STOPPING CYBER THREATS

YOUR FIELD GUIDE TO THREAT HUNTING

DIGITALGUARDIAN®

TABLE OF CONTENTS

WHY READ THIS GUIDE?

Your security team should proactively and regularly hunt for cyber threats in order to stay on top of the ever evolving cyber threat landscape. If you are a CISO, information security manager, or security analyst, this eBook is a practical guide to help you understand how to set up your own threat hunting initiative. You will learn how to make your hunt as effective as possible in order to stop advanced persistent threats and prevent serious damage to your organization.

HOW TO USE THIS GUIDE

IF YOU ARE...	GO TO...
New to threat hunting	Part One: Understanding Threat Hunting
Not sure where to start	Part Two: Getting Ready
Familiar with threat hunting, but not sure how to implement it into the organization	Part Three: Five Stages for Threat Hunting
Struggling with how to make the business case for threat hunting	Tips From Tim: How to Build Your Business Case (Page 20)
Worried about managing threat hunting with limited resources	Part Four: Advanced Threat Protection as a Service
Looking to understand what makes Digital Guardian different	Appendix: Digital Guardian — Next Generation Data Protection

THREAT HUNTING EXPERT

This eBook is written by Tim Bandos, the Director of Cybersecurity at Digital Guardian. He has over 15 years of experience in cyber defense at a Fortune 100 company with a heavy focus on Internal Controls, Incident Response & Threat Intelligence. At this global manufacturer, he built and managed the company's threat hunting team.

Tim joined Digital Guardian to help build our Managed Security Program (MSP) to deliver advanced threat protection to our global customer base. He brings a wealth of practical knowledge gained from tracking and hunting advanced threats targeted at stealing highly sensitive data.

SEE OUR BLOG

· To learn why Tim joined Digital Guardian read his blog post, Why I Signed on with an IT Security Vendor.

TIM BANDOS
Director, Cybersecurity
Digital Guardian CISSP,
CISA, CEH & CASS

DIGITALGUARDIAN®

PART ONE
UNDERSTANDING THREAT HUNTING

WHAT IS A CYBER THREAT?

INTENT

The goals your adversary wants to achieve

+

CAPABILITY

The ability of your adversary to successfully breach your organization and achieve their intended goal(s)

+

OPPORTUNITY

Your adversary's timing and knowledge of your environment, including its vulnerabilities

=

A THREAT

A threat to your organization

SEE OUR BLOG

· Read Tim's blog on 'The Evolution of an Insider Threat: How a Business Analyst Turned into a Rogue Hacker'.

WHAT EXACTLY IS CYBER THREAT HUNTING?

Cyber threat hunting is the proactive practice of detecting, isolating and neutralizing advance threats. It involves searching and analyzing network and endpoint activities which otherwise evade automated solutions.

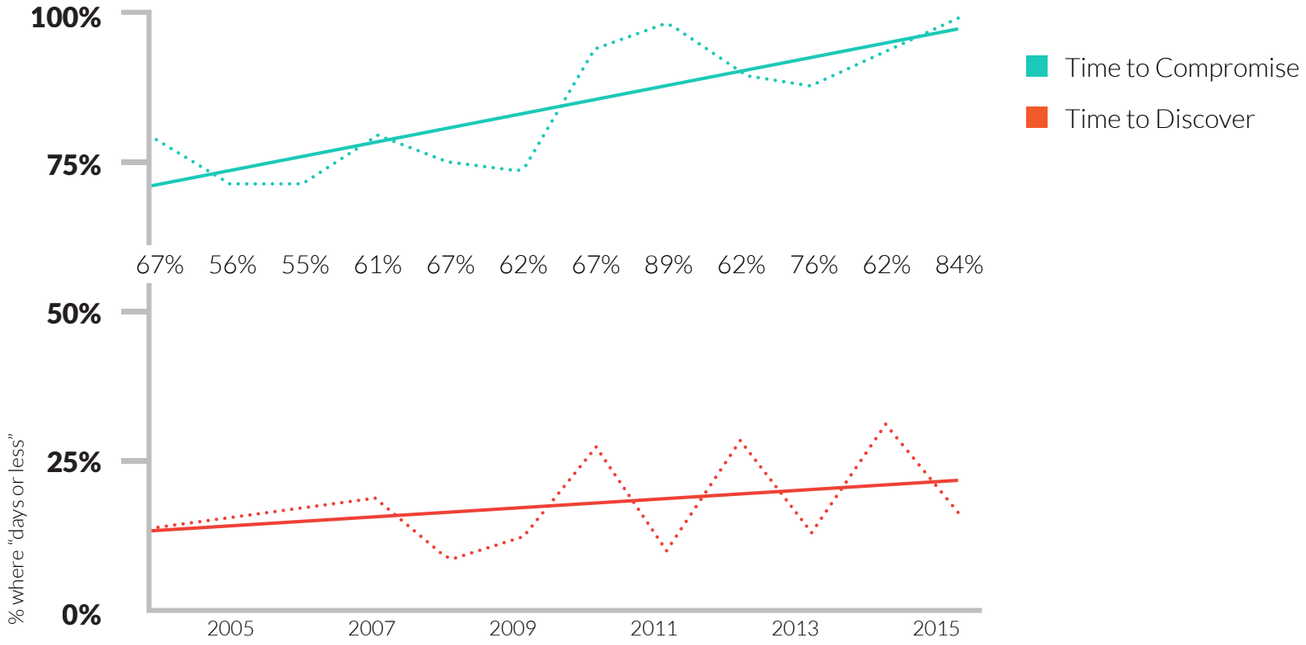
INTRUSION LIFE CYCLE

INFILTRATION	BACKDOOR INSTALLATION	COMMAND & CONTROL	EXECUTION	PERSISTENCE	ESCALATION OF PRIVILEGES	LATERAL MOVEMENT	EXFILTRATION
Identification of the weakest link and exploiting to penetrate defenses.	Malware installed on targeted system(s).	The adversary's primary communication between the installed malware and their own infrastructure.	Adversary commands and/or custom code running on compromised system(s).	Persistent presence on the compromised system irrespective of system restarts or a loss of privileged credentials.	Obtaining a higher level of permissions, to the system to gain complete control.	Moving across an environment from one system to the next.	The removal of data to an external location.

WHY HUNT FOR THREATS?

THERE IS A BIG "DETECTION DEFICIT" BETWEEN THE CYBER ATTACKS AND YOUR DETECTION

Advanced cyber attacks are sophisticated, targeted and difficult to detect. As shown in Verizon's latest Data Breach Investigations Report, time to compromise is almost always less than the time to discover. The trends suggest that 70%-90% of all malware reported was unique to an organization and companies on an average went more than 200 days between the time they were breached and the day they discovered it.



3 FUNDAMENTALS OF THREAT INTELLIGENCE

Threat Intelligence can be defined as knowledge about the tools, tactics and procedures used by adversaries; that'll potentially qualify threats, through the dissemination of this information to security monitoring devices for detection & prevention. The concept of Threat Intelligence is a little abstract though, and quite honestly could have an entire guide by itself. However, we can break it down into three fundamental pieces:

1

INDICATORS

Often described as an 'Indicator of Compromise', is an artifact (IP Address, Domain, File Hash, etc.) that has been linked with a certain level of confidence to an intrusion.

2

THREAT RESEARCH & ANALYSIS

Include statistics, write-ups, analysis of malware, etc. to assist Incident Responders in detecting patterns of an attack. A good example of this would be the yearly Verizon Data Breach Investigation Report.

3

TTPs

Tactics, Techniques, & Procedures go beyond simple indicators and describe the specific motivations, intentions, and capabilities of an adversary. When profiling Threat Actor groups, it's important to identify these traits to improve overall defenses within the organization.

TIPS FROM TIM

TIM BANDOS
Director, Cybersecurity
Digital Guardian CISSP,
CISA, CEH & CASS

BUILDING YOUR THREAT INTEL IN 20 MINUTES

No matter the size of your Company or number of endpoints you're protecting, it's critical to leverage Threat Intelligence to assist in providing context to alerts and deploying indicators to security devices for preventing successful cyber intrusions. Depending on the available resources and budget an organization has, it's relatively easy to stand up a Threat Intelligence database that houses Indicators of Compromise (IOC's), TTPs, and your malware samples for free of charge. My budget was thin at my last job so I literally used a spare laptop with 8 gigabytes of memory, installed Ubuntu, and stood up a CRITS instance to manage our intel. Total time: 20 minutes. From there I identified some external Threat feeds like AlienVault, ThreatConnect, etc and ingested them into the solution. You can also use a tool called CIF (Collective Intelligence Framework) that'll automate the process of pulling in threat feed data and will come with a bunch of sources already out of the box. You'll discover though that some of the BEST threat intel, is derived internally from your own incidents.

PART TWO
GETTING READY

LAYING THE GROUNDWORK

BUILD AN INCIDENT RESPONSE PLAN

Having a well-defined, formal incident response (IR) plan is recommended as a prerequisite to threat hunting. Whether your organization has a formal IR program or simply IR procedures, it is imperative to have a prescriptive method of responding to events and alerts in a controlled manner. This will help everyone avoid panic mode!

1. **PREPARATION**
2. **DETECTION AND REPORTING**
3. **TRIAGE AND ANALYSIS**
4. **CONTAINMENT AND NEUTRALIZATION**
5. **POST-INCIDENT**

INCIDENT RESPONDER'S FIELD GUIDE

· Get this guide for easy-to-follow steps to craft an incident response plan that works for your organization.

APPROACH TO THREAT HUNTING

While IR is best pursued as a well-accepted, business-wide initiative, your approach to threat hunting should be an effort centralized to your information security team. Threat hunting is less formal, more mission-oriented. It is a commitment to take a more proactive approach to identifying cyber threats to the organization, and to actually ***act*** on those threats sooner rather than simply waiting for an alert to go off.

While cyber threat hunting isn't exactly looking for a needle in a haystack, your efforts need to remain a bit more flexible, a little less formalized than Incident Response. There will be fewer boundaries when following where the hunt leads you.

TIPS FROM TIM

TIM BANDOS
Director, Cybersecurity
Digital Guardian CISSP,
CISA, CEH & CASS

TO KNOW YOUR ADVERSARY, FIRST KNOW YOURSELF

At my last job, we outsourced our IT administration to a third party vendor. Basically, they would authenticate each day to our network to conduct day-to-day maintenance activities on each of our servers. One day I was hunting through logs and noticed something strange. The third party vendor was accessing a subnet that they weren't responsible for. Upon further investigation I had discovered that the vendor had been compromised and an adversary was leveraging the trusted connection between our network and theirs to move laterally into our environment. The advice here is to never underestimate the importance of contextual knowledge and awareness of your network to recognize threats as they occur.

4 BUILDING BLOCKS

Before pursuing an active cyber threat hunting initiative, complete these four necessary actions:

1 **BUILD AN ARCHITECTURE**

Your organization must be capable of planning, establishing and maintaining its systems with cybersecurity in mind.

2 **IMPLEMENT PASSIVE DEFENSE**

Systems such as intrusion prevention should be added to your base architecture to provide a reliable defense against threats (once configured), without needing consistent human interaction or intervention.

3 **DEVELOP ACTIVE DEFENSE**

Define processes for human analysts to monitor data internal to the network, triage any advisories, and respond actively to any incidents to contain and neutralize the threat.

4 **DRIVE INTELLIGENCE**

Finally, data collection should be used to learn how the organization can better exploit information for insight and internal intelligence.

TIPS FROM TIM

TIM BANDOS
Director, Cybersecurity
Digital Guardian CISSP,
CISA, CEH & CASS

AVOID CHASING FALSE POSITIVES

Successful cyber threat hunters should know the value and the limitations of threat intelligence. Every organization may have its own misconceptions or internal biases. Understanding these up front will help your security team avoid the pitfalls of wasted time and resources spent chasing down alerts or false positives that really don't matter to your business.

3 TOOLS YOUR ORGANIZATION NEEDS FOR THREAT HUNTING

LOGS

Threat hunters require data. At a bare minimum, having log data logs to sift through is imperative. The top five event sources to examine are:

- Endpoint Data
- Windows event logs
- Antivirus
- Proxy and firewall

SIEM

A centralized security information and event management system can correlate all your log data better than humans alone. It eases your ability to pivot from individual pieces of information to links and correlations that reveal the true threat.

ANALYTICS

Machine learning and data analytics are a bonus for organizations that can afford them. Since they have the ability to automate the detection of cyber threats and identify the proverbial needle in the haystack.

TIPS FROM TIM

TIM BANDOS
Director, Cybersecurity
Digital Guardian CISSP,
CISA, CEH & CASS

HUNTING ON A BUDGET

For organizations on a budget, there are a multitude of great open source tools available for log capture & analysis, host and memory forensics, reverse engineering malware, etc. For example, a cost effective SIEM alternative is to set up an “ELK” Stack – Elastic Search, Logstash and Kibana – all wrapped into one.

4 SKILLS YOUR ANALYSTS NEED FOR THREAT HUNTING

ENTERPRISE KNOWLEDGE

Contextual knowledge and awareness of your environment.

HYPOTHESIS

Hypothesize threat attacks, source vectors and impact in the organization.

STATISTICS

Interpret data from statistical significance.

FORENSICS

Investigate the root cause and develop an attack timeline of events that transpired through network and endpoint forensics.

TIPS FROM TIM

TIM BANDOS
Director, Cybersecurity
Digital Guardian CISSP,
CISA, CEH & CASS

HOW TO BUILD YOUR BUSINESS CASE

Never let an Incident go to waste. If your team doesn't have the correct resources or adequate funding, I always recommend leveraging each and every incident as an opportunity to build your case. Go to upper management and say this: "The breach or incident that just occurred was a result of lacking a more robust security program with layered controls. In order to be more effective at detecting/preventing future attacks, we need A, B, and C". When I first started out doing this type of work at my last job, we and operated on a shoe string budget. I was on a team of 1, just me. There was no one to rely upon so I started to develop our capabilities myself. But as soon as we had our first incident or two, that's when I was able to start building a case for a budget and adding on to our architecture. Following that we implemented passive defense tools and then developed active defense procedures through people, process and technology. Finally, we strived for a data-driven defense process that was based on intelligence and ultimately the individuals at the top understood the value of a cybersecurity investment when I reported metrics on the number of breaches we prevented.

DIGITAL GUARDIAN®

PART THREE

5 STAGES OF THREAT HUNTING

1 **HUNT FOR KNOWN PREY**

2 **WATCH FOR UNKNOWN PREY**

3 **BIRD DOG THE THREATS**

4 **READY, AIM**

5 **PREPARE FOR THE NEXT THREAT**

1. HUNT FOR KNOWN PREY

The day has come! You've committed as a security organization to embark on an active threat hunting mission. You've laid the groundwork with incident response processes and procedures, built a defensive architecture, and acquired the tools and skills you need for a successful hunt. Now put on your camouflage and grab your ammo!

Hunting the adversaries you know is easy, or at least easier. Known adversaries have become known because they have revealed themselves in a number of ways:

- They match an indicator or signature that has been developed to detect them.
- Your anti-virus software vendor is aware and has listed them.
- Maybe you read about the exploit in a blog post or news article.
- Some known attacks are fairly amateur, easy to detect, or not well hidden
- The best case is that your Level 1 analyst has found the adversary!

2. WATCH FOR UNKNOWN PREY

Hunting for the unknown requires patience, persistence and more effort. This is because, unknown threats are more sophisticated, well-hidden and harder to detect. However, these adversaries leave indicators of their movement around your network. They will try to mimic the normal activity of authorized users to stay under the radar.

If you are vigilant, eventually they will reveal themselves as an outlier – primarily by taking actions that reveal their precise targeting and IT savvy:

- Leveraging new techniques for persistence
- Working through encrypted channels
- Creating command & control infrastructure
- Compiling their own toolset, like a malware or binary
- Pursuing authorized actions that lie outside of baseline activity data

WATCH YOUR LOGS

Here are some examples of what to examine from your event sources. There's a wealth of information in these logs! You'd be surprised what can be revealed simply by correlating information. By baselining a particular activity within your environment, and noting how often it occurs, you will start to see things pop up that are worthy of closer scrutiny. Patterns of suspicious behavior will emerge over the course of 30 days or even a couple of weeks. Anything that steps above the baseline is worthy of an alert to investigate. In many cases these early, seemingly benign activities are the reconnaissance or initial setup steps indicative of an impending attack.

PROXY LOGS

- Traffic being sent out port 22
- Network connections with same pattern of bytes in and bytes out
- Dynamic DNS visits
- Unique User Agent Strings
- Base64 Encoded Strings in URLs
- Executables being Downloaded

WINDOWS LOGS

- Explicit Logon Attempts (4648 / 552)
- User added to Privileged Group (4728, 4732, 4756)
- Failed Logon Attempts via Multiple Accounts
- Log Clearing Activity (104, 1102)
- EMET Crash Logs (1, 2)
- Application Crashes & Hangs (1000, 1002)
- Windows Defender Errors

ANTI-VIRUS

- Password Dumping Programs
- Specific Backdoors Detected (PlugX, 9002, Derusbi, Nettraveler, Winnti, Pirpi)
- Detections with Dropper in the name
- Custom Detection Creation

Get to know all the tools you already have and understand the type of data and reports that they generate. This level of awareness will allow you to start utilizing their outputs to actively start hunting for prey.

3. BIRD DOG THE THREATS

Every hunter needs a trusty hunting dog. Bird dogs are highly trained and bred specifically for the job at hand. The characteristics of a good bird dog (and how they apply to threat hunting) are:

SENSORY AWARENESS

A bird dog's five senses are highly tuned and always aware of their surroundings. Cyber threat hunters need to be just as vigilant, to better pick up the "scent" or actions of our adversaries. Be actively looking for specific types of threats on a regular, even daily, basis.

QUICK REFLEXES

A bird dog reacts to situations in a shorter amount of time than other dogs. As threat hunters "in the field", we need to continuously improve our processes of incident investigation and response for maximum efficiency.

INSTINCT

Bird dogs are bred to heighten specific instincts, such as a pointing and retrieving game. Your entire security team needs to develop new hunting tactics, excel at logistics, and operationalize whatever proves most effective.

COMMUNICATION

Bird dogs are excellent at communicating with their owners with wags or whimpers. As a security team, meet consistently to share the latest threat intelligence or suspicious indicators within your environment. This will help propel your threat hunting mission forward.

INTELLIGENCE

One of the hallmarks of a great bird dog is its superior intelligence. Superior threat hunters are innovative, analytical, and are able to hypothesize both meaning and insight from data.

As the security bird dog for your enterprise, you need to understand your environment better than anyone, and coordinate your team to hunt and counter adversaries better over time.

4. READY, AIM...

EXECUTE THE INCIDENT RESPONSE PLAN

So you found something! You have identified malware or something malicious within your environment. Your target has been flushed out of its hiding place and is on the run! Now what do you do?

Here's what comes next, and in what order...

1. **Gather as much information as you can about what transpired, where, and when.**

2. **Engage forensics experts.** Forensics reveals the "how" and sometimes even the "why" of what transpired when the bad actor was on that box or inside your software. It tells the story of what has been compromised and maps out every system to remediate.

3. **Engage and execute your incident response plan!** It's why you have one.

4. **Neutralize the bad guys.** First contain the threat, and then take all affected machines down at the same time so your adversary doesn't have an opportunity to come back. Wipe and clean everything.

5. PREPARE FOR THE NEXT THREAT

After the threat passes and you resolve the incident, here are a few recommendations of things you should do to be ready to confront the next threat.

1. LEARN

Learn from the adversary's behaviors by reviewing the incident as a security team.

2. DOCUMENT

Document the adversary's tactics, techniques and procedures.

3. DEVELOP ADVERSARY PROFILE

Develop a profile of the adversary, including region of operation, motive, intent and capability.

4. UPDATE THREAT INTELLIGENCE

Organize & manage all the threat indicators associated with the adversary's activity – file names, file paths, IP addresses, domains, what commands or control infrastructure was used, etc.

5. STORE

Store all this information in a central database.

6. DISRUPT

Disrupt adversary's future operations in your environment by applying updated threat intelligence.

TIPS FROM TIM

TIM BANDOS
Director, Cybersecurity
Digital Guardian CISSP,
CISA, CEH & CASS

YOUR ATTACKERS ARE CREATURES OF HABIT

At my last job, we had profiles on all of the different adversaries who had targeted us. So if there was a successful intrusion, we could tell whether it was this group or that. The first thing that one particular group would do was run the following command “ping -n 3 8.8.8.8”. What they were basically doing was checking for Internet connectivity by pinging Google’s DNS server. As soon as we received an alert for that command being run, I knew an attack was taking place! That’s a technique or tactic that particular adversary would leverage every time, so it was a huge indicator for us that they were in. Even if all of their malware and tools were missed, that one piece of information was something that we were able to detect successfully to start our investigation and response.

DIGITAL GUARDIAN®

PART FOUR

ADVANCED THREAT PROTECTION AS A SERVICE

WHEN DOES IT MAKE SENSE TO CONSIDER ATP AS A SERVICE?

If any of these apply to your organization it may make sense to outsource or augment your Incident Response team with an Advanced Threat Protection Managed Security Program:

SECURITY TALENT SHORTAGE

The severe security talent shortage, especially for cyber security professionals, is preventing you from finding and retaining the people you need to build an IR team.

HEADCOUNT CHALLENGES

The political climate of your organization makes it difficult to gain approval for the 3-5 people you need to build an effective IR team.

COMPLEXITY OF STAYING ON TOP OF SOPHISTICATED MALWARE

Modern malware is sophisticated, targeted and difficult to detect. According to Verizon's latest Data Breach Investigations Report, companies on an average went more than 200 days between the time they were breached and the day they discovered the malware. As malwares get smarter, your ability to prevent the loss of sensitive data on your own gets harder and harder.

ADVANCED THREAT PROTECTION MANAGED SECURITY PROGRAM

THE LATEST DEFENSE STRATEGIES AND INTELLIGENCE

Our Advanced Threat Protection Managed Security Program is led by Tim Bandos, Director of Cybersecurity. The program combines security researchers and analysts' expertise, Digital Guardian's Next Generation Data Protection Platform and a centralized threat intelligence management system. This combination enables Digital Guardian to detect and remediate threats faster and more efficiently. You can expect the highest level of protection from threats including polymorphic malware, zero-day attacks, advanced persistent threats (APTs), ransomware and attacks involving sophisticated data theft methods.

DIGITALGUARDIAN
MANAGED SECURITY PROGRAM
FOR ADVANCED THREAT PROTECTION

WHY DIGITAL GUARDIAN?

REAL-TIME VISIBILITY

Digital Guardian's continuous endpoint monitoring includes real-time and historic visibility into more than 200+ parameters associated with system activities. Visibility into the entire kill chain lifecycle means more effective detection & analysis by our team.

THREAT INTELLIGENCE

Our team harnesses both externally and internally generated intelligence feeds for immediate detection based on known threat activity.

EYES ON GLASS IDENTIFYING YOUR REAL RISKS

Our analyst team is constantly reviewing your data for anomalous behavior and alerting you immediately upon discovery. Alerts generated by your team will provide you with a summary of what's been detected and details around the type of alert.

INDICATORS OF EXECUTION

Our service utilizes behavioral-based signatures based on profiled malware and threat actor activity that is delivered via your content feeds. Your team is constantly researching emerging threats and developing these signatures to keep up with the dynamic & evolving world of threats.

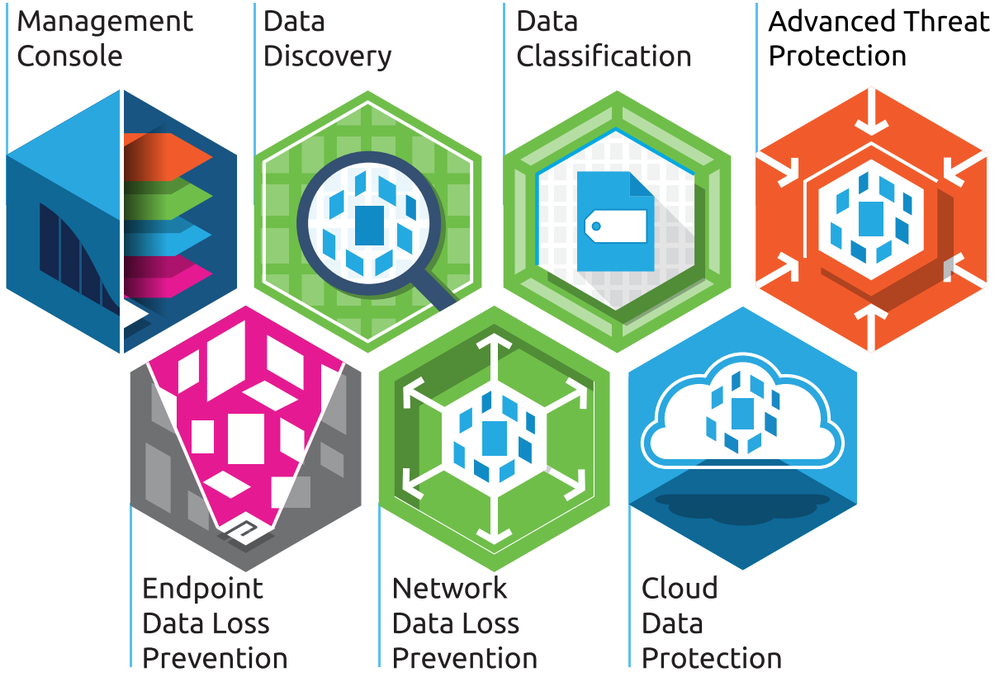
APPENDIX

DIGITAL GUARDIAN NEXT GENERATION DATA PROTECTION

NEXT GENERATION DATA PROTECTION

Data protection is at the core of our company mission. Our next generation data protection platform is purpose built to stop data theft. This platform is designed to:

- Discover and protect sensitive data through out the data lifecycle and across the enterprise
- Protect sensitive data on the network at the endpoint, in storage and in the cloud
- Provide automated classification
- Provide integrated advanced protection to protect data from external threats
- Provide flexible deployment options including a managed security service manned by our peerless analyst team with deep, real-world expertise



FREE DOWNLOAD

Digital Guardian Platform Technical Overview

FREE DOWNLOAD

Digital Guardian Managed Security Program Technical Overview

A LEADER IN THE GARTNER MAGIC QUADRANT

- "Digital Guardian offers one of the most advanced and powerful endpoint DLP agents due to its kernel-level OS integration. In addition to Windows, both Apple OS X and Linux are supported."
- **"The Digital Guardian solution for endpoint covers DLP and endpoint detection and response (EDR) in a single agent form factor…"**
- "…Digital Guardian [is one of] two vendors most frequently mentioned by clients looking for a managed services option."

FREE DOWNLOAD

· Gartner 2016 MQ for Enterprise DLP

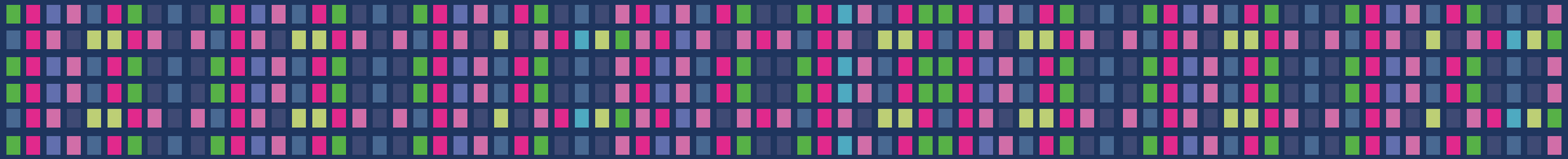
Gartner 2016 Magic Quadrant for Enterprise Data Loss Prevention, 1 February, 2016 , Brian Reed and Neil Wynne.

2016 GARTNER MAGIC QUADRANT FOR ENTERPRISE DATA LOSS PREVENTION

DIGITAL GUARDIAN®

60 MILLION TERABYTES

OF SENSITIVE DATA IS PROTECTED DAILY BY DIGITAL GUARDIAN AGENTS



OVER **2.5 MILLION** AGENTS DEPLOYED WORLDWIDE

TRUSTED DAILY BY MORE THAN **450** OF THE LARGEST BRANDS IN THE WORLD

...ONE OF THE LARGEST AND MOST RESPECTED COMPANIES IN THE WORLD HAS DEPLOYED OVER

300,000 AGENTS

INCLUDING...

7 OF THE **TOP 10** PATENT HOLDERS

AND 7 OF THE **TOP 10** AUTO COMPANIES

THE ONLY AGENT-BASED TECHNOLOGY COVERING

250,000 EMPLOYEES

USING A SINGLE MANAGEMENT SERVER

WE ARE THE **DATA PROTECTOR** OF **CHOICE** IN

BECAUSE WE'RE FOCUSED ON PROTECTING **ONE THING:**

STOPPING CYBER THREATS

JUST FOR FUN

We found this handy online glossary of hunting terminology. Like cyber threat hunting, real hunting has a language all its own!

QUESTIONS?

1-781-788-8180
info@digitalguardian.com
www.digitalguardian.com

DIGITAL GUARDIAN®