Sales Briefing

by Access Smart

Smart Access Enterprise Password Security

POWER LOGON ADDS SECURITY AND CONVENIENCE TO MICROSOFT'S PORTFOLIO

"When security is cumbersome, users will always circumvent security for convenience. Power LogOn is so convenient it keeps your network secure."

~ Dovell Bonnett

Dovell Bonnett

Founder and CEO of Access Smart®, LLC

POWER LOGON ADDS SECURITY AND CONVENIENCE TO MICROSOFT'S PORTFOLIO

By Dovell Bonnett, Founder and CEO of Access Smart. LLC


Agriculture


Airports


Electric Power Plants


Emergency Response


Energy


Financials

INTRODUCTION

Recently, a customer asked what features does Power LogOn add to the existing Microsoft cybersecurity architecture? In other words, where are Microsoft's cybersecurity weaknesses that Power LogOn fixes? The customer wanted to determine why they needed Power LogOn instead of just using what Microsoft already offers.

Power LogOn doesn't add new Windows features nor does it rewrite any of their existing security elements. Instead, Power LogOn takes the existing Microsoft infrastructure and adds two-factor authentication that is centrally managed by the Information Technology (IT) Administrator and easy to use for both IT and employees. When cybersecurity becomes too cumbersome or inconvenient for the user, they will always find ways to circumvent security for convenience and increased productivity. It's this circumvention that has caused many of today's data breaches. That is what Power LogOn solves.

Microsoft offers a security-rich environment of encryption, complex passwords, smartcard interfaces, LDAP (Active Directory) management, and many more features. However, what Microsoft doesn't offer are product solutions that tie all these features together into a single cybersecurity solution. Microsoft relies on third-party developers to do that. That is what Access Smart has done with Power LogOn.

For example, Active Directory stores employees' passwords and allows employees to be in control of their passwords. However, research has shown that if employees manage passwords, they will be very weak or re-used, a severe cybersecurity authentication weakness. So, how do employees login to Windows/Active Directory? If they're logging in with a password and an employee's login passwords are compromised, IT has no way of authenticating that the correct person is the one logging onto a network because all they can do is verify the password.

Most hackers use Phishing emails and social engineering to steal credentials. When employees don't know their passwords, which is the case with Power LogOn, then there is nothing to steal. IT does not always encrypt the password data files. Power LogOn uses AES-256, SHA-256, and hash salting secures all password data files automatically. Unlike certificates, passwords can be changed quickly and frequently at no cost.

CRITICAL INFRASTRUCTURE CYBERSECURITY BACKGROUND

Defense


Federal Government


Hospitals


Manufacturing


Utilities


Water Treatment

With the multitude of cyber attacks hitting companies, institutions, infrastructure, and agencies, the US Government and industry standards organizations are mandating, or highly recommend, the use of multi-factor authentication (MFA) for all computer and network access by every employee. The Department Of Homeland Security (DHS) released its Presidential Policy Directive 21: Critical Infrastructure Security and Resilence policy identifying 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

The sixteen critical infrastructures identified by Homeland Security are:

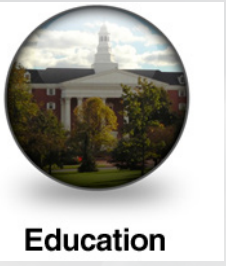
- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industry Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Health and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

DHS is working alongside the National Institute of Standards and Technology (NIST) with requirements like 800-171 for the Defence industry, 800-63b for Information Technology, and 800-53 for Emergency services. Healthcare has HIPAA and HITECH. Law enforcement has CJIS. The North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection Committee (CIPC) have implemented their CIP-002 and 003 requirements on the Energy Sector. It doesn't matter if their computer systems are online, offline, or on a VPN, they all require MFA. If a person has to access data, machines or instruments to make any changes then MFA is now required.

It also doesn't matter the size of the company that is being required to implement these cybersecurity standards. The US government is imposing strict cybersecurity standards onto their prime vendors. In turn, those primes must impose cybersecurity onto their suppliers. If anyone in the link does not incorporate cybersecurity best practices, they will be dropped as a vendor. Plus, if the prime does not follow through with enforcing cybersecurity on their suppliers, they too will be cut by the government.


Construction


Cybersecurity


Education


Pharmaceuticals


US Government Agencies


The Cloud

MICROSOFT AUTHENTICATION METHODS

There are a few different security authentication methods that Microsoft has implemented. However, the security industry has highlighted some concerns:

Hello: This is a biometric + PIN authentication. The biometrics can be either facial or fingerprint. Computer cameras are required, and many critical infrastructures do not allow network cameras. The facial recognition has already been hacked. Fingerprints have also been hacked. And, biometric information cannot be changed. Passwords allow for long complex passwords that can be changed as frequently as required at virtually no cost.

Authenticator: Authenticator is a Secure Messaging Service (SMS). SMS is not MFA but rather a two-step verification, or as I like to call it “Double-single factor authentication.” It is Something you know plus Something you know. SMS has already been declared insecure by NIST and DHS.

FIDO: FIDO-2 is a new implementation by Microsoft. While it is still being evaluated by the security community, there are some questions that have started to pop-up. One, users must carry a separate token instead of using their existing physical access ID badge. Two, all software applications must be modified to accept FIDO credentials. And three, it will require the use of Hello, where Microsoft captures, stores, and accesses the login data.

POWER LOGON

Power LogOn ties together the many different Microsoft security features so IT Administrators do not have the burden of managing all these features separately. With Power LogOn:

- Every site, network, application, and computer can have it’s own unique, long, complex password that the user doesn’t know, remember, type, generate or manage.
- Passwords can be auto-changed as frequently within Active Directory as IT requires and instantly synced to the employee’s account.
- Security settings can be customized based on each industry’s policies.
- Existing physical access ID badges can be used without any re-badging or re-issuances of badges.
- No software or backend server modifications are required.
- The employee does not need to know, remember, type, generate, or manage any company network passwords.
- The IT Administrator can create different user groups so authorized users can only access what IT determines.
- Implementation is affordable because Power LogOn leverages off a company’s existing Microsoft and Physical Access infrastructure.

POWER LOGON FOR THIN CLIENTS

Power Logon supports Thin Client environments, where multiple Thin Client terminals connect to Windows Terminal Services servers. In order to be able to use contact or contactless smart cards or ID cards at a Thin Client for logon, a card reader and reader driver must be installed on the thin client. In a typical Thin Client environment, the Power Logon client software gets installed on one or several Terminal Services servers, usually running under Windows 2012, 2016, or 2019. Once a Thin Client has initiated a Windows session, the Power LogOn client software connects to the Power LogOn server, which is typically running on another dedicated Windows server machine.

There is no need to install the Power Logon client software on the Thin Client itself. The Thin Client must support the card reader/driver. For this reason, the Thin Clients themselves can be running on operating systems such as Linux or proprietary operating systems, as long as they support the card reader and driver and the RDP protocol to connect to Windows Terminal Services.

Advantages: Typical reasons for using Thin Clients are better central control of installations, easy deployment, lower cost for terminals.

Disadvantages: Requires Terminal Services server(s) infrastructure, response times might get slower with resource-hungry applications or too many sessions running on a TS server.

CONCLUSION

Securing our critical infrastructure is paramount. However, there seem to be four significant barriers preventing implementation: Security, Compliance, Convenience, and Cost. We refer to these four parts as the Four Pillars of Cybersecurity. Power LogOn address all four of these barriers:

Security: Employee managed passwords cause over 85% of data breaches. Multi-factor authentication discourages over 95% of hackers. In the cyber chain of trust, Power LogOn secures the credentials.

Compliance: There are many different government and industry compliance regulations and these all include very similar security recommendations across all of them. Power LogOn concentrates on the recommendations and is compliant with HIPAA, CJIS, NIST 800-171, NIST 800-63b, NIST 800-53, FIPS 140-2, AES-256, SHA-256, Hash Salting, and others.

Convenience: When security is cumbersome for either the user or the IT Administrator, security will be circumvented for increased convenience and productivity. Power LogOn makes login and the management of passwords easy and secure.

Economics: Many companies and institutions still believe that a breach will not happen to them. So they take the stance of, “Pay you now, or maybe pay you later.” The “pay later” mentality can bankrupt a business. Power LogOn uses as much of the existing security and computer infrastructure as possible. Rip and Replace is not always a reasonable business model.

Login is the first line of cybersecurity defense, and it starts when the computer device is first turned on. It continues during access authenticating and record keeping. It finishes up with a secure log off so an access node is never left unattended. Power LogOn does all this and so much more.

Contact Access Smart or your reseller for access to a live, online demonstration where you can get all your questions aswered.

Dovell Bonnett
CEO – Access Smart
12400 W. Hwy. 71
Ste. 350-259
Austin, TX 78738

O: 949-218-8754
E: Dovell@access-smart.com
W: www.access-smart.com