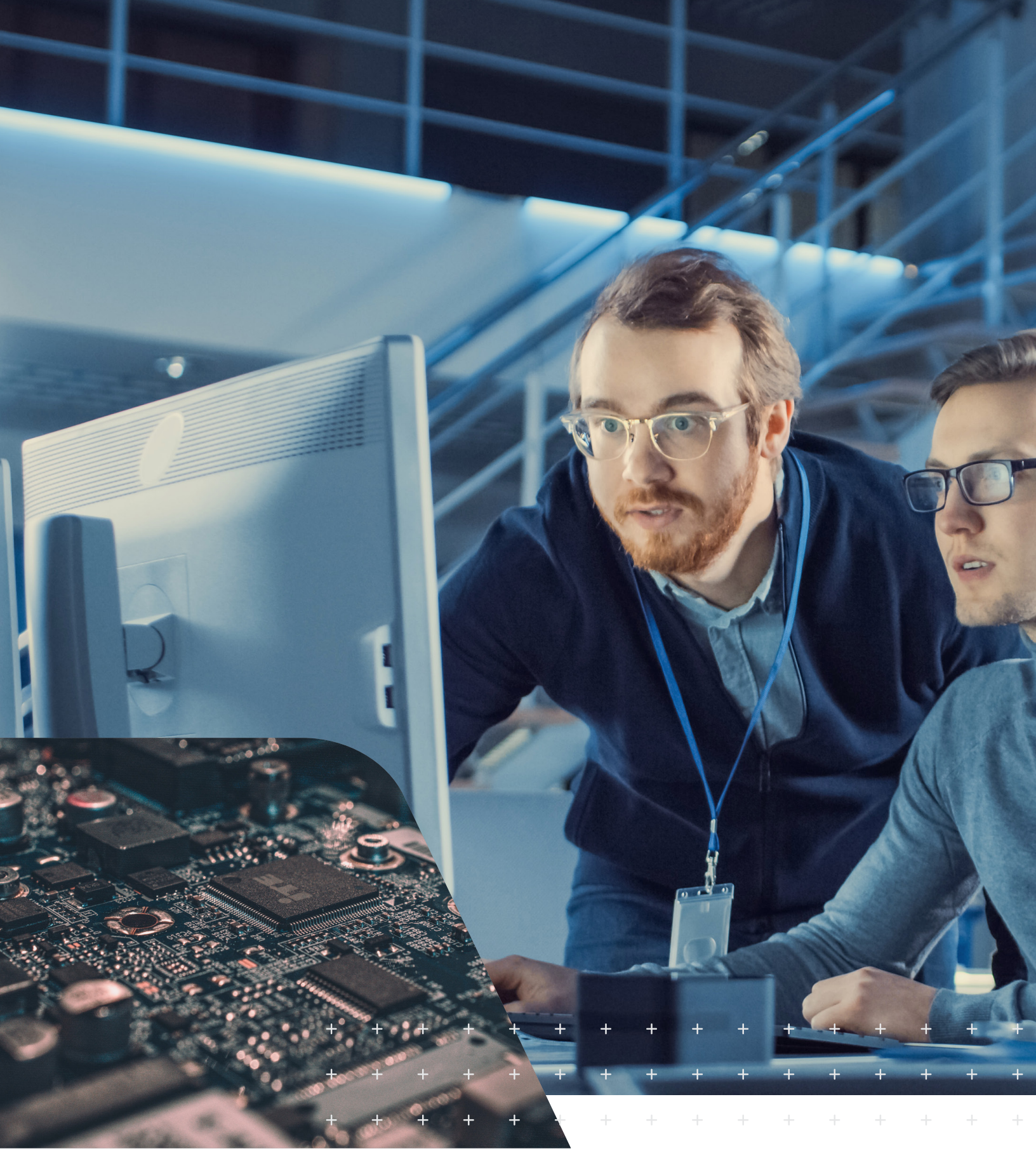


Cyber Solicitation

Over the past couple of years, cyber-crime has become more prevalent on a global scale. There are many tactics businesses can take to prevent ransomware.

Preventing a Ransomware Incident

+ Does the network require two-factor authentication for all remote access?
+ Is there a secure data backup solution in the event of a ransomware attack?
+ Are the right email spam filters in place?
+ Is there a behavior-based antivirus software to help recognize malware?

What is Business Email Compromise?

Business email compromise (BEC) or "phishing" is a cyber-crime used to gain access to company email. This allows criminals to steal sensitive data and money by impersonating a coworker, manager or other trusted business partner through fraudulent wire transfer requests, fake invoices, or diverting payrolls. BEC emails are default to detect because they usually contain no malware.

Cyber criminals obtain email credentials through social engineering.

Social engineering involves a class of attacks using manipulation to gain access to confidential information or assets. Cyber criminals use this data by deploying malware or holding information in a system hostage.

Here's How the Threat Actors Work:

Phishing pages: Cyber criminals send a link to a fake login page for a false Office 365 or Google page requesting your credentials that looks identical to the real O365 or Google login page.

+ O365 example: An email is received stating Jane Doe shared a file with you. When the link is clicked, it opens a fake O365 login page. When credentials are entered, information is compromised.
+ Google example: An email is received that appears to be from Google warning compromised account and passwords need to be changed. The website will provide a link to a fake Google login page where credentials are entered.

Another common way to steal credentials is via "Keyloggers"," which is a malicious software that secretly captures keyboard strokes.

A phishing email may contain an innocent-looking link, but the link is clicked, a keylogger is instantly downloaded and installed. Now, all keystrokes (including passwords and information like personal bank accounts, social media logins, etc.,) are sent to threat actors, including usernames and passwords.

Email Spoofing

A common social engineering technique used by threat actors to gain access to confidential information is email spoofing, which occurs when the email appears to be sent by a legitimate sender but is actually sent by a threat actor. In this instance, cyber criminal has either directly gained access to the email account or they have "spoofed" the email with a forged sender address that looks legitimate.

For example, an accounts payable department receives an email from the CEO, who is traveling abroad, asking for $100,000 to be immediately wired to a new bank account of a trusted business partner. The employee complies. The company later discover the new bank account belongs to a criminal who spoofed the CEO's email account to divert the money. The bank is called immediately but the money has already been transferred.

4 Key Cyber Smart Technologies:

+ Two-Factor Authentication
+ Online Backups
+ Spam Filtering & Email Configuration
+ Next Generation Anti-Virus: Behavior-based Protection

Protect Businesses and Employees from Ransomware

+ (2FA) – A dual authentication technique that includes something known or had (e.g. text message or a confirmation within a smartphone app).
+ Phishing Training – Online or in-person training and simulation.
+ Spam Filtering & Email Configuration

How to Prevent BEC Attacks:

THREE EASY STEPS THAT CAN SAVE A BUSINESS:

1. **Enable Dual-Factor Authentication (2FA) on Email**

   Dual-factor (2FA) or multifactor authentication is quickly becoming a "must have" for businesses instead of a nice to have. Enabling this layer of protection may be the easiest and, most effective method an organization can use to reduce the risk of transfer fraud.

   Some service providers offer multifactor authentication at no extra cost. 2FA adds another layer of protection to password-protected remote access to a network. The vast majority of successful hacking/ransomware attacks are a result of the threat actor gaining access to a company's network using compromised login credentials. By using 2FA this can be prevented as even if the hacker has stolen an employee's login credentials, the dual-factor authentication prevents them from accessing your network, since they would also need to have the employee's mobile phone which is being used as the second authentication factor.

   2FA should also be used on all remote access to your email servers (Office365 and GSuite have free solutions). Threat actors use compromised email accounts to launch ransomware or social engineering attacks against your contacts.

   Information on how to enable 2FA on O365 and GSuite can be found below:

   + Microsoft Office 2FA
   + Support Google 2FA Support

2. **Employee Training to Recognize Phishing**

   Teaching employees to stay alert and recognize dangerous phishing emails helps block BEC attacks. Employees should never click on an attachment or link an email from an unverified sender. Offering training to employees can help protect against a cyber-attack.

   Conducting a live phishing simulation is another great way to train employees to recognize dangerous BEC/phishing emails. Phishing simulations help identify those employees who are susceptible to phishing attacks and require additional training.

3. **Spam Filtering & Email Configuration**

   Email servers can automatically filter out certain suspicious phishing emails. Activating filters is an easy way to prevent dangerous phishing emails from landing in employees' mailboxes. Companies can enable email filtering to quarantine suspicious emails and scan documents and files before they are opened.

   In Office365, administrators can develop alert policies to detect specific behavior.

Creating an Inbox Rule:

+ Log into protection.office.com and navigate to Security and Compliance center > Alerts > Manage Advanced Alerts.
+ Create a new alert for "New-InboxRule Create Inbox rule from" and select Outlook or Outlook Web App or both. It is also recommended to create a rule for "Set-InboxRule." Details can be found here.

Online Backups

Backups can be another effective strategy to reduce ransomware damages and business disruption. If infected with a ransomware virus, businesses will not need to pay the ransom to get back up and running. Instead, they will be able to wipe out the virus, clean devices and network, and reinstall everything from a recent, clean backup.

Recently threat actors have been effectively attacking backups that are not properly protected. All backup solutions that are connected to the network are highly vulnerable to cyber criminals.

Just because a company is using the cloud does not mean the cloud backups are properly isolated or segregated. Be sure to properly configure any cloud backups to ensure they are isolated from the operating environment.

Create internal procedures for maintaining on-site and off-site backups of critical systems and data through periodically testing backups by restoring the systems from backup to ensure they work when needed.

Next Generation Anti-Virus or Behavior-based Protection

Behavior-based security software scans devices for unusual behavior and can decide if the deviation is a threat. These solutions are typically connected to the cloud, so their ability to detect new malware variants is updated in real time.

Anti-virus software on user devices, networks and servers is used to find or block suspicious activity, which traditionally relies on a vast database of virus signatures to help the software identify malicious applications on computers. Modern malware can easily be modified to not match existing signatures.

Popular next generation anti-virus end point protection tools include Microsoft Defender Advanced Threat Protection, BitDefender Gravity Elite, CarbonBlack and CrowdStrike's Falcon/Protect. Behavior based endpoint protection is an efficient way to protect against new threats and prevents ransomware from spreading throughout your the network.

Cyber Glossary

Endpoint application isolation and containment technology is a form of zero-trust endpoint security. Instead of detecting or reacting to threats, it enforces controls that block and restrain harmful actions to prevent compromise. Application containment is used to block harmful file and memory actions to other apps and the endpoint. Application isolation is used to prevent other endpoint processes from altering or stealing from an isolated app or resources.

Common Providers: Authentic8 Silo; BitDefender™ Browser Isolation; CylancePROTECT; Menlo Security Isolation Platform; Symantec Web Security Service

Endpoint Detection and Response (EDR), also known as endpoint threat detection and response, centrally collects and analyzes comprehensive endpoint data across your the entire organization to provide a full picture of potential threats.

Common Providers: Carbon Black Cloud; Crowdstrike Falcon Insight; SentinelOne; Windows Defender Endpoint

Multi-Factor Authentication (MFA) is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge (e.g., password), possession (e.g., phone or key), and inherence (e.g., FaceID or hand print). MFA for remote email access can be enabled through most email providers.

Common MFA providers for remote network access: Okta; Duo; LastPass; OneLogin; and Auth0

Next-Generation Anti-Virus (NGAV) is software that uses predictive analytics driven by machine learning and artificial intelligence and combines with threat intelligence to detect and prevent malware and file less non-malware attacks, identify malicious behavior, and respond to new and emerging threats that previously went undetected. For purposes of completing this application, NGAV refers to anti-virus protection that focuses on detecting and preventing malware on each individual endpoint. If an organization has a NGAV solution AND is centrally monitoring and analyzing all endpoint activity, please indicate that the company has NGAV & EDR on the application.

Common Providers: BitDefender™; Carbon Black; CrowdStrike Falcon Prevent; SentinelOne; Sophos; Symantec

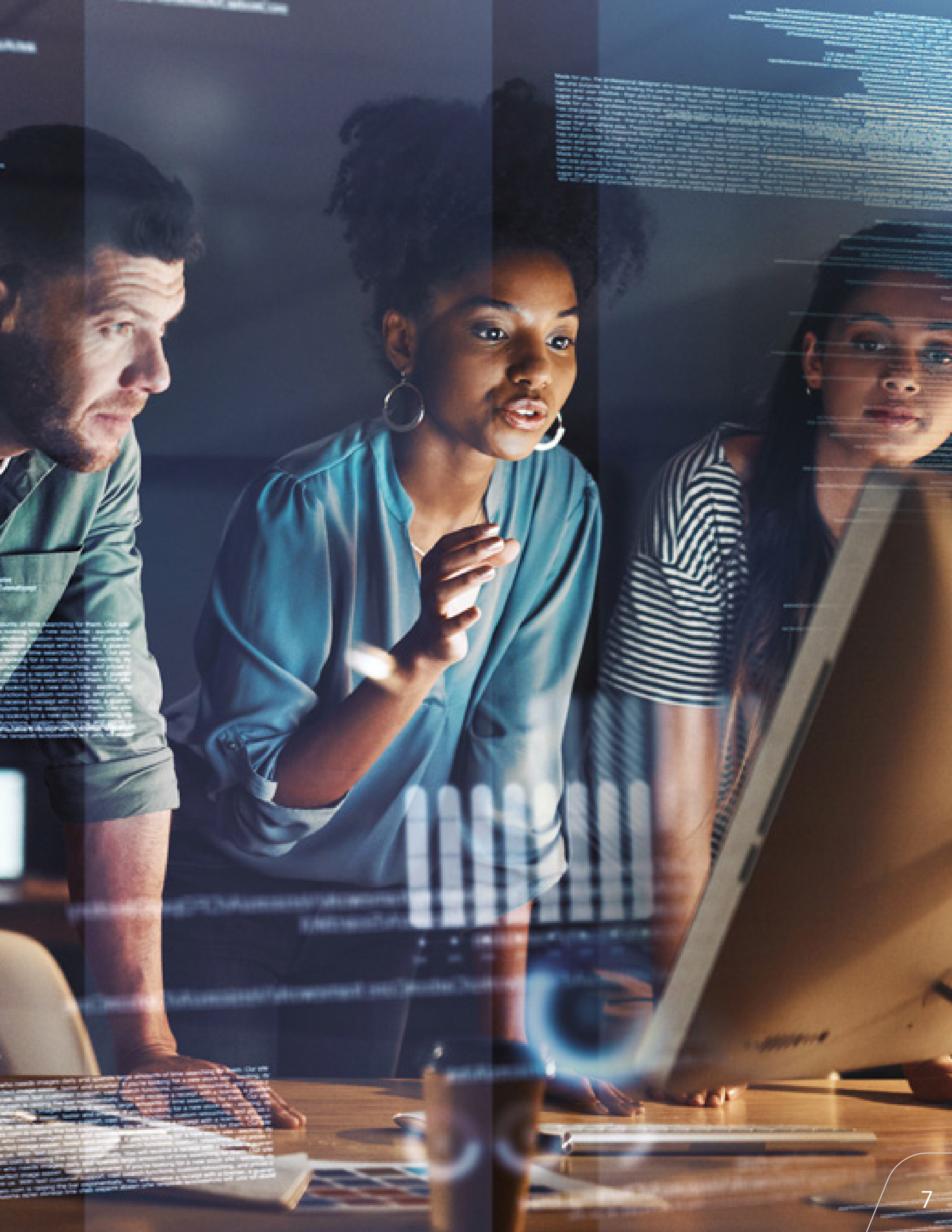
Privileged Account Management Software (PAM) is software that allows security for privileged credentials in a centralized, secure vault (i.e., a password safe). To qualify as PAM, a product must allow administrators to create privileged access accounts; over a secure vault to store privileged credentials; and monitor and log user actions while using privileged accounts.

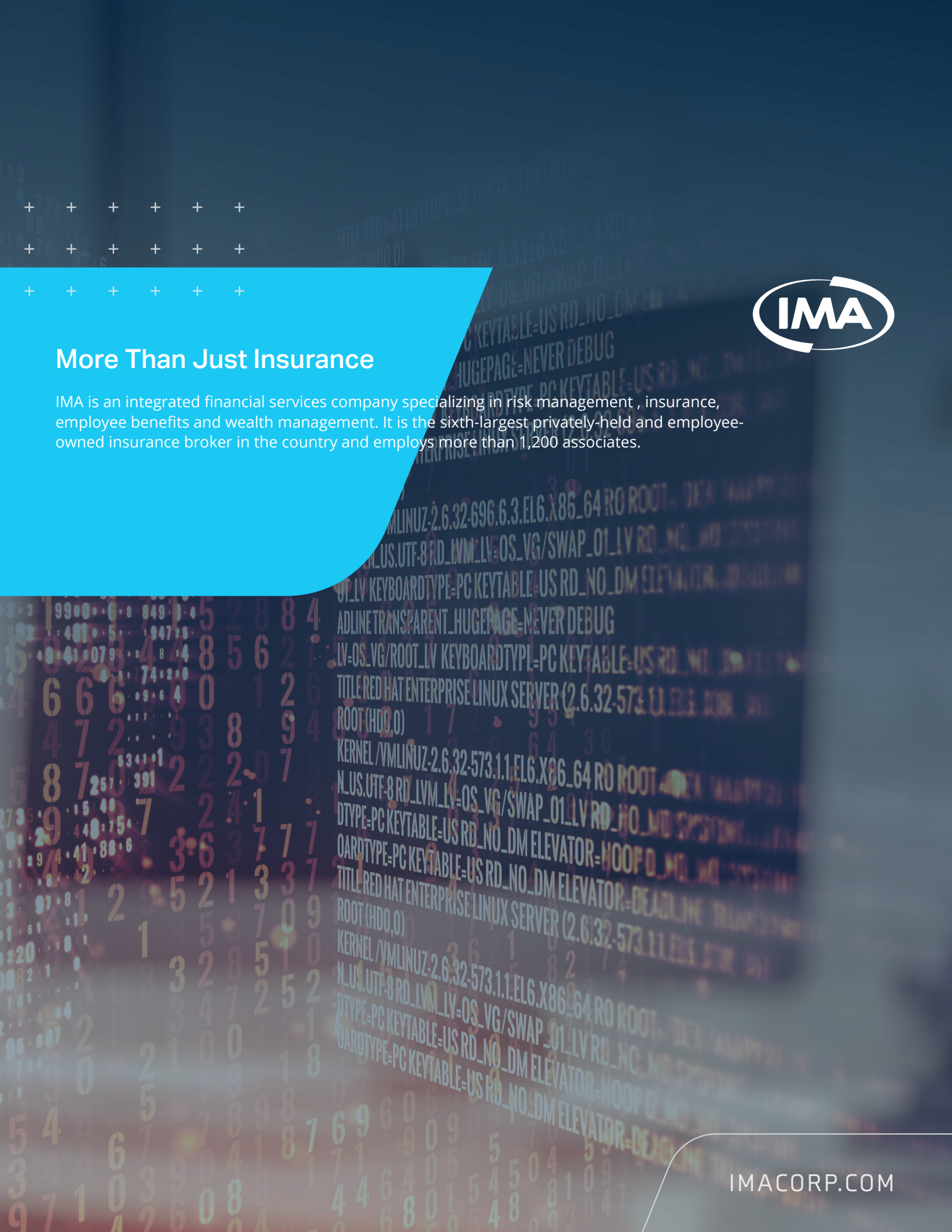
Common Providers: CyberArk and BeyondTrust

Remote Desktop Protocol (RDP) connections is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. The Microsoft RDP provides remote display and input capabilities over network connections for Windows-based applications running on a server.

Security Information and Event Management system (SIEM) is a subsection within the field of computer security, wherein software products and services combine security information management and security event management. SIEM provides real-time analysis of security alerts generated by applications and network hardware.

Sender Policy Framework (SPF) is an email authentication technique used to prevent spammers from sending messages on behalf of the domain. With SPF, organizations can publish authorized mail servers.





More Than Just Insurance

IMA is an integrated financial services company specializing in risk management , insurance, employee benefits and wealth management. It is the sixth-largest privately-held and employee-owned insurance broker in the country and employs more than 1,200 associates.

IMACORP.COM