mimecast | Datasheet

Mimecast Web Security

Improving Web Security

Email and the web make up the source of nearly all security incidents and breaches that occur. According to the Verizon Data Breach Investigations Report 2018, 99% of malware, such as ransomware, was delivered via malicious email attachments or via the web. But, however it was delivered, most malware accesses the web and does so using Domain Name Services (DNS) to connect with its command-and-control site. The problem is most organizations don't monitor their DNS activity, leaving them blind to this communications path.

Malicious links can be delivered to users in many ways, including via embedded links in otherwise harmless websites, through instant messaging systems, via social network sites, and by ad networks – not just email. But like email organizations can't turn off access to the web or DNS to protect themselves because the productivity of employees, as well as many business operations, depend on this access.

Many organizations also have Acceptable Web Use Policies designed to protect against undesirable employee online activities, such as using company resources for private gain, wasting time browsing the web during work hours, and exposing the organization to risk or legal liability. Accordingly, organizations need systems that will monitor and enforce these policies. Certain websites while not malicious from a security standpoint (i.e. shopping, web mail, social networks, pornography, weapons, etc.), often need to be monitored and blocked when the employee is using the organization's computing resources.

Traditionally, many organizations have attempted to block access to malicious or business inappropriate sites using on-premises firewalls, Unified Threat Management (UTM) systems, endpoint software or web appliances (gateways/proxies). These can be costly to acquire, operate and maintain and may not provide the most current protections. As a result, increasingly organizations are moving their web security systems to cloud-based providers for the same reasons that this is happening for email security: cost, lack of security staff and skills, ease of deployment and management, and improved security efficacy.

Key Capabilities

- Administered via a single administrative console supporting both email and web security
- Site, user, and group-specific policies and exception lists administered by the organization.
- Integrated with Mimecast Targeted Threat Protection – URL Protect to provide consistent web security controls no matter the source of the web access.
- Leverage existing configurations for Directory Synchronization, Branding, Role-Based Access Control, and other core Mimecast platform features.
- Blocks both policy violating and malicious web sites which often deliver malware or are part of credential stealing phishing attacks.
- Inspection of file downloads via a Mimecast web proxy service with multiple AV engines.
- Delivers comprehensive historical web access audit logging. Accessed data can be exported to .csv files.
- Built-in reporting dashboard including visualizations of the top 10 accessed domains, accessed site categories, blocked domains, blocked by site category, as well as DNS requests that were associated with malware or malicious sites.
- Full audit log of system access, events, policy creation and changes.
- Mimecast Security Agent available for Windows and Mac computers to provide off network protection.
- Globally distributed datacenters providing minimal latency and high performance and reliability with a 100% uptime SLA, leveraging the highly flexible Mime|OS platform that has been used for years in support of the Mimecast Secure Email Gateway services.
- Very fast deployment, often connected and deployed in less than 60 minutes.

Mimecast Web Security

The Mimecast Web Security service protects against malicious web activity initiated by user action or malware (ransomware and other malicious software), and blocks access to business inappropriate websites, based on policy – all as a fully cloud-based service. This Mimecast service adds strong security at the DNS layer of the web, and is easy to implement and manage. When combined with the Mimecast Secure Email Gateway with Targeted Threat Protection organizations can use a single, cloud-based service that protects against the two dominant cyberattack vectors: email and the web.

How it Works

- The user, typically in a browser, makes a request for a web-based resource by clicking a link, or typing an address in the browser.
- The DNS request, depending on the configuration - via a local Mimecast Security Agent or internet gateway based configuration - is forwarded to the Mimecast Web Security service for inspection and resolution or filtering.
- The Mimecast service applies the organization's acceptable use controls based on user, group, and site policies, any bypass exceptions, and evaluates the sites classification to determine if the site is acceptable/unacceptable or non-malicious/malicious.
- Access to unacceptable or malicious web resources are blocked and the user is notified via a browser-based communication.
- Access to legitimate web resources are immediately allowed. The IP address of the requested site is returned and is used by the browser to request the desired web page.
- Access logs and associated reports are generated by the Mimecast service and are available for review by an appropriately privileged system administrator.

Mimecast (NASDAQ: MIME) makes business email and data safer for thousands of customers with millions of employees worldwide. Founded in 2003, the company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management.