Providing Advanced Threat Protection to Small and Midsize Businesses

Advanced Threat Protection (ATP), powered by Teqworks, represents a quantum shift in the focus on network security. While some portions of ATP represent incremental changes to solutions we already provide, we are addressing significant changes to how security events happen and threaten the networks we promise to secure. The need to provide solutions – software, hardware, skills, and processes – that best protect you from these evolving threats has never been more critical.

This article is intended for business owners, office managers, partners, directors, assistants, and anyone else who is interested in protecting their company from technology security threats.

The Threat Landscape

Next Generation threats to business technology are increasing in frequency and sophistication.

According to a Gartner report in 2020, by 2025 at least 75% of IT organizations will face one or more Next Generation attacks. This predicts that virtually every IT environment is going to experience a threat – an attack, a breach, a security event – that is not detectable or preventable by conventional methods, such as antivirus, spam filters, and firewalls.

CrowdStrike[1], a leading global security firm, reported that 68% of detections in the last 90 days were not malware based, meaning there is no file or program on a computer for antivirus to detect, no malicious attachment in an email for spam filters to remove, no hacker traffic for a firewall to block.

The technology threat landscape is changing, drastically. Supply-chain attacks, ransomware, and social engineering have grown in frequency to threaten viability of businesses and organizations of any size. Technology professionals have learned that conventional approaches and solutions that have worked for decades are not effective against these emerging risks and actors.

The stories are scary and true:

- A small business owner is phished, and tricked into allowing attacker's access to bank accounts.
- An office manager purchases hundreds of dollars in Amazon gift cards on behalf of someone spoofing the organization owner.
- A project manager's Microsoft 365 mailbox is compromised and then used to spam customers.
- A wealth management firm loses thousands of dollars in a fraudulent wire transfer.
- A manufacturing company is shut down for 6 weeks because computers and servers were encrypted by ransomware.

Cyber-attacks are not just big game hunting. Small and midsized companies are becoming favorite targets

- In 2020, 43% of reported cyber events were from small businesses, representing a 424% increase over 2019.[2]

[1] *CrowdStrike Falcon OverWatchTM annual report, 2021*
[2] *Verizon, Data Breach Investigations Report*

- Regardless of the size, victims can expect costs to surpass $200,000 in legal fees, recovery efforts, damages, forensic analysis, and corrective actions.[3]
- Accenture reports that only 14% of small and midsize businesses are prepared to defend themselves, through technology, process, or finances.[4]
- Most small businesses – 60%, reportedly – will not survive the year after experiencing a data breach, usually closing doors within 6 months.[5]

It is not a matter of if, but when a security event will happen. And the question is whether enough can be done to protect and recover before a Next Generation threat – one that cannot be predicted or prevented by conventional defense – arrives.

Understanding Conventional Threats

To understand what is meant by a Next Generation threat, we need to first understand how Next Generation threats differ from Conventional Threats.

Conventional threats are those that we're all familiar with: Viruses, spam, phishing, malware, adware, spyware, trojans, and other unauthorized attempts to reach your secure network and assets; all of these pose risk to your business. With general adoption and maintenance of firewalls, antivirus, antimalware, spam filters, virtual private network (VPN) connections, and encryption, these types of attacks are largely held at bey.

These conventional defense approaches work because the threats are known and understood. They rely on the understanding of how each attack works and where they come from, learning the signature of each, and updating the protection tool with rules to detect and remove the threat.

For example:

- **Firewalls** are programmed to watch traffic between the internet and your internal network and computers, and allow or deny different types of traffic (or "protocols") based on rules. For example, if your internal network has an email server, the firewall is programmed to allow email traffic (e.g. TCP port 25) to flow freely between the email server and other email servers on the internet. However, internet traffic that uses a protocol that is ~~>~~ unusual or is unknown is blocked automatically.
- **Firewalls** also scan what is **inside the traffic** (known as packets). This stateful packet inspection is used to determine whether known malicious code is hidden in traffic that comes through allowed ports.
- **Antivirus and antimalware** programs are updated regularly to import the latest set of rules to detect all known viruses, spyware, and other malicious software. Antivirus then uses these definitions to clean and block future instances of the virus. A computer that has not been updated with the latest virus definitions is susceptible to infection by new viruses.

[3] *Hiscox Cyber Readiness Report*
[4] *Ponemon Institute, State of Cybersecurity in Small & Medium Size Businesses*
[5] *US National Cyber Security Alliance*

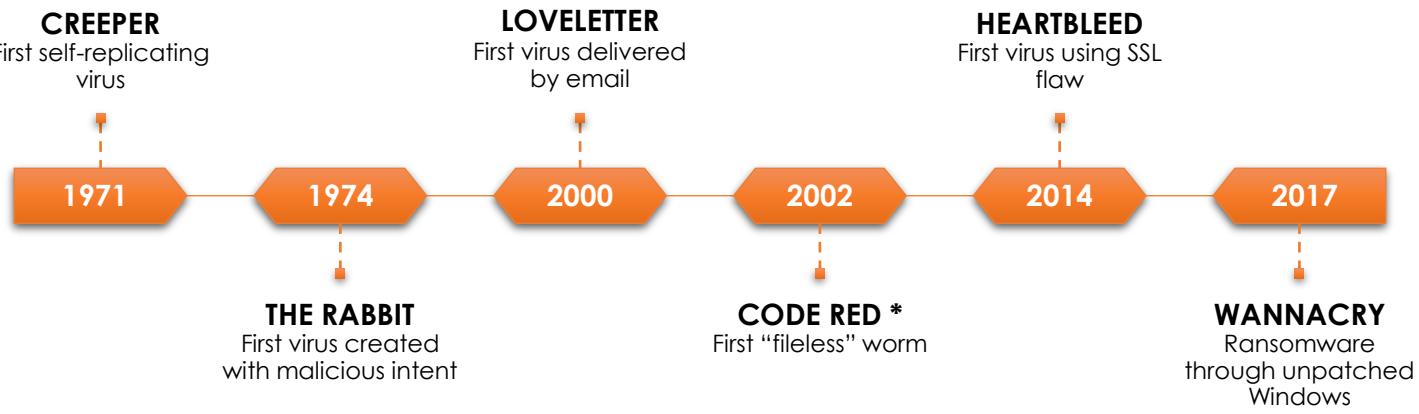
- **Spam filters** work similarly to antivirus and antimalware applications to identify known types of junk email.

Every day, at least 560,000 instances of new viruses, malware, or spam are created by malicious actors and released into the internet wild. Firewall rules, spam filters, and antivirus definitions are updated to protect from the new malicious code. In the lifecycle of a conventional threat, new malicious code is released, security professionals become aware of it, the threat is decoded, and the security software is updated to detect and stop it in the future.

The dangerous time for a conventional threat is the early stage before detection instructions are known, security solutions have not yet been updated with the keys to detect and prevent. Without the instructions, antivirus/spam filters/firewalls do not have enough information to identify the risk.

A Brief History of Conventional Threats

Conventional viruses have been around for at least 50 years. The first noted in 1971 when a self-replicating file was first proven possible.



The first virus created with malicious intent was identified in 1974, and incremental "improvements" were made over time.

In 2002, CODE RED was the first documented instance of a virus that stayed in memory, and did not write a file to disk.

In May 2017, the business world saw the emergence of WannaCry, a ransomware attack delivered through phishing emails. WannaCry targeted Microsoft Windows computers that were missing a security patch (which had been known and available for 91 days before the attack), and a $300 Bitcoin ransom was demanded in return for a decryption key.

While many paid the ransom, few got their data back. It was from this experience, we were reinforced to

1) keep software updated with security patches,
2) never count on paying the ransom,
3) plan on having a way back to recovery, and
4) ransomware was real and here to stay.

Next Generation Threats

Next Generation threats, by comparison, do not use conventional methods to reach your electronic assets. They can disguise themselves as trusted traffic. They can use legitimate programs – like Outlook or Adobe Acrobat – to run rules to manipulate data on the computer or server. Next Generation threats can use your own employees to do the work for them.

None of these are detectable by conventional antivirus or spam filters.

- So, what if the threat is unknown, or unknowable?
- What if there is no malicious software, or programmable signature of a file for antivirus to detect?
- What if the malicious activity is simply malicious behavior of a trusted program, file, or protocol?
- What if malicious code is delivered through compromised software updates?
- What if a major software application – like Microsoft Exchange, Outlook, or Adobe Reader – were to be used to spy on and compromise an entire business network of servers, files, and databases?

One such Next Generation Threat is one that's been around for a long time: The Zero-day Vulnerability.

Sometimes, trusted software has security holes. There are errors in software code, and these security holes can be used right through the software to deliver malicious attacks. When a hole is used by a malicious actor or is discovered to present a risk, it is referred to as a "zero-day vulnerability." This means it is not in the future, but is a vulnerability that exists today and malicious actors are already working to utilize it to gain access. Zero-day vulnerabilities are closed by the software manufacturer engineers providing patches or hotfixes.

Again, antivirus won't find these – the software with the security hole is trusted. There is no malware to detect.

Zero-day vulnerabilities introduce what we refer to as the **Supply-Chain attack**.

The Supply-Chain Attack is one that is delivered through compromised code in trusted software, usually through a software update. A malicious coder inserts program instructions in the software update, allowing them to use the software right under our noses.

January 2021, a set of malware code – referred to as Sunburst and Sunspot – was reported to be found in trusted IT management software, called SolarWinds. This malware was inserted into the development process for the popular software sometime in 2019. This malicious code was used to monitor and encrypt computers that had the SolarWinds Orion software installed, unknown to hundreds of IT departments who used the software.

March 2021, four zero-day vulnerabilities in Microsoft Exchange Server were being actively exploited by state-sponsored threat actors to open backdoors, harvest information, and deliver malware. Microsoft reported that they became aware of the exploits – referred to as ProxyLogon and Hafnium – in early January 2021, and issued patches to fix the vulnerability in March 2021. It is still unclear as to the extent and depth of the exploit, but the threat was demonstrated to allow remote execution of programs and commands on servers, and could be used to collect information and inflict ransomware on internal networks. Cloud-based versions of Microsoft Exchange (Microsoft 365) were not impacted by this vulnerability.

July 2021, another infrastructure software application – Kaseya – was compromised in a similar fashion as SolarWinds. In this case, when the monitoring software was updated overnight, the latest version had the malicious code (REvil) embedded. Endpoint devices were encrypted within two hours of update, locking networks worldwide. When IT departments arrived at their desks the next morning, the damage was done and their only options were to pay a ransom or restore servers and computers from backup.

In all three cases, conventional protection could never detect or stop these threats. There was no delivery of malware to a computer. There was no spam or phishing. There was no link to click, and no attachment to open. They were delivered through trusted software, critical to everyday business operations.

If these threats were not detectable – were not *knowable* – could they be stopped? Are they inevitable?

In the case of SolarWinds and Kaseya, the malware was introduced through the IT department – those specifically responsible for watching for the safety of the network.

The Case for Targets Prediction and Behaviors Detection

There are two common characteristics of knowable and unknowable attacks:

- the targets,
- and the behaviors resulting from the attack.

Targets are going to be weak points in a network, including cloud apps and data, network devices (firewalls, wireless access, network switches), endpoints, and users.

Behaviors – rather than known signatures or the malware to be detected – are what the malicious actor does and affects on the target. From lateral movement on a network (or, moving from computer to computer), to changing rules and how Microsoft Outlook works, to modifying files and folders, these are abnormal behaviors that indicate something is not right.

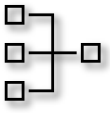
Conventional prevention cannot detect behaviors, and targets include virtually anything that can be influenced. Non-conventional solutions are needed to address unconventional threats. With the application of artificial intelligence, and humans using threat-hunting skills and expertise, the introduction of MDR (Managed Detection and Response), with better protection and real-time monitoring and incident response has become necessary.

Target Prediction

In today's business technology world, there are three primary target planes which must be included in any approach to protect the enterprise from compromise or breach:

Cloud

Apps, data, and connectivity provided through cloud-based solutions, like email and Microsoft 365



Network:

Firewalls, routers, network switches, wireless access, remote access, VPNs

Endpoint:

Servers, computers, laptops, printers, storage, tablets, phones, and – yes – users

Behavior Detection

Behaviors of how solutions and devices operate at each level have a normal, expected range.

- A certain number and type of files are accessed on a day-to-day basis. Changes to that number and types of files ~~in~~ is abnormal.
- An application used to open a specific type of file doesn't normally start sending large amounts of data to the internet.
- Users log in to their accounts from expected locations. If your office is in Aurora, they don't log in from Aurora at noon, and then appear to log in again from Hawaii (or Belarus) at 2:00PM that same day.
- Wireless network settings – like names and passkeys – are generally static. The don't change regularly.
- Files usually remain in one place. They don't normally copy and propagate from computer to computer (lateral movement).
- It is unusual to see a computer change file permissions on other computers.
- Outlook rules to automatically delete messages from a coworker don't make sense.
- It is uncommon for switches to suddenly redirect packets to an internet destination.

None of these events are preventable by conventional protection. Only observance of the behavior triggers indication that something is wrong.

Solving Next Generation Threats with Advanced Threat Protection

So, we've established that many of today's threats cannot be handled by conventional defense. We introduced how to detect and protect from next generation threats with Managed Detection and Response (MDR), target predicting, and behavior monitoring.

Teqworks recognizes that the primary objective of security should be to prevent threats from occurring in the first place, keeping the business running, and providing a way back in the worst-case scenario.

Teqworks is changing the game of protecting the small and medium sized business with the introduction of Advanced Threat Protection. With ATP, Teqworks now offers 24x7 monitoring, detection, response, **and** mitigation to protect your organization's cloud apps and data, network, and endpoints.

The Principles Behind Advanced Threat Protection

Teqworks espouses a robust 5-stage approach to Advanced Threat Protection:

1. **PREDICT**: We use artificial intelligence and human-based threat hunting to identify, watch, and mitigate expected weak points in the network. A strong point today, could be a weak point tomorrow, and using deep knowledge and automation to predict these points is crucial.
2. **EDUCATE**: No organization can operate without its talent – its people. However, those people present unique risks to an IT environment. No employee today can claim they are not IT savvy, and must take on the responsibility to help protect the organization from social engineering and threats that get through conventional barriers. We assess user susceptibility, educate users on current threats, train them on how to respond, and remove ineffective behaviors.

   We want to arm users with knowledge and understanding of common risks, behaviors to appropriately respond, and confidence to continue work without interrupting productivity.
3. **PREVENT**: Upgrading antivirus to EDR software (Endpoint threat Detection & Response), plus implementing security policies and best practices are critical. There is still a place for many conventional solutions, but improvements are needed to prevent next generation threats.
4. **DETECT & RESPOND**: We introduce our biggest change to Teqworks security, by offering Managed Detection & Response. MDR utilizes a 24x7 Security Operation Center (SOC) that monitors all events and behaviors on cloud, network, and endpoints. The SOC evaluates the activity (automated and human) in real time to assess abnormalities, and is able to identify, notify, and mitigate threats within minutes.
5. **RECOVER**: The final safety net is the ability to recover. We can never assume that nothing can get through. While MDR is lightyears beyond conventional protection, we never want it to be the last line of defense.

Teqworks offers full backup & disaster recovery solutions for cloud, network, servers, and user devices. Always offer a path back in the worst-case scenario.

Solution: Advanced Threat Protection

Advanced Threat Protection, powered by Teqworks, is a subscription-based complete solution that enhances our standard Managed IT Service. ATP is comprised of three capabilities.

- **EDR** (Endpoint threat Detection & Response): This is the solution to provide endpoint protection software, artificial intelligence, target prediction, and behavior detection. EDR replaces conventional antivirus on all supported endpoints to deliver superior levels of performance, resource management, effectiveness in threat prevention, behavioral recognition, and reporting. Its AI, deep learning, and false positive rate are superior to conventional antivirus and antimalware.
- **SIEM** (Security Information and Event Management): This is a centralized event collection system that is used to document and evaluate all events and behaviors on a network, perform root cause analysis, and collect data from network traffic and endpoint activity (EDR). This is the data repository that all the AI and monitoring uses to detect the bad things. Teqworks provides an on-premises appliance to perform this collection and replication to our MDR service for analysis and detection.
- **MDR** (Managed Detection & Response) is 24x7 monitoring, assessment, and mitigation. Through MDR, Teqworks provides Security Operations Center (SOC) services to deliver the most complete security solution to small and midsize organizations.

Does Your Organization Need Next Generation Threat Protection?

Contact Teqworks today to schedule an assessment and discussion to help you better understand the technology risks your organization faces today, and how Advanced Threat Protection can mean the difference between business continuity and another nightmare ransomware story.

Who is Teqworks?

Teqworks is a Managed IT Services and Security company in St. Charles, Illinois, serving small and midsize organizations throughout the Chicagoland area in their search for technology solutions and support. Unlike break-fix technology mechanics who fix problems only after they break, Teqworks aims to avoid problems, keep your business running, and help plan for changes so you can run your business with continuity. And we've been doing it this way since 2002 when we opened our doors. Teqworks is ranked among the very top Managed IT service providers in the world each year since 2013.

Address: 3805 E. Main Street, Ste H, St. Charles, IL **Phone**: 630.482.2227

Email: ATP@teqworks.com **Web**: https://teq.works or https://www.teqworks.com

Twitter: https://twitter.com/teqworks (@teqworks) **LinkedIn**: https://www.linkedin.com/company/teqworks