AKCP Security Blog

Data Center Security

A data center contains the enterprise's IT equipment, applications and critical data, so it's essential to provide proper security systems and security policy.
The main concerns regarding a data center's security problems are data loss (whether it's because of human error or from external attack, or from natural disasters), data alteration, Denial of Service (DoS), identity theft, and theft of confidential information.

Hardware-wise, it starts with the physical security of a data center to prevent any physical damage and unauthorized access to the IT equipment storing critical data, including protection from natural disasters.
On the software side, having proper antivirus/antimalware solutions, up-to-date software products, proper backups and conducting frequent security audits can significantly lessen the impact of a possible security breach.

In the Cost of a Data Breach Survey where 49 U.S. companies in 14 different industry sectors participated, the following were found:

- The average cost of a security breach could reach $5.5 million
- 39% of the companies say that negligence was the primary cause of their data breaches
- Malicious and other criminal attacks have accounted for 37 percent of the total breaches
- The effects of a data breach can have severe consequences on both the company managing the data center and on the customers whose data are copied

Security status of AKCP products

Below we provide the latest information on malware and vulnerabilities in our product line (updated monthly):

- sensorProbe+ (SP+)
- sensorProbe (SP)
- securityProbe (SEC5)
- AKCPro Server (APS)

Every **firmware** release undergoes **strict security vulnerability testing**, using commercially available security vulnerability testing software. This ensures that our products are running up-to-date firmware which is free from known cyber security issues and zero-day software vulnerabilities.

A typical vulnerability test runs between 30 minutes to 2 hours, depending on the network services and open ports available on a given product family. The security scan runs on a dedicated closed network. It consists of common vulnerable ports testing, penetration testing, SNMP, SSL and web application tests, compliance checks and standard vulnerability tests.

The **antivirus scan** of AKCess Pro Server's executables is performed with **well-known antivirus engines**, such as:

- Avast
- Avira
- AVG
- BitDefender
- ClamAV
- Comodo

- ESET-NOD32
- F-Prot
- Kaspersky
- Malwarebytes
- McAfee
- Sophos
- TrendMicro
- Symantec
- Windows Defender

While we aim to provide correct and up-to-date information, it is possible that new vulnerabilities will be found before the status has been updated and new software released. If your security scanner detects a new vulnerability, don't hesitate to contact us to investigate it.

Last update: 2021-04-26

Common false positive detections in AKCP products

By default, all units have the following *possibly un-secure* configuration. This is to provide the user with ease of access and a simplified installation. It is the end user's responsibility to change the default settings of the following, if they are considered to be security flaws:

SNMP v1/v2 enabled with community: public
Remediation: change the community to a customized string, and/or disable the SNMP v1/2 protocols (disabling might affect the product's functionality).

Built-in default SSL certificate for HTTPS: un-trusted self-signed, using a possibly weak hash algorithm
Remediation: the default certificate has to be replaced with a trusted SSL certificate of the user's choice, if HTTPS access is required (we provide manuals for changing the SSL certificates on our units).

Telnet and/or SSH service: enabled by default, where supported
Remediation: disable these services if they are not needed. This might affect the product's functionality.

SNMP 'GETBULK' Reflection DDoS
The SNMP server running on our units is designed to be able to send large amounts of data quickly, if necessary. This is to avoid losing important sensor data and alerting functionality.
Remediation: configure SNMP alerts and SNMP Trap messages with only the necessary information, and distribute sending the alerts to multiple hosts.

sensorProbe+ (SP+) products

Security status: **SECURE**
Latest firmware: 1.0.5489
Vulnerabilities: NONE

sensorProbe+ units are running embedded RTOS (RealTime OS).
The lwIP network stack and a customized web server is used.
No shell access is provided.
As of firmware 5233, only the TLS v1.2 SSL protocol is enabled.

securityProbe (SEC5) products

Security status: **SECURE**
Latest firmware: 405u
Vulnerabilities: NONE

securityProbe units are running an embedded OS based on a customized Linux kernel.
The Linux network stack and a customized web server is used.
SSH and Telnet shell access is provided.
As of firmware 405u, only the TLS v1.2 SSL protocol is enabled.

sensorProbe (SP) products

Security status: **ATTENTION**
Latest firmware: 476
Vulnerabilities: SOME (see below)

sensorProbe units are running an embedded custom OS.
A customized embedded web server is used.
No shell access is provided.

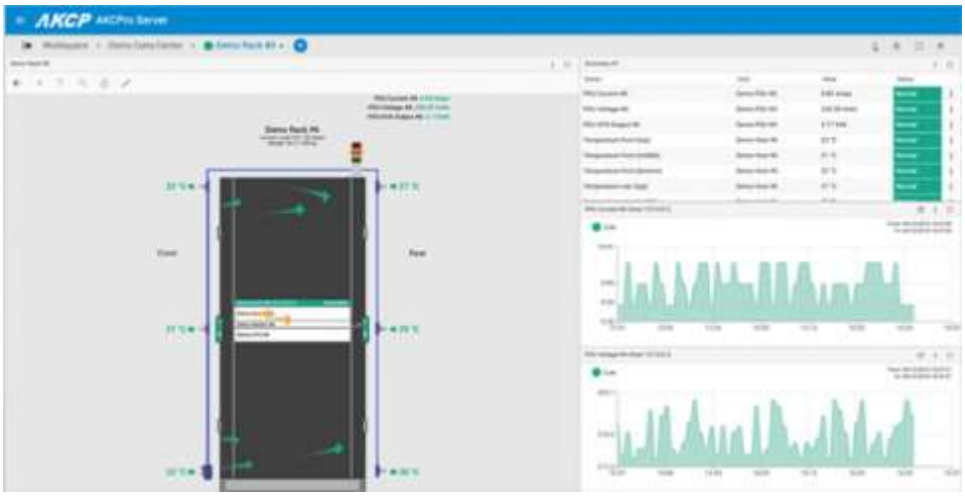
Important: the sensorProbe family doesn't provide support for any secure protocols such as SSL or HTTPS. Therefore, it doesn't support secure email or web access, and only SNMP v1/2 is supported. This might make the product unsecure in some environments, unless it's running in an isolated network.

Security scan results:

Web Application Potentially Vulnerable to Clickjacking (low risk)
The built-in web server does not set X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) for the HTTP header. This would prevent the page's content from being rendered by another site when using the frame or iframe HTML tags.
However, the sensorProbe WebUI does not utilize frames.

Web Server Transmits Cleartext Credentials
The sensorProbe family doesn't provide support for any secure protocols such as SSL or HTTPS. This might make the product unsecure in some environments, unless it's running in an isolated network.

AKCPro Server (APS)



Security status: **SECURE**
Latest version: 14.2.48
Vulnerabilities: NONE

AKCPro Server is a DCIM/CMS application (Central Monitoring Software) running on Windows platform.
A customized web server is used.
No shell access is provided.

WebApp scan results:

CGI Generic Unseen Parameters Discovery (medium risk)
There is a potential flaw which allows access to view the contents of restricted folders used by APS, such as listing the used demo image files or font files. This does NOT affect user data in any way. Our engineers are investigating this issue.

VirusTotal scan results:

We regularly scan AKCPro Server binaries with VirusTotal. This is a free service that analyzes files and URLs for viruses, worms, trojans and other kinds of malicious content.
VirusTotal inspects items with over 70 antivirus scanners and URL/domain blacklisting services, in addition to a myriad of tools to extract signals from the studied content. Any user can select a file from their computer using their browser and send it to VirusTotal.

Below is the scan result summary of each executable file used in APS. If there are some false-positive detections, we list them along with the functions of these binaries.

APS Installer file "AKCProServer-14.2.48.exe"
https://www.virustotal.com/gui/file/909618eb106fb3188b51ab2924b5ab5a5197cd82de8883c7975291aa46c0e8bd/detection

This file is the installer for the current version of APS.

VirusTotal lists 1 engine detected this file:
VBA32: BScope.Trojan.Shelma

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as program installation, service starting and Registry modification.

"C:\Program Files (x86)\AKCP\AKCPro Server\uninst.exe"
https://www.virustotal.com/gui/file/0c22c7904e021305aafa3042260a924128773b11d2a5e01d670bd3d9956c3abd/detection

The uninst.exe is the uninstaller EXE of APS, it performs file and registry removal functions when APS is uninstalled from a system.

VirusTotal lists 1 engine detected this file:
SecureAge APEX: Malicious

This is a false positive result, since only 1 of all antivirus engines have detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as automatic service stopping and Registry modification.

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\AKCProServer.exe"
https://www.virustotal.com/gui/file/f0f10cb768cb23f6baa24d365b139f461d8e707a6f6ada7674ef43eb9b38011f/detection

AKCProServer.exe is the main process (Control) of APS.

VirusTotal lists 1 engine detected this file:
Bkav: W32.AIDetectVM.malware1

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as low-level network socket creation (RPC port, communication with the monitored devices) and multiple sub-process spawning (for handling notifications).

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\CustomNotification.exe"
https://www.virustotal.com/gui/file/742e5ee06e47570abb2e4013f9a3d9b0377961e4f1cbe4d957983919a9509aed/detection

CustomNotification.exe is a notification sub-module of APS.

VirusTotal lists 1 engine detected this file:
Bkav: W32.AIDetectVM.malware2

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.

There are some patterns within this application that could resemble behavior of a virus, such as running scripts as a system user (for handling notifications).

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\DbRecovery.exe"
https://www.virustotal.com/gui/file/6cd2665776d82560e932abb4682807916b7f59f31316c9d422eac8fb3cac1bfc/detection

The DbRecovery.exe is a standalone process of APS, it only runs when necessary. It is used for checking and fixing the internal database (SQLite) when needed.

VirusTotal lists 1 engine detected this file:
Cylance: Unsafe

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as database modification.

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\DialNotification.exe"
https://www.virustotal.com/gui/file/0055ed3b1e668665e509d5a70f1d7d51ce246ee84daef13034de16ffa386aa5b/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\DoorLockNotification.exe"
https://www.virustotal.com/gui/file/86dddc2bcb23dbc53404dead8c62b6d99fb9d06b22f08a7c468549364e256536/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\DryContactNotification.exe"
https://www.virustotal.com/gui/file/0d0e164655f7f8cc2b72bfd99969b6e2425474d270d13a6e8136e0ed7eb735b1/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\EmailNotification.exe"
https://www.virustotal.com/gui/file/fa3f0bc86e9a75eef82b6181964b6ef74016f61618cf0f8590fae716b9d44390/detection

The EmailNotification.exe is a notification sub-process of APS and is used for sending emails.

VirusTotal lists 1 engine detected this file:
Bkav: W32.AIDetectVM.malware2

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as automated email sending.

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\FaxNotification.exe"
https://www.virustotal.com/gui/file/3be56cd6a21a13c48a9b11100e1dd7d5957124996454b30e98ac98ade59851ae/detection

The FaxNotification.exe is a notification sub-process of APS and is used for sending faxes.

VirusTotal lists 1 engine detected this file:
Bkav: W32.AIDetectVM.malware2

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.

There are some patterns within this application that could resemble behavior of a virus, such as automated fax sending.

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\FTPNotification.exe"
https://www.virustotal.com/gui/file/1f887ffe903e40a8bb784ae9c7a5085b2135f2cf4bb5b92547e575c7046015a3/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\mergeLangJson.exe"
https://www.virustotal.com/gui/file/fb56c5e307d4c5b75798779b5d68a813b8731bb4c7500a511c22ebcc456d4c58/detection

The mergeLangJson.exe is used by the APS installer to merge old and new language files together.

VirusTotal lists 1 engine detected this file:
SecureAge APEX: Malicious

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as automatic file modification.

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\MMSNotification.exe"
https://www.virustotal.com/gui/file/a8f8393cc9c8b786fbea71d8140bda275939305465e9181e57a19cfa0e9b68eb/detection

The MMSNotification.exe is a notification sub-process of APS and is used for sending MMSes.

VirusTotal lists 1 engine detected this file:
Bkav: W32.AIDetectVM.malware1

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as automated MMS sending.

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\ModbusNotification.exe"
https://www.virustotal.com/gui/file/7d39830f31c7e293145bcd9fb84c3a63e23f82f337c3f08bd37e373eb15eb171/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\notificationServer.exe"
https://www.virustotal.com/gui/file/f283e86a2a4f9e006194144f8952db134de570b9789d6416633bc67bfd3f538c/detection

The notificationServer.exe is the notification handler sub-process of APS and is used for controlling each notifications.

VirusTotal lists 1 engine detected this file:
Bkav: W32.AIDetectVM.malware2

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as automated process starting/stopping.

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\RecorderNotification.exe"

https://www.virustotal.com/gui/file/328c854d02d6078b07ab6425178d7e8719c2f14a97156ebfac7c8a736685ccd7/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\RelayNotification.exe"
https://www.virustotal.com/gui/file/a4d23228753ddeff67e7f409e8334dfdfff21039d8df9ecd555a36ea4be6f721/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\serverManagerService.exe"
https://www.virustotal.com/gui/file/f16cf6d30894e7aa359e7e41398e221a69edc29ca4f6f455e7e98716d793b033/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\serverManagerUI.exe"
https://www.virustotal.com/gui/file/3ded9cb346ec1801e9a0a1a1141850845ca9ee1c098df90ba3c4de6850a8f636/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\ShutdownNotification.exe"
https://www.virustotal.com/gui/file/009c44761760de7ab1b1df458fbed79c736bf2c2da3e0a7a548c9cc926d5a1ca/detection

The ShutdownNotification.exe is a notification sub-process of APS and is used for sending a shutdown command to a prepared Unix or Windows system (for example when power failure is detected).

VirusTotal lists 1 engine detected this file:
Bkav: W32.AIDetectVM.malware1

This is a false positive result, since only 1 of all antivirus engines has detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as low-level network socket creation (communication with remote systems, remote shutdown).

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\SirenNotification.exe"
https://www.virustotal.com/gui/file/f07182656292cc0b4e91ab591cd34bd333b450e714301213b871b38f689d2425/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\SkypeNotification.exe"
https://www.virustotal.com/gui/file/46d901760753ccbc3321c2d3f39d5d3926aee7856e97af0145e75fd506453f60/detection

The SkypeNotification.exe is a notification sub-process of APS and is used for sending Skype messages.

VirusTotal lists 1 engine detected this file:
Bkav: W32.AIDetectVM.malware2

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as automated message sending.

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\SMSNotification.exe"
https://www.virustotal.com/gui/file/0c93754e7b2ba75bf19ad93a5e86ad58b4039f9a1fd72f8fda13e301d72e0331/detection

The SMSNotification.exe is a notification sub-process of APS and is used for sending SMS notification messages to mobile phones using supported modems.

VirusTotal lists 1 engine detected this file:
Bkav: W32.AIDetectVM.malware1

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as automated message sending.

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\SnmpSetNotification.exe"
https://www.virustotal.com/gui/file/6b7c150fe611dfaccfd0be8024a2f90397d12aba92a7837927f812480bebc3c9/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\SoundNotification.exe"
https://www.virustotal.com/gui/file/572d533cfac2c902c651f9db267cdea639ebaee2725f14c5f2a8b1584d9e89b7/detection

The SoundNotification.exe is a notification sub-process of APS and is used for generating sound notification messages on the local PC.

VirusTotal lists 1 engine detected this file:
Bkav: W32.AIDetectVM.malware2

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as low-level control of the sound card for playing an alarm.

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\SpeechNotification.exe"
https://www.virustotal.com/gui/file/9eb923bbd4b5b492730ee03f018dbe943e6d2c015ea1ad147a4359a61d9e315b/detection

The SpeechNotification.exe is a notification sub-process of APS and is used for sending telephone call (voice) notification messages to mobile phones using supported modems.

VirusTotal lists 1 engine detected this file:
Bkav: W32.AIDetectVM.malware2

This is a false positive result, since only 1 of all antivirus engines has detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as low-level network socket creation (communication with modem serial port to perform a voice call).

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\StopRecorderNotification.exe"
https://www.virustotal.com/gui/file/4210cc53b75095ac0962a7476d61fa3fcae359838c1736e2955d058569888a79/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\TrapNotification.exe"
https://www.virustotal.com/gui/file/a673b2af80d3e087afee61f0a6282a155c1021333365fe02c88397efdeccbfbc/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\VPNAuthen.exe"
https://www.virustotal.com/gui/file/c8058fac3395c5db7b48d5459b74c356c33d86c232e7ad864da64181606c1e2e/detection

"C:\Program Files (x86)\AKCP\AKCPro Server\bin\WindowsNotification.exe"
https://www.virustotal.com/gui/file/7fbe244ed37fe15d1ea55dce0da4fa8bbb7a22a6fa969997363fd8ff0979f4aa/detection

The WindowsNotification.exe is a notification sub-process of APS and is used for sending Windows alerts (requires the Windows Alert installed on the target machine).

VirusTotal lists 1 engine detected this file:
Bkav: W32.AIDetectVM.malware2

This is a false positive result, since only 1 antivirus engine have detected the file as malicious.
There are some patterns within this application that could resemble behavior of a virus, such as automated connection to another PC for alert sending.