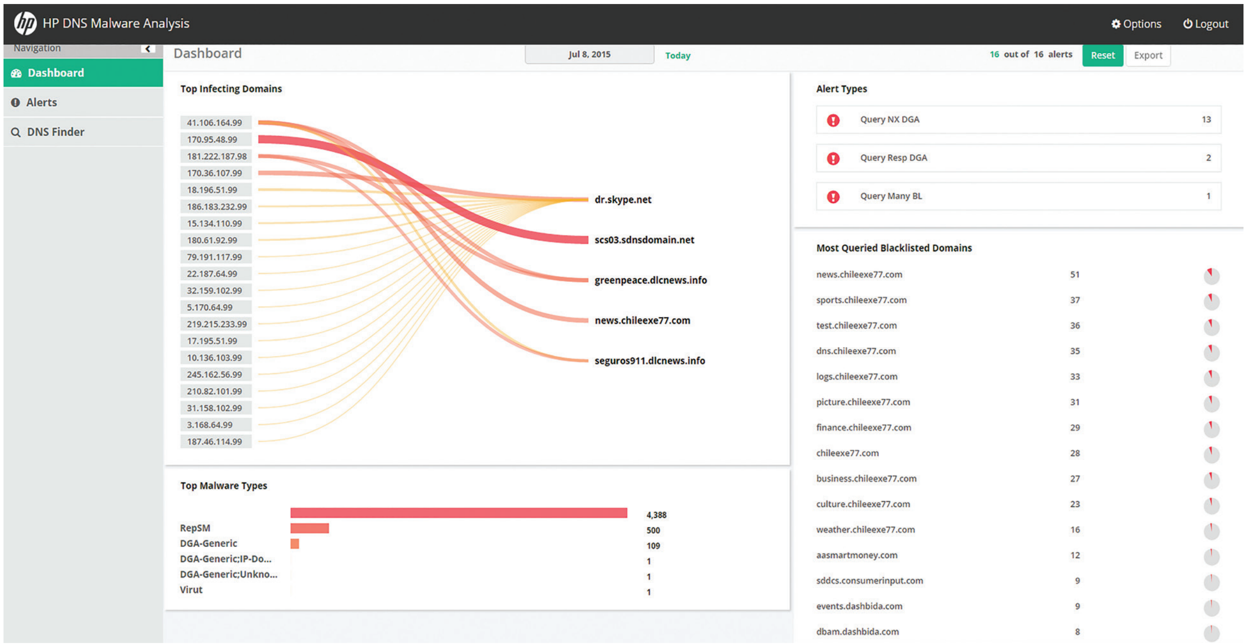
Data sheet

HP ArcSight DNS Malware Analytics

HP ArcSight DNS Malware Analytics, a security analytics solution, detects malware-infected hosts and endpoints—servers, desktops, mobile devices—rapidly with high fidelity. Our patent-pending, unique data analytics approach analyzes DNS traffic to identify “bad” traffic among hosts and IPs in real time to detect breaches before damage occurs.

Designed in partnership with HP Labs, HP’s central research organization, DNS Malware Analytics (DMA) equips users with an automated system for host breach detection, allowing enterprises to address the unknown threats quickly, especially those that are the biggest source of risk to enterprise applications, systems, and data. With DMA, users can detect threats without overloading SIEM systems with an overwhelming number of DNS logs.



Alert Types

!	Query NX DGA	13
!	Query Resp DGA	2
!	Query Many BL	1

Most Queried Blacklisted Domains

news.chileexe77.com	51
sports.chileexe77.com	37
test.chileexe77.com	36
dns.chileexe77.com	35
logs.chileexe77.com	33
picture.chileexe77.com	31
finance.chileexe77.com	29
chileexe77.com	28
business.chileexe77.com	27
culture.chileexe77.com	23
weather.chileexe77.com	16
aasmartmoney.com	12
sddcs.consumerinput.com	9
events.dashbida.com	9
dbam.dashbida.com	8

Highlights

- Security analytics with high fidelity detection of malware-infected systems and endpoints
- Real-time analysis of “bad” traffic to detect breaches before damage occurs
- Automated breach detection that allows enterprises to eliminate unknown threats quickly
- Detect threats without overloading SIEM systems with an overwhelming number of DNS logs

Find the “bad guys” with advanced threat detection and reduce breach impact

DMA identifies infected devices with high fidelity, positively discovering threats on systems, desktop, and mobile devices so they can rapidly be contained. This helps to find the “bad guys” faster by calling out the malware and reducing the impact of breaches by identifying these threats before they gain a foothold inside your network. With look-back capability, sources and spread of malware infections can be identified to reveal threat intent.

Faster event resolution

Enable IT as well as Big Data security staff to prioritize and remediate the highest risk devices, helping to achieve faster event resolution and contain threats quickly.

Lowers monitoring and management costs

Achieve investigation efficiency by reducing DNS signal noise, enabling organizations to widen their detection footprint, prioritizing, and scoring the critical alerts, which simplifies the alert management process. Removing false positives is a huge time saver for IT staff as well, which saves investigation and staff required to locate infections.

Reduces the cost of DNS security

Lower the cost of DNS security by employing security analytics that help you protect current DNS deployments and help eliminate the costly extraction, backhaul, and processing of DNS server logs.

Seamlessly integrates with SIEM to take action on infected hosts

DMA detects infected hosts enabling customers to utilize their SIEM analytics to get additional detail and take further action to address the threat. It integrates seamlessly with HP ArcSight ESM by sending alerts in CEF format; ESM enables correlation with other data sources to take action on the alert information.

About HP Enterprise Security

HP is a leading provider of enterprise Big Data security analytics and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HP ArcSight, HP Fortify, and HP TippingPoint, the HP security intelligence platform uniquely delivers the advanced log and event correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Developed with HP Labs

Learn more at
hp.com/go/arcsightanalytics

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document