently, we started exploring how to separate our administrators from our developers and using a different security approach for the developer roles. In general, developers require more flexibility than administrators.

There also continue to be many other security initiatives around device health, identity and access management, data loss protection, and corporate networking. We’re also working on the continued maturity of our compliance and governance policies and procedures.

Getting started

While it has taken us years to develop, implement, and refine our multitiered, defense-in-depth approach to security, there are some solutions that you can adopt now as you begin your journey toward improving the state of your organization’s security:

- **Design and enforce hygiene.** Ensure that you have the governance in place to drive compliance. This includes controls, standards, and policies for the environment, applications, identity and access management, and elevated access. It’s also critical that standards and policies are continually refined to reflect changes in environments and security threats. Implement governance and compliance to enforce least-privileged access. Monitor resources and applications for ongoing compliance and ensure that your standards remain current as roles evolve.
- **Implement least-privileged access.** Using proper RBAC approaches with an emphasis on providing access only to what is absolutely required is the concept of least-privileged access. Add the necessary access controls to remove the need for Global Administrator or Domain Administrator access. Just provide everyone with the access that they truly need. Build your applications, environments, and tools to use RBAC roles, and clearly define what each role can and can’t do.
- **Remove all persistent access.** All elevated access should require JIT elevation. It requires an extra step to get temporary secure access before performing elevated-privilege work. Setting persistent access to expire when it’s no longer necessary narrows your exposed attack surface.
- **Provide isolated elevated-privilege credentials.** Using an isolated identity substantially reduces the possibility of compromise after a successful phishing attack. Admin accounts without an inbox have no email to phish.

Keeping the information-worker credential separate from the elevated-privilege credential reduces the attack surface.

Microsoft Services can help

Customers interested in adopting a defense-in-depth approach to increase their security posture might want to consider implementing Privileged Access Workstations (PAW). PAWs are a key element of the Enhanced Security Administrative Environment (ESAE) reference architecture deployed by the cybersecurity professional services teams at Microsoft to protect customers against cybersecurity attacks.

For more information about engaging Microsoft Services to deploy PAWs or ESAE for your environment, contact your Microsoft representative or visit the Cybersecurity Protection page.

Reaping the rewards

Over the last two years we've had an outside security audit expert perform a cyber-essentials-plus certification process. In 2017, the security audit engineers couldn't run most of their baseline tests because the SAW was so locked down. They said it was the "most secure administrative-client audit they've ever completed." They couldn't even conduct most of their tests with the SAW's baseline, locked configuration.

In 2018, the security audit engineer said: "I had no chance; you have done everything right," and added, "You are so far beyond what any other company in the industry is doing."

Also, in 2018, our SAW project won a CSO50 Award, which recognizes security projects and initiatives that demonstrate outstanding business value and thought leadership. SAW was commended as an innovative practice and a core element of the network security strategy at Microsoft.

Ultimately, the certifications and awards help validate our defense-in-depth approach. We are building and deploying the correct solutions to support our ongoing commitment to securing Microsoft and our customers' and partners' information. It's a pleasure to see that solution recognized as a leader in the industry.

For more information

Microsoft IT Showcase

microsoft.com/itshowcase

Protecting high-risk environments with secure admin workstations

IT Expert Roundtable: How Microsoft secures elevated access with tools and privileged credentials

CISO series: Secure your privileged administrative accounts with a phased roadmap

Privileged Access Workstations

If you shopped at these 16 stores in the last year, your data might have been stolen