White paper

VECTRA®

Surviving the ransomware pandemic

VECTRA®

TABLE OF CONTENTS

Introduction

A strong file-recovery plan, a bit of deception, and a keen eye for detecting attacker behaviors can keep ransomware from holding an organization hostage

Ransomware attacks have sidelined organizations in a no-win situation. Victims must pay up to get their data back or face the consequences of losing their operational livelihood.

In the not so distant past, criminals made easy money targeting consumers with ransomware from CryptoLocker, Locky and TeslaCrypt. But in search of higher profits, attackers have quickly spread from consumers to enterprise organizations.

The con is the classic hostage scenario where thieves demand a ransom for something that's held valuable. A nasty screen pops up saying that important files are encrypted and the only option is to meet the attacker demands and get the key to decrypt them.

According to the FBI Internet Crime Complaint Center, ransomware victims paid more than $24 million to criminals in 2015, and a growing portion of the payers were enterprises. Criminals are trolling for bigger payouts by targeting enterprise file shares, code repositories and databases.

No group is safe from the attacks that can come through spam and drive-by downloads – or more dangerously, from network-wide attacks. The list of victims includes police departments, hospitals and banks. Even Mac users that previously seemed immune to malware can fall prey to ransomware.

The spike in attacks is not difficult to understand. It's a simple risk-and-reward equation where the reward for stealing someone's belongings far outweighs the risk. For criminals, ransomware weighs in as a fast and easy attack with a bigger payout than stealing credit cards or personally identifiable information (PII), both of which have a declining value as time passes after their theft.

Cyber crooks don't worry about whether they have stolen data that is valuable to someone else. They just need to encrypt and hold for ransom the data that is valuable to an organization. Attackers may even raise the ransom if it is not paid by the deadline.

Eliminating the need to find an eager buyer, ransomware attacks are simple, direct criminal threats with a fast close. There's no middleman needed to validate the data, provide laundering services or package the data.

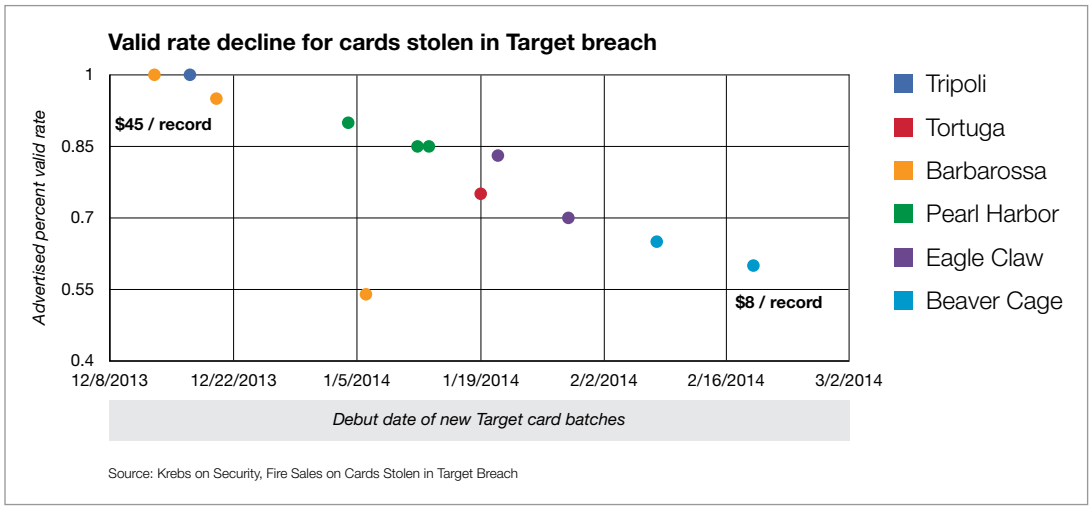
The simplicity of the threat makes ransomware extremely popular with criminals. Add in Bitcoin, an anonymous, hard-to-trace currency, and it's easy to see why cybercriminals like ransomware's clean, no-fuss business model.

The appeal of ransomware isn't expected to dim anytime soon, but organizations can prevent their valuable data from being taken hostage from these modern-day pirates. With the proper strategy and plans in place, organizations can completely recover from a ransomware attack.

Spoiling the scam for these criminals requires sending them down the wrong path, implementing a solid backup and recovery plan, and real-time threat detection so IT security teams can respond to the attack before damage is done.

Mitigating ransomware damage

Preventing an attack requires understanding the attack plan. Unlike older consumer ransomware that focused on a single machine, enterprise ransomware seeks to expand across the network. Ransomware attackers seek out network file shares where large amounts of enterprise data are centrally stored.



The declining value of stolen data

The danger for organizations starts when the ransomware encrypts shared files that are stored on file shares and file servers. When cybercriminals target these key assets, organizations are left with few options.

However, the covert attack isn't completely invisible if security teams know what to look for and where to look. Ransomware follows a series of identifiable network behaviors that send clear signals, which can be tracked and stopped. If an organization recognizes those behaviors early in the attack, it can prevent ransomware from causing damage.

The signs of ransomware are pretty universal, but they happen quickly once a host is infected. Ransomware on the infected host contacts the command-and-control (C&C) server, encrypts local files on the machine, and begins searching for other files on the network.

Once discovered, the attacking host begins to encrypt files on servers, sometimes renaming the encrypted file, and leaving ransom notes in the affected directories that explain who and how to pay.

Defining a backup and recovery plan

Organizations can mitigate the impact of a ransomware attack by having a solid backup and recovery plan. Strong backup and recovery strategies can avoid the worst ransomware attacks, but the immediate damage will disrupt business in the short-term, depending on the storage plan. Typically, organizations have three backup and recovery strategies: Hot storage, cold storage and cloud backup.

Hot storage is the most vulnerable. These systems depend on constant connectivity to file servers and frequent backups that ensure rapid restoration of files. In the case of a ransomware attack, the backups could be overwritten with the encrypted version or may be directly encrypted by the ransomware itself.

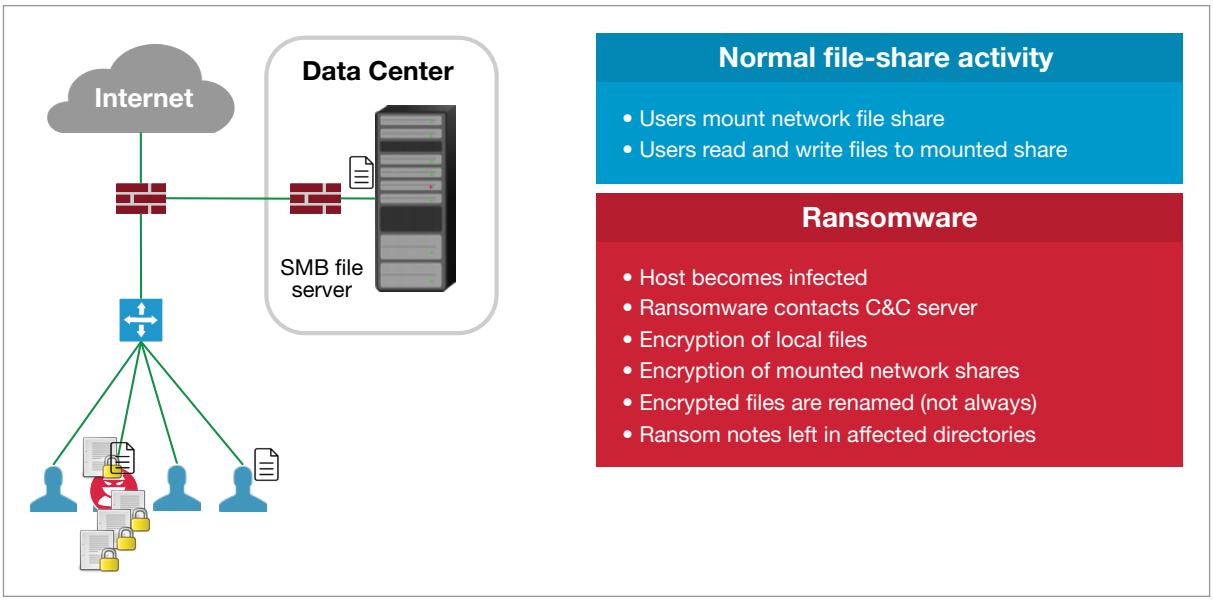
Organizations should also have cold backup storage where there is no permanent connection between the file servers and the backups. By being disconnected from the network, these backups are less vulnerable to ransomware attacks, but also may not have the most up-to-date files for recovery of encrypted data.

Cloud backup scenarios are the least vulnerable. Storage is offsite and has built-in disaster resiliency and stored versioning. Organizations can go back to a previous, non-damaged version of its files. Having a solid backup and recovery strategy can help organizations avoid having a ransom payment as their only option to recover files.

Setting decoys with canary or honeypot file-share techniques

Another low-cost technique to foil ransomware attackers involves setting up canary or honeypot file shares. IT can set up shared files that act as lures during an attack. These canary file shares are mounted at A:\ and Z:\ and can be filled with large, dummy files.

Ransomware attacks usually begin encrypting files on a mounted share at the beginning or end of the alphabet and proceeding serially through the mounted drives in alpha or reverse alphabetic order.



Anatomy of a ransomeware attack

When an IT security team sees the unusual behavior of a host reading the never-accessed canary files, it can quarantine that user to isolate the attack. Making the canary files larger simply buys the security team more time because the larger files take more time to encrypt, providing more time to stop the attack.

Security teams have a couple of options to stop a ransomware attack. The network administrator can revoke the infected host's access to the file server, block the machine from the network entirely, or temporarily disconnect the file server.

Disconnecting the file server is the most disruptive for the organization. To get back up and running, the administrator will need to re-image the client machine and recover the previous intact versions of damaged files from the backups.

Vectra stops ransomware in its tracks

Canary files and a strong file-recovery plan are good first steps to defend against a ransomware attack, but they won't prevent an organization from being taken hostage.

If IT constantly monitors the file server, it might notice ransomware's dangerous behaviors. Or, organizations could turn that responsibility over to a security solution that automates ransomware detection and prevents file damage and potential financial extortion.

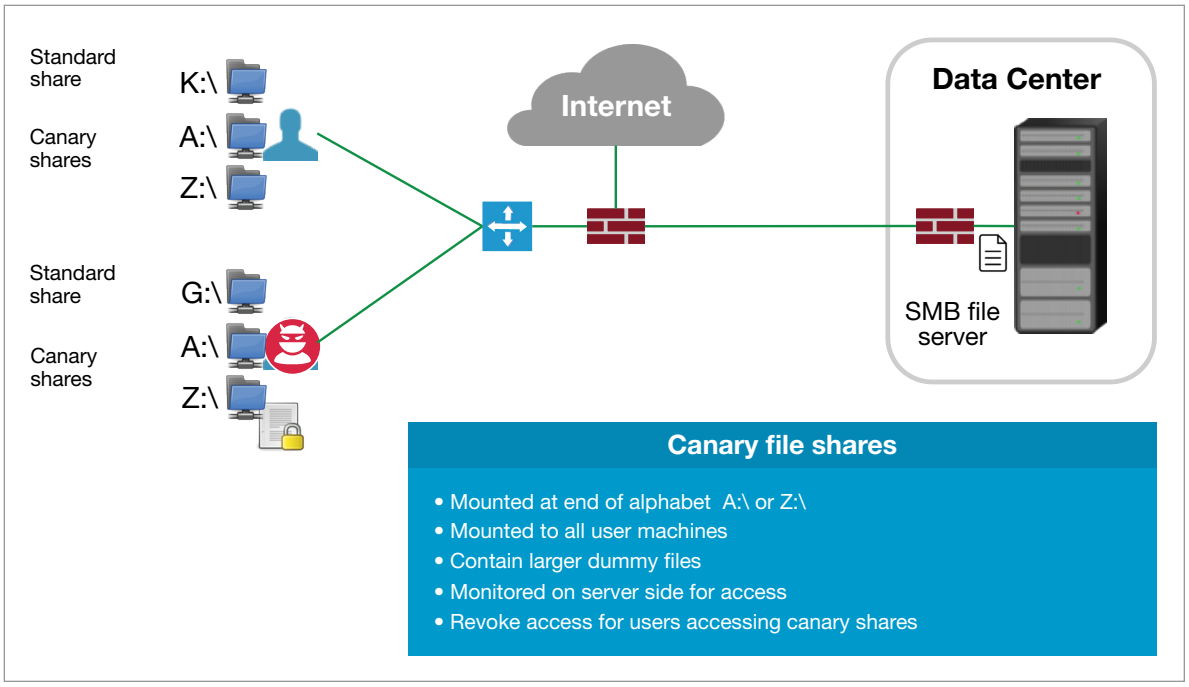
Vectra® Networks identifies and detects ransomware behavior and automatically sends alerts to IT security teams and Security Information and Event Management (SIEM) systems.

By detecting the fundamental actions of attackers, Vectra's real-time behavior-based threat analytics provides blanket coverage for widely differing families of ransomware, including HydraCrypt, CTB Locker, CryptoWall, CryptoLocker, Locky and others.

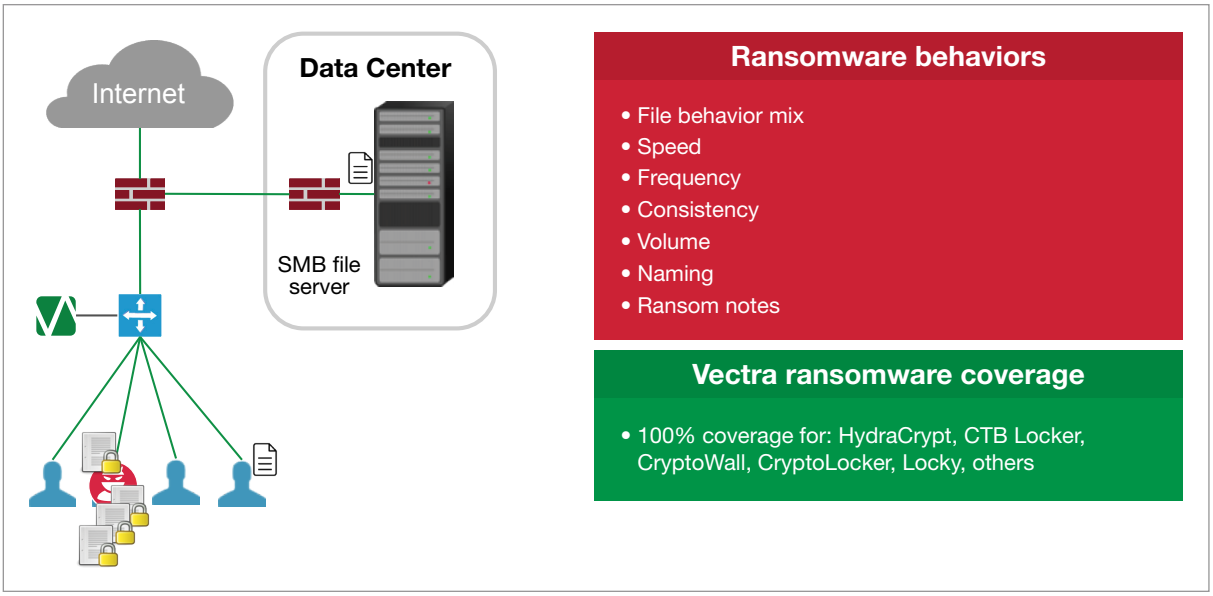
Vectra works on the premise that once underway, a ransomware attack triggers a set of consistent network behaviors. These detectable behaviors are shared across ransomware attacks, regardless of the malware variant.

Within organizations, these attacks rely on the network and don't simply remain idle on a single, specific host. Being on the network separates ransomware attacks against enterprises from the familiar consumer attacks and it makes them exceptionally dangerous.

Let's revisit how a successful attack unfolds. First, cybercriminals must find and access the file shares. They have to read files, encrypt them, write them back to the file share, and leave ransom notes. These activities, which aim to encrypt as many files as possible in the shortest amount of time, depend on speed, frequency, consistency, volume, file naming, and ransom notes.



Canary and honeypot file shares



Vectra ransomeware detection

Vectra's unique approach identifies and detects network threats by analyzing network traffic and exposing the fundamental behaviors of cyber attackers. In a ransomware attack, Vectra identifies all the behaviors that pose threats to a host.

A first activity could involve the infected host contacting the C&C server. A second could be the infected host scanning the network to find a host that responds on Port 445 – the port used by the storage message block (SMB) protocol for mounting file servers.

Vectra identifies the network scans that ransomware relies on to find these victims, even when the scans are extremely slow, and correlates them to the host with the C&C behavior.

In the next phase of attack, the ransomware begins reading, encrypting and writing to the file server. Vectra instantly recognizes this behavior and raises a high-priority alert for the security team in real time.

Time is of the essence during an attack because every extra minute allows cybercriminals to encrypt more files. Vectra enables security teams to respond quickly by sending alert notifications to designated team members' phones, letting them know exactly what is happening inside the network.

Vectra also sends notifications to SIEMs via syslog events that provide alerts to Splunk, ArcSight or QRadar to automate incident response workflows. When a ransomware event pops up, Vectra sends an event through syslog – including detection type, threat and certainty score, source and destination IP, and other information – to let security teams know what to start investigating, even to the point of knowing exactly what desktop or laptop to quarantine from the network.

In environments with network access control, Vectra can kickoff automated workflows and switch off systems from the network and cut off offending hosts before damage occurs.

Enterprises are ransomware's most lucrative targets

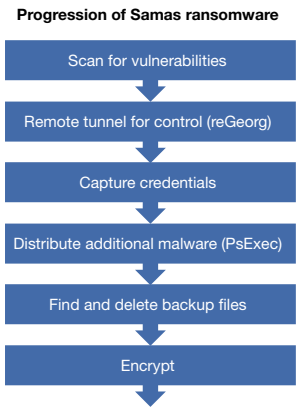
Ransomware is becoming too popular among cybercriminals for organizations to not recognize it as an imminent threat. The most significant change is how cyber thieves are leveraging the network to launch more advanced, hard-hitting attacks. Criminals have moved from attacking single laptops to casting a wider net that surrounds the network, which is similar to targeted, persistent enterprise data breaches.

Microsoft recently conducted an analysis of the Samas ransomware attack that hit North American organizations, and the path Samas took through the network showed it clearly understood standard enterprise file sharing and storing behaviors.

Once launched, Samas first scans the network for vulnerabilities. After locating a victim, it sets up remote tunneling to gain control of the network so it can quietly and persistently search for and capture user credentials and distribute ransomware.

Ransomware in the enterprise

- Attacker strategy maturating from consumer to enterprise
  - Demand much higher ransom from fewer victims
  - More patient and APT-style of attack
  - Focus on encrypting file shares in addition to end-user machines
- Samas/MSIL
  - Ransomware campaign recently analyzed by Microsoft
  - Largely focused on enterprises in North America
  - Uses tunneling and stolen passwords to pivot through the network
  - Finds and destroys file backups before encrypting files



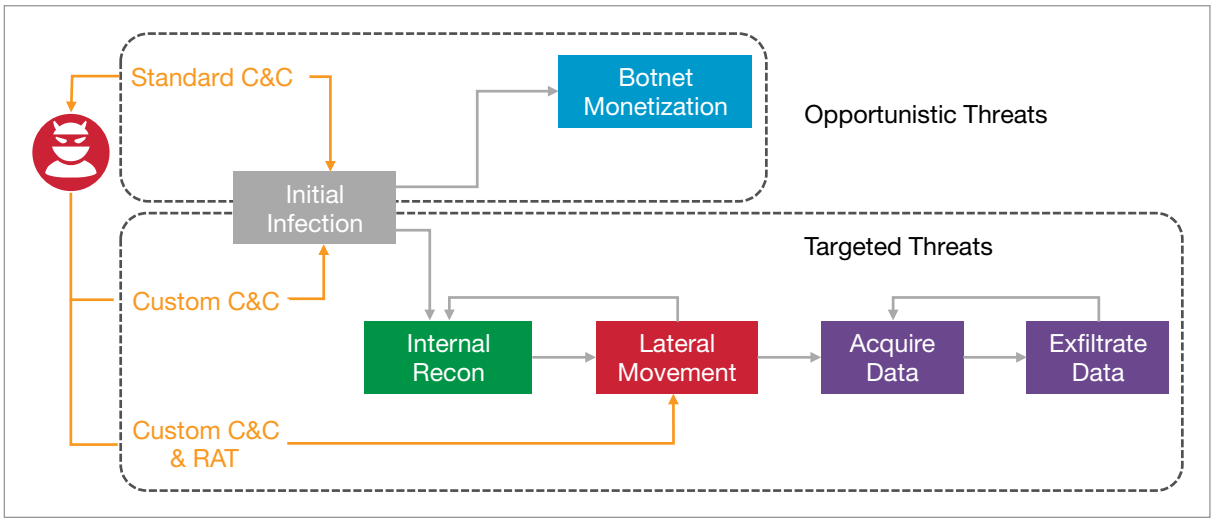
Ransomware in the enterprise

The attack doesn't stop there. Samas dangerously wends its way deeper into the network and looks for and starts deleting backup files before encryption even begins.

For security professionals, this chain of events has some good news. Samas is convincing evidence that ransomware attacks are following the same activities and the familiar kill chain that is prevalent in targeted threats.

They enter a custom or standard C&C and begin with internal reconnaissance to understand the environment. Next, they start some type of lateral movement to dig deeper into the network with elevated credentials before they identify and encrypt key assets to extort a ransom from the organization.

Vectra has multiple opportunities to detect ransomware threats. Vectra detects the attacker's C&C traffic, the malware update of ransomware onto the infected host, the internal darknet scan looking for file shares, the theft of credentials to escalate privileges, and the ransomware file encryption activity.



Detect across all phases of attack

All detections are correlated to the infected host, driving up the threat and certainty score with each attack phase detection, and raising the priority for response to the security team.

This precursor activity is identified by Vectra before the damaging phases of the ransomware attack occur. Detecting this activity prior to an organization's files becoming encrypted is what separates Vectra from other threat detection solutions.

Vectra stays in front of threats

Vectra puts organizations ahead of attackers, rather than constantly chasing and responding to the next incoming attack. This proactive approach identifies a set of network behaviors that consistently lead to ransomware attacks and is fundamentally different from identifying malware signatures on an endpoint.

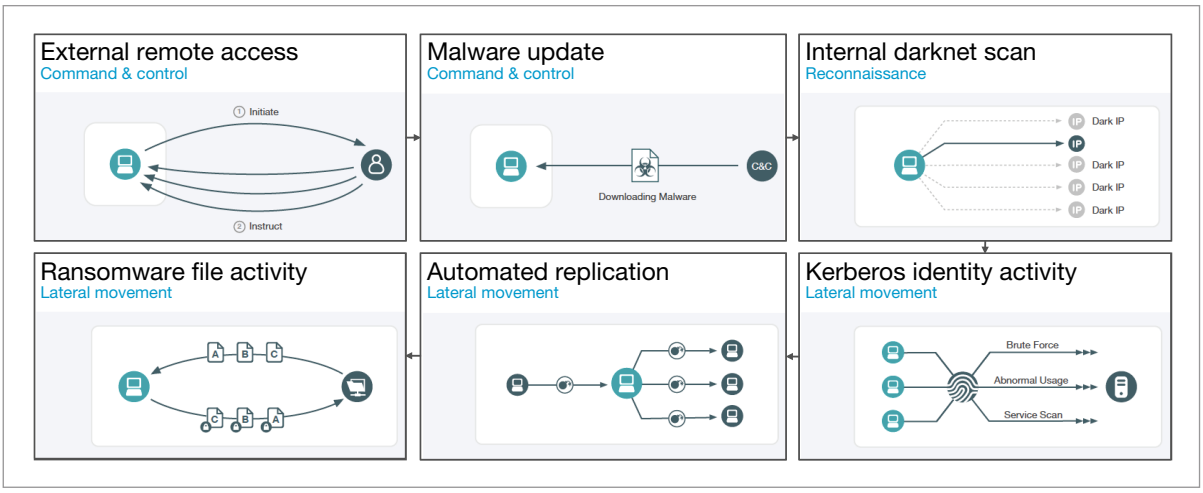
When organizations focus on securing endpoints, they are chasing the attack. Hackers can change the malware packaging they use and how they encrypt the package. This enables the malware to evade the antivirus solution. In addition, once most malware successfully installs on a host, the first action is to detect and disable all endpoint security.

Although malware is constantly evolving, the basic goals and actions of ransomware remain consistent. By focusing on the fundamental network behaviors that make ransomware successful, security teams can reliably identify and detect the threat and stop the attack before damage is done.

Conclusion

Staying ahead of ransomware threats is where organizations want to be because these insidious attacks are not going away. In fact, they are likely to become even more prevalent within organizations. The criminal appetite for juicy payouts and limited risk are just too big to ignore.

But organizations can fight back with a good plan to misdirect the thieves, a reliable backup strategy, and a security solution that identifies the progression of attack behaviors and detects the threat before the damage occurs.



Give yourself many chances to detect the threat

VECTRA

Email info@vectranetworks.com **Phone** +1 408-326-2020 www.vectranetworks.com