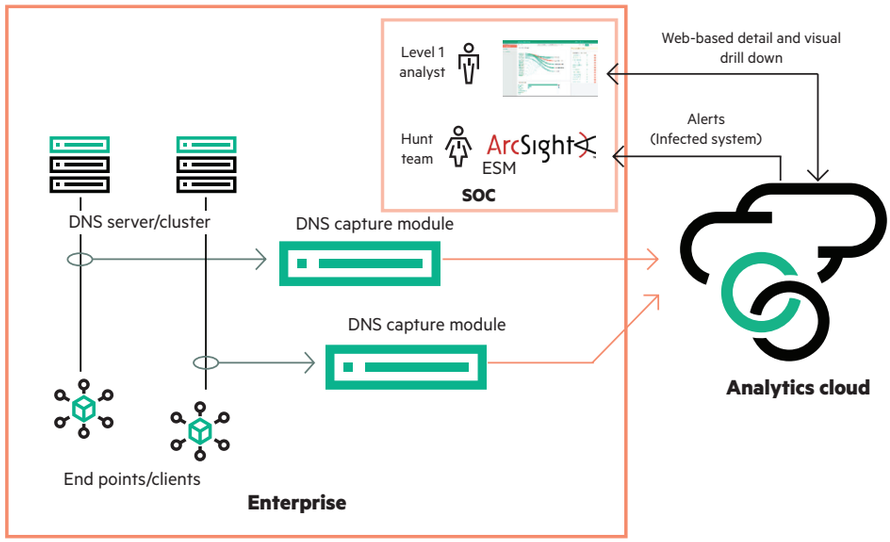
Hewlett Packard Enterprise

HPE Security ArcSight DNS Malware Analytics (DMA)

HPE Security ArcSight DNS Malware Analytics (DMA), a security analytics solution, detects malware-infected hosts and endpoints—servers, desktops, mobile devices—rapidly and with high fidelity. Our patented, unique data analytics approach analyzes DNS traffic to identify "bad" traffic among hosts and IPs in real time to detect breaches before damage occurs.

Highlights

- Security analytics with high fidelity detection of malware-infected systems and endpoints
- Easy to deploy and use, enabling everyone in IT to remediate malware, not just expensive analysts
- Automated malware detection that allows enterprises to eliminate unknown threats quickly
- Detect threats without overloading SIEM systems with an excessive volume of DNS logs

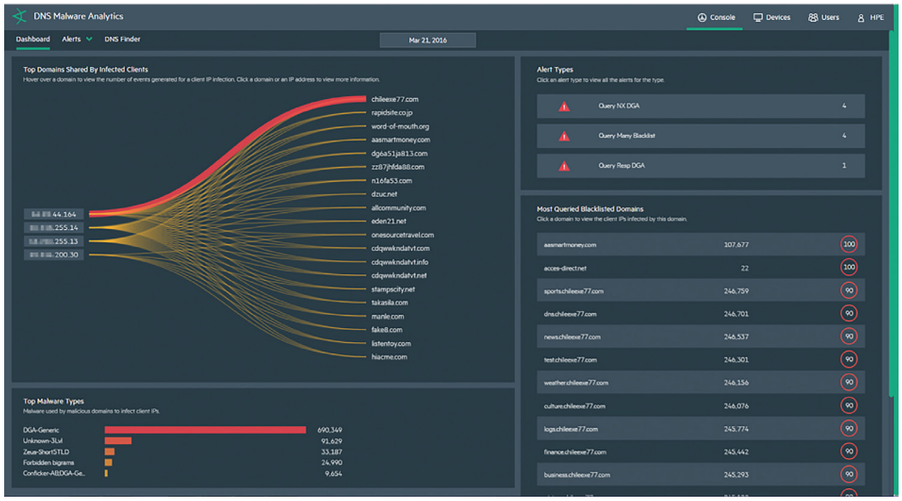


ArcSight DMA is a Service as a Solution (SaaS) offer and works in conjunction with the DNS Capture Module which is deployed in the network to capture and filter DNS packets, and send incidents of concern to the SaaS cloud.

Developed in partnership with Hewlett Packard Labs, the HPE central research organization, DNS Malware Analytics (DMA) equips users with an automated system for host breach detection. This allows 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 excessive number of DNS logs.

Types of Malware Detected

- General DNS Malware behavior instead of outdated rules or signatures,
- Sees both DNS Queries and Replies,
- Data Tunneling over DNS,
- Domain Generation Algorithms (DGAs) which use domain randomization to defeat firewalls, proxies and perimeter security,
- Blacklisted Domains,
- Zero-day and Malware Mashups.



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

ArcSight 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.

Resolve events faster

Enable general IT staff 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.

Lower 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, reducing the time to investigate and locate infections.

Reduce 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

ArcSight 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 ArcSight ESM by sending alerts in CEF format; ArcSight ESM enables correlation with other data sources to take action on the alert information.

Why HPE ArcSight?

ArcSight SIEM is the industry's leading SIEM solution. Scalable, powerful and simple to use, it delivers fast, accurate threat detection. Developed by security professionals for security experts, ArcSight's flexibility and fast time-to-security-value make it ideal for security operations of any size, from small groups up to the most sophisticated SOCs in the world. ArcSight takes a holistic approach to security intelligence, uniquely unifying Big Data collection, network-, user- and endpoint-monitoring and forensics, and advanced security analytics. Effective out-of-the-box use cases include real-time threat detection and response, compliance automation and assurance, and IT operational intelligence.

Rely on the security expertise, experience and leadership of the ArcSight team for your SIEM needs. ArcSight has been acknowledged as Magic Quadrant Leader by Gartner for the past 12 years, longer than any existing vendor—a testament to the power and effectiveness of the solution.

Hewlett Packard Enterprise, with industry-leading solutions, proven methodologies, and a decade of in-depth experience, is the right choice to help you achieve your desired security posture and reach operational excellence.

Learn more at
hpe.com/software/arcsight

Data sheet

4AA6-1039ENW, June 2016, Rev. 3