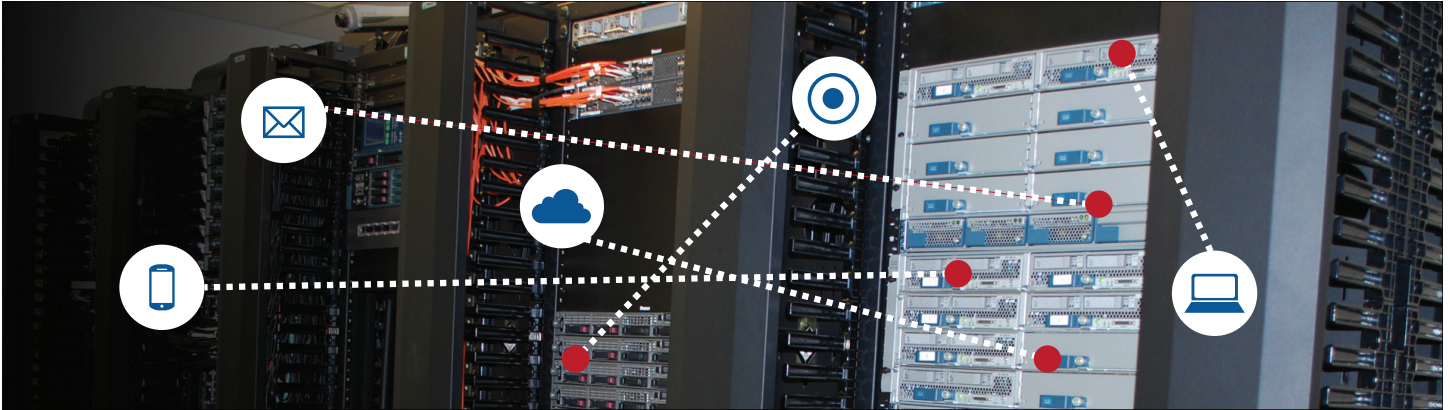




Cyber Security and Your Organization

Security threats are constantly evolving and are more sophisticated than ever. IDG estimates that cyber crime damage costs are to hit \$6 trillion annually by 2021, up from \$3 trillion just a year ago. The FBI is the lead federal agency for investigating cyber-attacks by criminals, overseas adversaries, and terrorists. According to the FBI, the threat is incredibly serious and growing. Our nation's critical infrastructure including private and public sector networks are targeted by adversaries.

Malware, Phishing, Spoofing, Ransomware, Identity Theft and more are real threats and organizations like yours are effected every day. In recent headlines, school districts, government, healthcare, utilities, businesses and others have been hit with spoofed email addresses, phishing emails, data breach and redirect of employee paychecks, data breach of W-2 information, and ransomware attacks! A California community college recently came under attack that caused widespread disruption to email, web, voicemail, locked out 1,800 students and teachers and ultimately cost the college \$28,000 per incident to unlock the ransomware.

Attacks come from many sources, including computer geeks looking for bragging rights, and criminals wanting to steal personal information for ransom or to sell on black markets. Hackers exploit network vulnerabilities along with new vectors including mobile, cloud, and Internet of Things (IoT) and others.

These cyber attacks can be catastrophic: from loss of sensitive data, disruption of operations, financial losses, embarrassment, harm to the organization's reputation and even lost jobs. Despite these statistics and the increase in frequency of security breaches, many organizations haven't seriously addressed the risks. It's not if a security breach is going to happen, it's when it will happen.

AMS.NET has a security solution that will fill in the gaps and deliver you comprehensive protection to minimize the risk to your organization. AMS.NET's security solution protects sensitive company information, banking information, employee social security numbers, tax forms and more. This security guide will walk you through real risks, security solutions and how to implement them to protect your organization!

Comprehensive Security Solution - Let us fill in the gaps!

Security Threats

MALWARE

Malware is a common and prevalent type of security threat and network attack. Malware means malicious software. This is a general term that encompasses many online security threats including spyware, viruses, worms, Trojans, ransomware and more.

Virus 🔥

A computer virus is a piece of code that infects software and then spreads from file to file on a system often through executable files (.exe). If the file is shared between computers, the virus then spreads to the new host.

Spyware 🔥🔥🔥🔥

Tracks your internet activities in order to steal information such as credit card numbers and passwords.

Worms 🔥

Worms replicate themselves and spread when they infect a computer. They spread across networks without the guidance of a hacker or file to latch onto. They use up your computer hard disk space and consume bandwidth while spreading.

Trojans 🔥

Trojans are designed to fool users so that they unwittingly install it on their systems and later use it to steal both financial and personal information.

Botnet 🔥🔥🔥🔥

This security risk installs malware to take control of all of the computer bots. It infects through drive-by downloads or Trojan infection. It then uses the victim's computer for a larger scale attack like DDoS.

Ransomware 🔥🔥🔥🔥🔥

Ransomware is a type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them. Ransomware utilizes emails that appear legitimate with embedded ransomware code or a legitimate looking URL that directs the victim to a website that infects their computer with malicious software. The malware encrypts local drive files and folders, attached drives, backup drives and other computers on the network. Gaining access to files requires a payment, often with bitcoins.

NETWORK ATTACKS

Network attacks are security threats to your network by passive means for monitoring or active with the intent to corrupt or destroy the data or network itself.

DDoS Attack 🔥🔥🔥

A DDoS (Denial-of-Service) Attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.

Sniffing/Snooping 🔥🔥🔥

This risk is essentially eavesdropping on your network and interpreting the traffic in order to obtain private information.

Spoofing 🔥🔥

An IP address is falsely assumed or spoofed. An attacker might use this to construct IP packets that appear to originate from valid addresses inside the organizations intranet.

Celebrating More Than **25** Years

Learn More!

Go to www.ams.net/security

800-893-3660

SOCIAL ENGINEERING

Security threats are rapidly becoming more complex and personal. As more private information becomes public through social media sites, including Facebook and LinkedIn, along with websites publishing executive bios and IT contact information, it becomes easier for hackers to carry out social engineering attacks. The proliferation of personal information such as where an individual works, whom they interact with socially and professionally, what conferences they attend, when and where they vacation, etc. has enabled hackers to use personalized emails and websites to carry out their attacks. These attacks involve some form of psychological manipulation to fool users or employees into handing over confidential or sensitive data. Social engineering invokes urgency or fear to prompt the victim to click a malicious link, open a malicious file and ultimately provide confidential information for financial gain and access to systems.

Phishing 🔥🔥🔥🔥

Phishing uses fake emails or websites to attempt to “fish” sensitive information by posing as a credible source. Phishing emails are designed with legitimate looking logos and are sent to large number of users in the attempt to get users to click on links of fake websites where they will steal credentials and the victims identity. The majority of data breaches come from some type of phishing.

Pharming 🔥🔥🔥🔥

Pharming is a specific type of phishing using DNS hijacking to redirect the users’ browser to fraudulent sites or servers.

Spear Phishing 🔥🔥🔥🔥

Spear phishing targets a select group of people with something in common - they work at the same company, bank at the same institution, order from the same website, etc. Emails are sent from the same organizations or individuals that the potential victim would normally get emails from and entice the user to click on a link and provide passwords, account numbers or other personal and confidential information. Once they have this information, they can access your bank account and create a whole new identity with that information.

Whaling 🔥🔥🔥🔥

Whaling is a form of personalized phishing usually aimed at senior executives in an organization who have access to not only financial information but access to systems. Hackers use personal information gained from social media sites and other methods to tailor messages that executives are more likely to respond to.

Common Social Engineering Scams

- FedEx and UPS tracking notices
- Banking emails
- Invoices or payment messages
- Order or quote request
- Spoofed emails from known user to yourself
- Spoofing emails from executives at your organization
- Urgent IRS notices
- Update password emails
- Shared files from email account- Office 365, Gmail, etc.
- Dropbox or Office 365 link
- Facebook messages

Celebrating More Than **25** Years

Learn More!

Go to www.ams.net/security
800-893-3660

Threat Prevention Steps

To effectively stop security threats and prevent Cyber security crime, organizations must rely on a comprehensive security solution along with training and education to address the social engineering aspect of cyber crime. Advanced malware protection, next-generation firewall, cloud security, and additional security technology components are vital. Along with technology safeguards, organizations must educate staff on security risks, what to look for, and how to avoid being a hacker's next victim.

4 Main Prevention Steps

1. Identify High-Risk Employees

High-risk employees for phishing and whaling attacks are CEO's, CFO's, CBO's, administrators, human resource personnel, financial employees and IT staff. These types of employees should have additional safeguards in place to minimize risk such as multi-level approval and phone call confirmations for banking information, wire transfers, etc.

2. Training

Employees need to be trained on the latest attacks. Examples should be provided based on the user group (executives, administrators, IT staff, etc.) so that everyone knows how to spot a suspect email or security threat. Techniques should be provided to identify security threats, including:

- How to identify phony links with mouse-over website link skills
- Look for awkward wording and misspelling
- Beware of time-sensitive issues
- Most companies, banks and agencies don't request personal information via email
- Looking at the "from" email address
- Always enter a URL manually instead of clicking the email link
- Identify encrypted website by secure browser icon (look for and click on lock icon in browser address bar)
- Never enter personal information in a pop-up screen or click on it
- Make employees aware that social media sites are used to obtain personal information
- Teach employees not to release personal or confidential information via phone or email

3. Policy

Organizations should set policies, publish them and make sure employees follow them. These should be reviewed regularly for gaps and adjusted accordingly. Policy suggestions include:

- Do not open attachments from an unknown source
- Do not click on links without first hovering over to see the url
- Do not reuse work passwords on other sites or machines
- Keep passwords confidential and enforce password change every 120 days
- Implement two-factor authentication for iCloud, Google Apps, Office 365, Salesforce, etc. for an added layer of security using both a password and a security code sent to your phone via text or call.
- Do not allow logging in or connecting using 3rd party applications
- Limit access to cloud services by IP address or subnet
- Implement a cloud access security policy
- Do not release confidential employee information via phone or email
- Restrict who can release banking information and set limits to wire transfers; require authorization by multiple people and phone confirmation

4. Technology- AMS.NET Security Solution

Organizations should evaluate current security solution and identify gaps and possible security breach points. Does your organization have the necessary security for virus protection, web security, email security, cloud security, next-generation firewall and others? [Refer to the AMS.NET Security Solution Chart →→](#)

Celebrating More Than **25** Years

Learn More!

Go to www.ams.net/security

800-893-3660



AMS.NET
Technology Solution Provider

AMS.NET Security Solution

Security Threat	Security Breach Point	Solution
Malware Virus Spyware Worms Trojans Botnet	Servers	Next-Gen Firewall (Threat), Endpoint Malware/AV Protection, Network Access Control, Network Visibility
	Desktop, Laptop, Tablets, Cell Phone	Next-Gen Firewall (Threat, Malware, Content Filtering), Endpoint Malware/AV Protection, Cloud Security, Network Access Control, Network Visibility
	Email	Endpoint Malware/AV Protection, Email Security, Network Visibility
	Web Traffic	Next-Gen Firewall (Threat, Malware, Content Filtering), Endpoint Malware/AV Protection, Cloud Security, Network Access Control, Network Visibility
	Cloud	Endpoint Malware/AV Protection, Cloud Security
Ransomware	Email	Next-Gen Firewall (Threat, Malware, Content Filtering), Endpoint Malware/AV Protection, Cloud Security, Email Security, Network Access Control, Network Visibility
	Web Traffic	Next-Gen Firewall (Threat, Malware, Content Filtering), Endpoint Malware/AV Protection, Cloud Security, Network Access Control, Network Visibility
DDoS Attack (Internal) (External)	Web Traffic	Next-Gen Firewall (Threat), Endpoint Malware/AV Protection, Network Access Control, Network Visibility
	Web Traffic	ISP Solutions
Sniffing/Snooping	Network	Next-Gen Firewall (Threat), Network Access Control
Spoofing	Website	Next-Gen Firewall (Threat, Malware, Content Filtering), Endpoint Malware/AV Protection, Cloud Security, Network Access Control, Network Visibility
	Email	Next-Gen Firewall (Threat, Malware, Content Filtering), Endpoint Malware/AV Protection, Cloud Security, Email Security, Network Visibility
Social Engineering Phishing Pharming Spear Phishing Whaling	Email	Next-Gen Firewall (Threat, Malware, Content Filtering), Endpoint Malware/AV Protection, Cloud Security, Email Security, Network Visibility
	Web Traffic	Next-Gen Firewall, Endpoint Malware/AV Protection, Cloud Security, Network Visibility
Identity Theft	Network Services	Two-Factor Authentication, Cloud Security, Network Access Control

**AV Protection is Anti-Virus Protection*

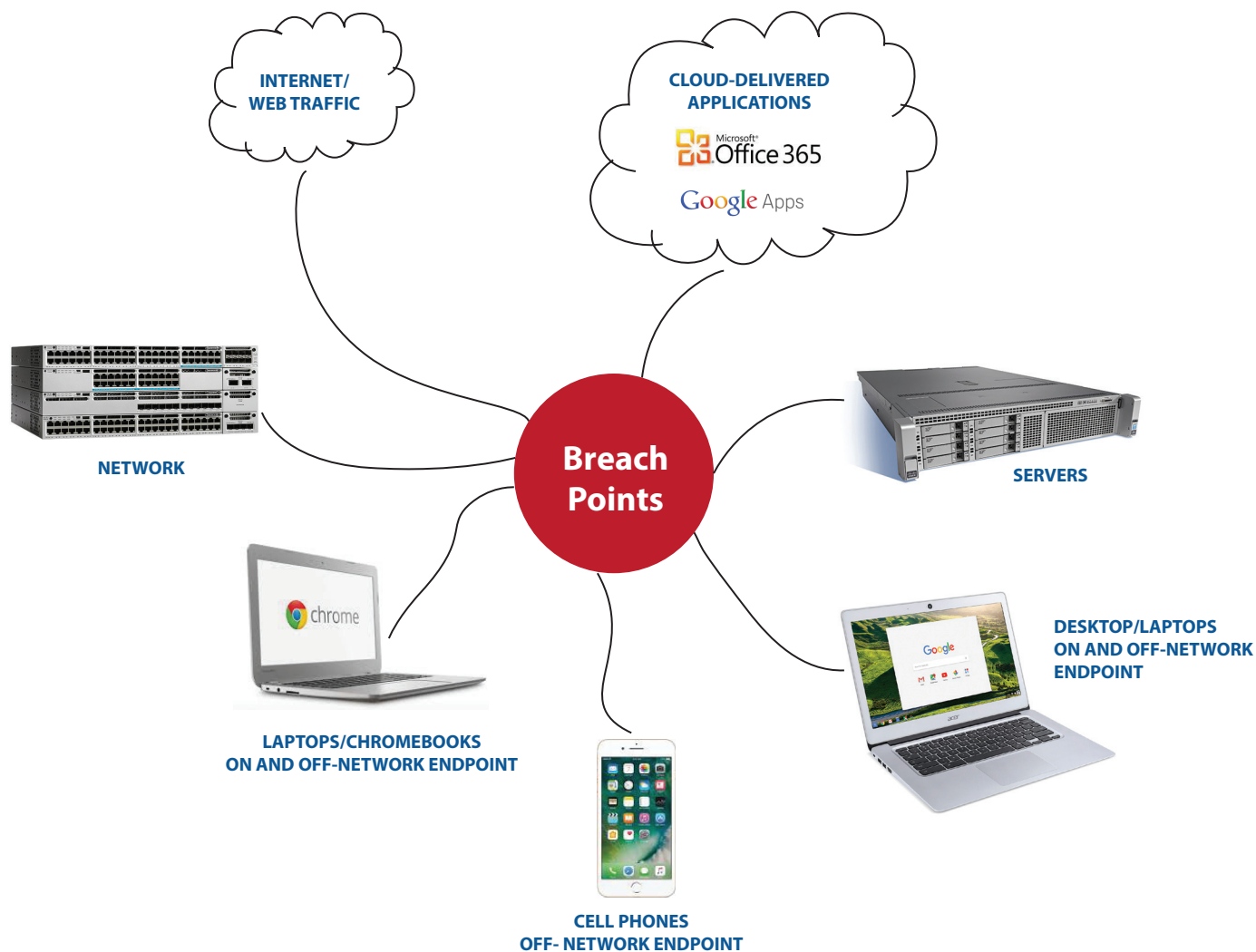
Where are your security gaps?

Celebrating More Than **25** Years

Learn More!

Go to www.ams.net/security
800-893-3660

Security Breach Points



Celebrating More Than **25** Years

Learn More!

Go to www.ams.net/security
800-893-3660

Security Solutions

Next-Gen Firewall

Next generation firewalls are fully integrated, threat-focused firewalls to stop security threats at the Internet edge, data center, branch or interdepartmental. Next-gen firewall provide full control of traffic based on applications, users, and traffic content.

Integrated visibility and control, threat defense, malware protection, content and URL filtering, policy management and other services provide superior visibility into your environment. These integrated solutions enable you to discover, track, and block the progression of suspect files and malware to prevent the spread of outbreaks and reinfection.

Centralized management provides configuration, logging, monitoring, and reporting for simplified management of the entire environment. Data including indicators of compromise (IoC) and automated event impact assessments provide actionable intelligence for IT staff.

Threat

Next generation firewall threat software gives you the visibility to help stop the latest threats. Real-time contextual awareness allows you to see and correlate applications, users, devices, operating systems, vulnerabilities, services, processes, network behaviors, files, threats and more. Intelligent security automation allows you to correlate threat events with vulnerabilities to prioritize threats and implement policies.

Malware

Integrated malware protection enables you to address both known and unknown threats with containment and remediation. Threat intelligence analyzes millions of malware samples per day, then malware software correlates files and behavior to defend against threats. Sandboxing provides automated analysis and allows your IT staff to prioritize and block attacks.

Content Filtering

Content and URL filtering integrated into the next generation firewall provides the security and control to thwart web security threats. Security intelligence provides real-time threat intelligence and protection against web-based attacks. This continuous protection is based on the identification of unknown, unusual behaviors and zero hour outbreaks through a heuristics-based, antimalware engine. Content filtering allows IT to set and enforce web use policies across the entire environment based on user, application and web content. You can enforce policies on hundreds of millions of URLs in more than 80 categories. A simple, centralized management tool provides visibility, tracking and reporting.

Highlights

- ▶ Integrated next-gen firewall provides full control of traffic based on users, applications, and the traffic content
- ▶ Consolidate security vendors with single vendor integrated solution
- ▶ Security and threat intelligence capabilities provide security across the entire attack continuum

Product Details

- ▶ Next-gen firewall at the Internet edge, data center, branch or interdepartmental
- ▶ Support for 1/10/40 Gigabit Ethernet

Celebrating More Than **25** Years

Learn More!

Go to www.ams.net/security
800-893-3660

Security Solutions

Endpoint Malware/Anti-Virus Protection

Endpoint malware and anti-virus protection blocks malware trying to enter your network from the point of entry in real time. Using AV detection engines, one-to-one signature matching, machine learning, and fuzzy fingerprinting, malware protection analyzes files at the point of entry to catch known and unknown malware. Protect your entire network including email and web traffic.

Global threat intelligence provides analysis of millions of malware samples and terabytes of data per day. This intelligence is used to correlate files, telemetry data, and file behavior against this context-rich knowledge base to proactively defend against known and emerging threats.

Once a file enters your network, malware protection continues to watch, analyze, and record its activity. If malicious behavior is spotted later, the malware protection sends your security team a retrospective alert that tells them where the malware came from, where it's been, and what it's doing. In a few clicks, you can contain and remediate it.

Cloud Security

Cloud security utilizes DNS-based security and an API-approach to protect users against threats on the Internet, wherever users go. With cloud-delivered security you can protect users, mobile devices, data and applications to stop malware before it reaches your network, endpoints or cloud applications.

Cloud security solutions provide protection for recursive DNS look-ups which lead to malware, ransomware and other security threats. Security intelligence analyzes terabytes of data in real-time across all markets, geographies, and protocols. This analysis provides visibility into where threats are coming from, who is launching them, where they call back to, and how widespread it is. This intelligence allows the cloud security solution to determine if a DNS request should be allowed or if it should block the request over any port or protocol to prevent infiltration and exfiltration attempts. Proactive security stops threats before a connection is even established. Protection is provided to every device on or off the network.

The cloud API-approach to security protects organizations against data breaches in any cloud environment and application. Advanced machine learning detects anomalies in account usage, identifies suspicious activities and discovers and controls malicious cloud apps connected to your environment.

Highlights

- ▶ Network, endpoints, web and email protection
- ▶ Global threat intelligence
- ▶ Continuous malware/virus protection
- ▶ Protects devices on & off the network

Product Details

- ▶ Deploy on endpoints- Mac, Windows, or Linux desktop, Mac, Windows, or Linux laptop
- ▶ Web-based management portal

Highlights

- ▶ Threat prevention- stop threats before they reach your network
- ▶ Protects devices on & off the network
- ▶ Protects SaaS environments
- ▶ Provides web content filtering
- ▶ Utilizes DNS blocking algorithm API-approach and security data
- ▶ Superior visibility & analytics
- ▶ Fast deployment

Product Details

- ▶ Implement roaming client to protect endpoints when VPN is off
- ▶ Web-based management portal

Celebrating More Than **25** Years

Learn More!

Go to www.ams.net/security
800-893-3660

Security Solutions

Network Visibility

Network visibility solutions extend your network visibility to detect attacks faster. Visibility into all traffic flows, applications, users, and devices that are known and unknown enables IT to monitor the entire infrastructure and detect attacks that get past perimeter defenses. Continuous network traffic analysis provides the visibility to quickly detect and respond to security attacks.

Network Access Control

Network access control as a part of a security solution provides secure access control based on role to provide consistent network access from the wired or wireless network. Visibility into the users and devices accessing the network enables you to ensure only the right people get access.

Network access control can assess vulnerabilities, apply threat intelligence and dynamically change network privileges in the event that an endpoint's threat score changes. This enables you to contain threats before they spread further in the network. Management tools allow you to easily provide secure guest access and support bring-your-own device programs (BYOD). You are able to manage the entire network, get visibility during an attack and contain infected endpoints for remediation or removal.

Email Security

Email is the number one threat vector for cyberattacks! Phishing and Spoofing Attacks spread malware through use of email. Cloud-based SaaS applications including Office 365 need an updated security solution to minimize security risks. Email security as a part of a comprehensive security solution is essential to protecting your organization against these threats.

Email security solutions monitor and filter all inbound and outbound email traffic using effective policy-based data loss prevention and encryption. Its sophisticated filter strategy blocks spam and targeted attacks using reputation, malware, and outbreak filters. Security intelligence continually monitors and detects threats from more than 75TB of web data per day and more than 1.6 million deployed devices.

Highlights

- ▶ Complete network visibility
- ▶ Detect threats faster
- ▶ Speeds up incident response

Product Details

- ▶ Deployed as a physical, virtual or cloud-based appliance
- ▶ Web-based management console

Highlights

- ▶ Secure access control
- ▶ Management of wired & wireless network
- ▶ Apply threat intelligence
- ▶ Superior visibility & analytics
- ▶ Dynamic profiling of users or devices

Product Details

- ▶ Deployed on physical or virtual server
- ▶ Easy-to-use interface for visibility of users and devices

Highlights

- ▶ Detect Phishing and Spoofing attacks
- ▶ Spam filtering
- ▶ Secure Office 365
- ▶ Continuous monitoring

Product Details

- ▶ Protects on-premises and cloud email platforms
- ▶ On-premise, cloud, virtual and hybrid deployments available

Celebrating More Than **25** Years

Learn More!

Go to www.ams.net/security
800-893-3660

Let us help fill the gaps in your security solution.

What's Next?

Call us at 800-893-3660 to schedule a security review with your AMS.NET Account Manager and Sales Engineer. They'll sit down with you to analyze your current environment, review the high risk security threats, potential gaps in your existing solution and develop a plan to provide greater protection for your organization.

About AMS.NET

AMS.NET is an innovative technology solution provider delivering business outcomes to organizations for more than 25 years. Our industry expertise, technology vision and people create a unique customer experience. Visit www.ams.net for more information.

**We cannot guarantee to protect against 100% of security threats but significantly reduce the risk and minimize threats. Information provided in this guide is service to our customers. Ask permission to use this content in any other manner.
- All Rights Reserved, 2017*

Celebrating More Than **25** Years

Learn More!

Go to www.ams.net/security
800-893-3660