ARTICLE

Advanced Threat Detection Services Are Ideal for Growing Companies

An In-Depth Cyber Defense Technology Comparison

SecureWorks®

There are approximately 28 million small businesses in the United States[1] and nearly 200,000 medium-sized businesses.[2] Given the revenue that these vital organizations generate and the intellectual property that they own, small and medium-sized organizations are not excluded from cyber incidents and security breaches. Threat actors are opportunistic in their operations, regardless of whether their motives are financial gain, intellectual property theft or compromising an organization in order to reach a business partner. Recent research and analysis of breaches indicate that organizations are not keeping up with threat actor tactics, techniques and procedures.

Evading Detection

65%

of organizations say attacks are more advanced and evade existing preventive security controls.[3]

Failed Alerting

24%

of organizations were alerted by their endpoint security technologies to a potential breach.[4]

Third-Party Discovery

66%

of breach notifications come from an outside entity, such as the FBI or SecureWorks.[5]

Living off the Land

>50%

of SecureWorks targeted threat hunting cases identified adversaries who used little to no malware.[6]

Security Failures

33%

of organizations discover breaches two or more years after the incident.[7]

[1] Small Business Administration, https://www.sba.gov/managing-business/running-business/energy-efficiency/sustainable-business-practices/small-business-trends

[2] National Center for the Middle Market at Ohio State University, “US middle market firms and the global marketplace: Should I stay or should I go?”, http://www.middlemarketcenter.org/research-reports/US-middle-market-and-global-marketplace

[3] Ponemon Institute, 2014: *A Year of Mega Breaches*, January 2015

[4] Ponemon Institute, *2014 State of Endpoint Risk*, December 2013

[5] SecureWorks Counter Threat Unit, Special Ops Division

[6] Ibid.

[7] Ponemon Institute, *2014 State of Endpoint Risk*, December 2013

Achieving Defense in Depth

Securing your business is not easy, but strategies like defense in depth can help. Defense in depth requires a combination of network- and endpoint-based solutions since each identifies different types of threats. iSensor, Advanced Malware Protection and Detection (AMPD) and Advanced Endpoint Threat Detection (AETD) are complementary solutions (Figure 1) that include SecureWorks intelligence to ensure the broadest range of protection, even if your organization has no security expertise or limited IT security staff.

iSensor is an intrusion detection and prevention system (IDS/IPS) that monitors network traffic and uses signatures developed by the Counter Threat Unit™ (CTU) research team. These signatures are based on previously seen behaviors and patterns to identify, prevent and respond to suspicious activity. SecureWorks threat researchers update the iSensor signatures within days of identifying new threats to ensure the best protection possible.

AMPD combines a network appliance, a team of security experts and SecureWorks Threat Intelligence to provide an early warning system that protects your organization from web- and email-based attacks, even unknown attacks that can't be identified via signatures. With new threats being created daily, it is critical to include security solutions that can identify zero-day and unknown malware. By monitoring activity at the network level, AMPD detects files and activities that appear to be suspicious and runs them in an isolated sandbox using full-system emulation to see exactly what would happen on a real endpoint. This allows AMPD to identify threats we've never seen or those that are specifically designed to evade other security tools. Our expert Senior Intrusion Analysts team identifies the risk and provides you with context on the threat and advise on how to quickly address it.

AETD is also backed by our Senior Intrusion Analyst team and uses behavioral detection methods to identify threats on the endpoint, even if no malware is used. Attackers "living off the land", using stolen credentials and native windows tools, are typically not detected by traditional network security tools because no malware is used. In over half of the targeted threat response engagements performed by SecureWorks in the last year, cybercriminals breached those organizations' networks by using little or no malware in their attacks. AETD detects these attacks and decreases response time by pinpointing affected assets and providing visibility on endpoints no matter where they are located, even outside the corporate security perimeter.

Figure 1: Defense in Depth - Complete Coverage with iSensor, AMPD and AETD

Threat	iSensor	AMPD	AETD
Packet-based attack attributes in http header, such as POST and GET commands	✓	✓	
Identify unique attributes with SSL certificate used for encrypted attacker communications	✓	✓	
Communications with known C2 infrastructure	✓	✓	✓
Identify malicious code in Word document attachment sent from partner organization		✓	
Exploit kit detection on the wire	✓	✓	
Analyze and identify malicious file served up by URL in an email		✓	
Detect malware evasion techniques		✓	
Can detect malware without signatures or pre-knowledge		✓	
Captures files and pcaps associated with threats on the wire		✓	
Provides manual file analysis option to analyze externally obtained suspicious files		✓	
Detect use of PowerShell script with valid credentials to download tools and programmatically delete files			✓
Detect use of credential theft tool on DMZ server and moving laterally inside the network			✓
Capability to obtain files from an endpoint associated with a threat			✓
Visibility of endpoints outside corporate perimeter			✓

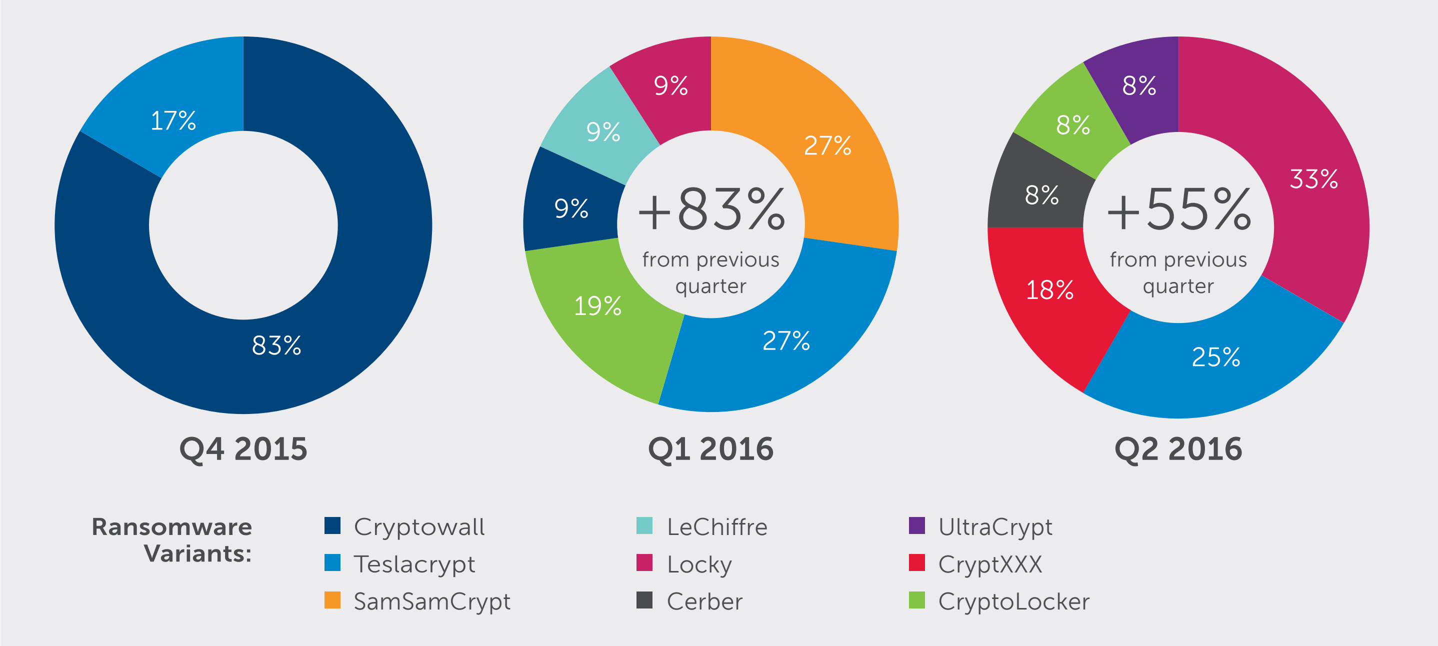
SecureWorks®

Malware Evolution

Cybercriminals are increasingly finding profitability through diversification and rapid changes in tools and delivery methods. Data compiled by the SecureWorks CTU and Incident Response (IR) teams (Figure 2) documents the level of ransomware activity and variants observed. Cybercriminals generally gravitate toward methods and tools that deliver the highest financial return for the lowest effort. These observations suggest how cybercriminals are challenging your organization to keep up with the continuously evolving threat actor methods.

Conventional security controls lack the technology to identify the delivery methods and embedded code within objects to protect your organization. For more sophisticated ransomware variants, like SamSam, endpoint visibility to detect compromised servers is critical in identifying the threat before file system encryption begins. The variation in the ransomware threat landscape will continue to pose challenges and emphasizes the need for robust preventative controls that are underpinned by intelligence and advanced analytics. Technology alone is not enough to identify these complex and constantly evolving threats.

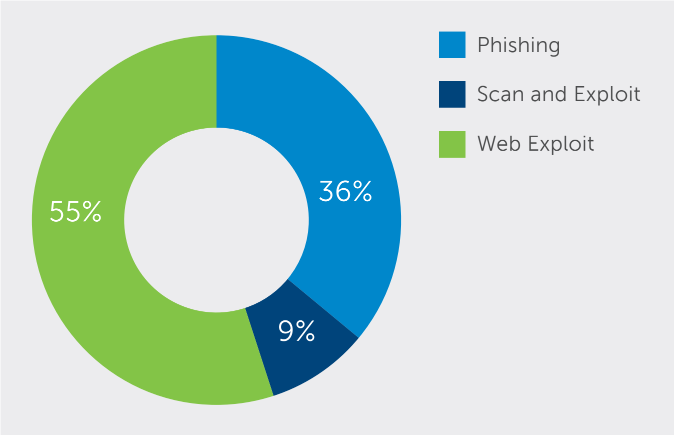
Figure 2: Proliferation of Ransomware



Shifting Attack Vectors

To further complicate the mission of protecting against new variants of ransomware and other malware, the distribution mechanisms are also shifting. The initial access vectors for malware in the first half of 2016 have shifted from phishing emails to web exploitation (Figure 3). Attackers are using exploit kits like Neutrino and RIG to exploit vulnerabilities in browsers and then deliver ransomware.

Figure 3: Initial Attack Vectors

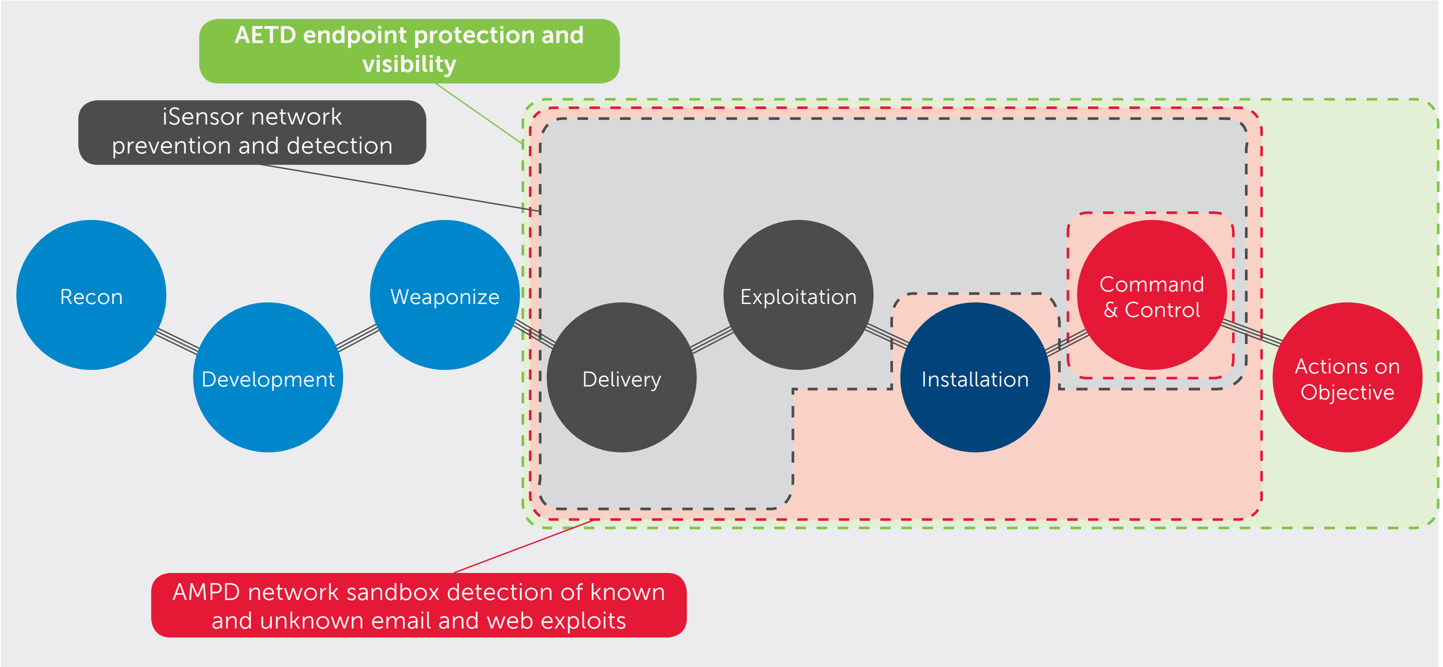


Mitigation Across the Kill Chain

Mitigating threats requires people, process and technology to address various levels of the kill chain (Figure 4) and predict, prevent, detect and respond to adversary actions. IDS/IPS and sandbox technology cover the same areas of the kill chain, but sandboxing adds visibility into unknown threats, including file objects with embedded malicious content. Advanced endpoint technologies extend visibility down to the endpoint and reduce time to detect and the effort needed to respond when prevention has failed.

SecureWorks provides an early warning system for evolving cyber threats so you can prevent, detect, rapidly respond to and predict cyber attacks. Combining unparalleled visibility into the global threat landscape and powered by the Counter Threat Platform — our advanced data analytics and insights engine — SecureWorks minimizes risk and delivers actionable, intelligence-driven security solutions for clients around the world.

Figure 4: How SecureWorks Addresses the Kill Chain Model


AETD endpoint protection and visibility
iSensor network prevention and detection
Recon
Development
Weaponize
Delivery
Exploitation
Installation
Command & Control
Actions on Objective
AMPD network sandbox detection of known and unknown email and web exploits

Security point products and tools aren't enough to address today's evolving threat landscape, especially for growing organizations without the skills or staff to make sense of the alerts and information these tools provide. SecureWorks Senior Intrusion Analyst team, backed by the Counter Threat Unit research team, provide intelligence to make sense of the noise that security tools can generate. By correlating information from multiple security tools, we help reduce massive amounts of data and alerts into actionable information.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com