EdgeWave™

White Paper

Cyber Security Essentials for Banks and Financial Institutions

EdgeWave

15333 Avenue of Science
San Diego, CA 92128.

Phone: 858-676-2277
Fax: 858-676-2299
Toll Free: 800-782-3762
Email: info@edgewave.com

www.edgewave.com

White Paper

High profile security breaches and the resilience of advanced persistent threats have clearly demonstrated why cyber security concerns have influenced the regulatory legislation governing all industries, and why regulations are here to stay. The fact that the majority of data gathered and compiled by organizations, including banks and other financial institutions, is now in electronic format and the failure to secure your network against emerging threats can open you to threats and greater risks, make securing this information as important for small banks and credit unions as it is for national chain institutions. While storing information electronically has certainly made storage and transmission of this information less costly and more efficient, it has also provided more opportunities for data to be lost, stolen or corrupted. According to one banking professional, "We see a growing dominance of hacking and malware used to grab credentials or create back doors." These back doors can let in criminal malware from the outside as well as create opportunities for data loss from inside your organization.

This White Paper

This paper will discuss the regulatory requirements facing your organization and present the consequences of non-compliance. It will also provide information about the major threats from malware and "hacktivism" and the risk of data loss that result in costly fines and litigation. Finally, it will present some solutions that can help your organization defend against threats and mitigate risks allowing you to not only protect your private and confidential data, but also help you maintain compliance with the many regulations governing your business.

The Regulatory Landscape

In order to protect sensitive customer data and safeguard intellectual property and financial records, the US Congress has passed a number of laws governing how this data is to be secured. These laws are applicable to almost every industry including banks and other financial institutions, medical organizations, government entities including schools, and businesses of all kinds. In addition to protecting data, these organizations must be able to document that they are in compliance.

Some regulations provide detailed requirements for the written security and privacy policies an organization must provide, while other regulations are less specific, requiring only that safeguards be "appropriate" depending on the size of the organization and the type of activity it conducts. In all cases, consequences for non-compliance can result in devastating financial, reputational and customer retention losses.

The following table contains a list of key regulations, the industries they govern, their general policy requirements and some information about the consequences of non-compliance.

Regulation	Requirements	Consequences of Non-Compliance
Sarbanes-Oxley Act (SOX) Governs: All Publicly Traded Companies	Requires executives and auditors to confirm the effectiveness of internal controls for financial reporting. • Ensures control of unauthorized access to data or data deletion • Requires robust access controls, interoperable with enterprise authentication, access and auditing	Violations can incur substantial fines and lost revenue. Here are some losses incurred by companies for SOX violations. The total includes settlement fees, lost business, fines and remediation costs: • American Home Products: $3.75 billion • Bank of Credit and Commerce : $17 billion • BAT Industries: $73 billion • IBM: $6 billion • Prudential Insurance: $4 billion
Gramm-Leach-Bliley Act (GLBA) Governs: Financial Services	Institutions governed by GLBA must assure the security and confidentiality of customer records and information • They must protect against any anticipated threats or hazards to the security or integrity of such records • They must protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.	Violation of GLBA may result in a civil action brought by the U.S. Attorney General. The penalties include those for the financial institution of up to $100,000 for each violation. In addition, "the officers and directors of the financial institution shall be subject to, and shall be personally liable for, a civil penalty of not more than $10,000 for each such violation". Criminal penalties may include up to 5 years in prison.

Regulation	Requirements	Consequences of Non-Compliance
The Prioritizing Resources & Organization for Intellectual Property Act Governs: All US Companies	In general, gives law enforcement more latitude in enforcing intellectual property (IP) laws • Protects IP including pharmaceuticals and manufactured goods, and artistic works such as MP3 and video files or other content transmitted electronically as well as on hard media • Organizations that are lax in securing their networks from illegal downloads face stiff penalties including criminal charges and having their computer equipment confiscated	As a result of this bill, U.S. Immigration and Customs Enforcement (ICE HSI) opened 1,033 intellectual property cases, which resulted in 365 arrests, 216 indictments and 170 federal and state convictions. [46]ICE HSI has identified and seized domain names facilitating the trafficking of pirated materials.[43] Customs and Border Protection (CBP) and ICE HSI had 19,959 intellectual property seizures, which resulted in 237 civil fines and penalties totaling over $62 million.
Federal Information Security Management Act (FISMA) Governs: Any entity that keeps Federally regulated information	FISMA provides a framework for ensuring the protection of Government information, operations and assets. The legislation requires agency officials to implement policies, procedures and practices to strengthen information security and reduce security risks. FISMA compliance requires agencies to: • Develop an agency-wide security program • Implement and adhere to security configuration standards developed by NIST • Identify and resolve risks • Perform ongoing assessment and testing • Conduct annual reviews on the effectiveness of the agency's information security and • privacy programs and report the results to OMB annually	Violations can result in termination of executives, budget reductions, and substantial fines
Payment Card Industry Data Security Standard (PCI DSS) Governs: Any US Companies that process credit cards	PCI DSS compliance has 12 requirements, often referred to as the 'digital dozen'. These define the need to: 1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor supplied defaults of system passwords and other security parameters 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks. 5. Use and regularly update antivirus software or programs 6. Develop and maintain secure systems and applications 7. Restrict access to cardholder data by business need-to-know. 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes 12. Maintain a policy that addresses information security for employees and contractors.	Non compliance with PCI DSS can result in large fines and even greater financial impact from lost business. Businesses face fines up to $500,000 and expensive litigation costs. Network security breaches can result in escalating compliance costs for merchants affected. In addition, non compliance impacts brand reputation and exposes corporations to extensive negative publicity that undermines consumer confidence.

Regulation	Requirements	Consequences of Non-Compliance
HIPAA (Health Insurance Portability and Accountability Act of 1996) Governs: Healthcare facilities and any other organizations that retain healthcare information such as schools HITECH HIPAA was expanded in 2009 as a result of the American Recovery and Reinvestment Act (ARRA) and the HITech Section:	HIPAA requires protection of confidentiality and assures the integrity and availability of all electronic protected health information (EPHI) that is created, received, maintained or transmitted. • Must protect against any reasonably anticipated threats or hazards to the security or integrity of health such information • Requires protection against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule; and • Organizations must ensure compliance by their workforces HIPAA was expanded in 2009 as a result of the American Recovery and Reinvestment Act (ARRA) and the HITech Section: Important HITECH Requirement • Includes ANY organization or individual who handles PHI for any reason and the Technical Safeguard requirements now apply to those organizations or individuals • Now includes organizations not previously governed by HIPPA such as banks, businesses, schools and others • New requirements include a stick and a carrot – penalties for not digitizing patient healthcare information and rewards for those who accomplish it sooner – digitized information required electronic security • Within organizations handling PHI, penalties can and will be imposed for lost or endangered data including the right of victims to sue individuals found culpable within those organizations	Fines can range from $50,000 to $250, 000 and 10 years in federal prison. A recent judgment against a Maryland healthcare provider resulted in a judgment of $4.3M Enforcement under HITECH has been beefed up and penalties for violations can be severe including: • Substantial fines, even imprisonment • Loss from expensive litigation and judgments against violators both organizations and/or individuals • Brand damage from the requirement to publicize violations against the provider.

Internet and Email Based Threats and Risks can Jeopardize Compliance

Botnets are Pervasive and Dangerous

Originally identified in 2006-2007, Botnets are a class of criminal malware designed and built to infect computers and networks, steal valuable data, and control victims' computers in order to commit other cybercrimes. According to experts, today's botnets are sophisticated, money-making machines that not only hijack data and compromise business networks, they are the backbone of an entire criminal ecosystem with the capability of putting all businesses and institutions at risk.

Among virus and malware protection efforts, bot defense can be the most challenging. Bots are autonomous applications that gain access to your network and can stay hidden for weeks. They can invade any OS, including Windows and malware protection used by most companies may not detect them. Once they 'phone home' to command and control outside your network, they join together with other computers to form botnets. These hijacked computers are called zombies and most traditional malware protection solutions are ineffective against them.

Botnets are different from Spam, Phishing and Viruses ("Spamware") and having both Web and Email security can increase your chances of protection:

1. Botnets are usually controlled by organized criminal syndicates or state actors with a malicious purpose, as compared to individual or small groups of hackers engaging in pranks, on-line graffiti, or spam marketing. Botnets are formed from bots, autonomous applications created by cybercriminals for financial gain. The criminals form vast networks of these applications that can infect organizations and do massive damage before they are detected.
2. Botnets are active exploits designed to get inside your network, often by social networking or piggybacking on devices brought in from outside, such as laptops, smartphones, and USB drives. The bots that form botnets are very stealthy and can lurk deep inside your network for weeks or months. They remain inactive until they communicate with their command and control hosts (C & C hosts) outside your network to receive instructions. Once the bot reports "I am here waiting for instructions", they begin to receive commands. They may be told to "replicate themselves" or to "infect other machines in the network". They can also receive instructions such as "steal credit card numbers from your customer database". By contrast, most spamware is acted on by the user, not through the control of a remote party, although bots are also sent via email.
3. Botnets are designed to steal your most valuable data, be it customer credit card numbers, your personnel data, or your engineering designs. Unlike these dangerous bot applications, the spamware we are used to seeing is primarily designed to get attention. While annoying, its main offense is to waste your time and slow down your machine. Botnets are a far more dangerous risk.

Botnet invasions can have serious consequences including:

- Financial loss from non-compliance fines or litigation
- Damage to e-reputation from phishing sites or proxy nets not blocked by other malware and virus protection solutions
- The hassle and cost of having to take virus and malware protection measures in the case of click fraud, DDoS and SPAM
- The cost of procuring and implementing multiple malware and virus protection solutions to detect or prevent compromised endpoints as recommended by many IT security vendors
- The costs associated with acquiring expensive startup malware and virus protection appliances

The Zeus Trojan – A Botnet Attack Aimed at Banks

The banking industry was hit hard by the infamous Zeus Trojan, a botnet invasion that continues to plague banks worldwide. It started out as a botnet kit, programs that allow hackers to build and exchange the bots used in forming botnets. The Zeus kit was specifically designed to defraud bank customers and experts estimate that the successful exploits using Zeus resulted in thousands of criminal hackers stealing hundreds of millions of dollars from banking customers all over the world. Although there have been many arrests in conjunction with Zeus, it is still out there and damage is still being done.

Zeus was able to infect computers via both Web and Email protocols. It worked by tricking the user into clicking on an email link or a web advertisement. Once the Zeus bot was introduced, it was able to execute and communicate with command and control outside the user's network. The hacker in charge of a particular Zeus infection could then join this computer with thousands of others to form his botnet army. Zeus was particularly treacherous and sophisticated because it could perform so many different criminal tasks including:

- Steal data submitted in HTTP forms
- Steal account credentials stored in the Windows Protected Storage
- Steal client-side X.509 public key infrastructure (PKI) certificates
- Steal FTP and POP account credentials
- Steal/delete HTTP and Flash cookies
- Modify the HTML pages of target websites for information stealing purposes
- Redirect victims from target web pages to attacker controlled ones
- Take screenshots and scrapes HTML from target sites
- Search for and uploads files from the infected computer

- Modify the local hosts file
- Download and executes arbitrary programs
- Delete crucial registry keys, rendering the computer unable to boot into Windows

According to one security expert "It's (Zeus) a very powerful Trojan. The key logger gives the ability to strike at random. The code can easily be modified. Once you have the user's credentials, anybody can access that account and drain it." He explained, "We are at a point where even technically illiterate, unsophisticated criminals can run these kinds of schemes because of the increasing commoditization of malware in the criminal underground".

Phishing Exploits have Targeted Banks

One method that has been widely used by criminal hackers to spread botnets and other malware is phishing. Phishing campaigns are email-based exploits that attempt to introduce botnets and other malware to unsuspecting recipients in order to steal data. They have been successful in mimicking official banking communications and fool customers into divulging private information.

Classic Phishing
Classic phishing exploits try to induce email recipients to provide personal and confidential data with bogus offers. These offers can be in the form of employment opportunities, which are particularly prevalent in an underperforming job market. They can also be in the form of get-rich-quick schemes or business opportunities that offer great reward for little effort. Phishing exploits like these cast a wide net, hoping to get a few gullible recipients to buy into the scheme.

Spear Phishing
A spear phishing campaign is a highly targeted form of phishing that focuses on a single organization or handful of individuals in that organization. Emails appear as if they come from a trusted source, such as a trusted retailer or your bank. Recently, the banking industry warned customers to be on the alert for phishing exploits via email that attempted to trick them into believing that their bank accounts had been closed due to fraud. The victims received an email requiring them to enter their credit card information, including the CV code and expiration date. Later, this information was used to perform illegal transactions.

Blended Threats
More recently, there has been a proliferation of blended threats. The goals of a blended campaign are to capture credentials and embed malicious software onto users' systems to facilitate stealing additional information and/or hijacking the system to send out more spam. In 2010, a blended threat attack that spoofed eBay used an embedded link that took users to a compromised site on eBay's network and a "Download Now" button that when executed installed a Trojan virus. Victims were then directed to log into their eBay accounts—scammers then captured eBay login credentials.

The Risk of Data Loss

Losing customer or client data due to lax security or insider misconduct has plagued banks and other businesses for generations. Since the dawn of cyber communications, these risks have increased, because breaches can involve thousands of victims, and fines or judgments against the offending institution can soar into millions of dollars. In a case against Bank of America in 2011, a breach coordinated by insiders resulted in $10 million being stolen from banking customers. An insider had leaked sensitive data on at least 300 B of A customers including, bank account numbers, Social Security numbers and more.

And the risk isn't only for large banks. Smaller community banks are subject to the same regulations as larger institutions and often don't have access to enterprise security the way a Bank of America or Citicorp might.

This chart shows some recent security breaches experienced by companies and the consequences of losing data:

Company	Event	Damage	Lessons Learned
Heartland Payment Systems (2010)	130 Million Credit Cards Compromised	• Lawsuits / Reputation • Customer Attrition	**Compliance alone is not "Best Practices"**

Company	Event	Damage	Lessons Learned
Sony PlayStation (2011)	PlayStation network breach results in 77 Million customer records being compromised.	• Remediation: $50M • Opportunity Cost: $10M / week • Customer Attrition	**Security to any business is invaluable**
Pentagon (2011)	24,000 files lost because of malware infection	• Compromised Security • Homeland Defense • Secret Data Loss	**Threats can come from anywhere**

The Heartland Case: How Malware can Hide in Your Network

In the case of the Heartland Payment Systems exploit, the method used to compromise Heartland's network was ultimately determined to be SQL injection. Code written eight years ago for a web form allowed access to Heartland's corporate network. This code had a vulnerability that was not identified through annual internal and external audits of Heartland's systems or through continuous internal system-monitoring procedures. In addition, it provided a means to extend the compromise from the corporate network to the separate payment processing network.

Even though the vulnerability had existed for several years prior, SQL injection didn't occur until late 2007. After compromising Heartland's corporate network, the intruders spent almost six months and many hours hiding their activities while attempting to access the processing network, bypassing different anti-virus packages used by Heartland. After accessing the corporate network, the fraudsters installed sniffer software that was able to capture payment card data, including card numbers, card expiration dates, and, in some cases, cardholder names as the data moved within Heartland's processing system.

EdgeWave Enterprise Solutions Support Regulatory Compliance

No matter what regulations govern your organization's activities, the ability to protect your sensitive and proprietary records is paramount to your fiscal health. As the data presented indicates, a lack of compliance carries serious consequences including substantial fines and litigation that can directly affect your bottom line.

Our Secure Content Management solutions, including iPrism Web Security and the ePrism Email Security Suite, not only secure your network against threats to your data from malware, spyware, botnets, P2P and IM, they provide comprehensive drill-down and real-time monitoring and reporting that can help you document your compliance and consistently stay within the boundaries of the legislation affecting your organization. ePrism Data Loss Protection includes automated encryption and data loss detection that can insure sensitive data never leaves your organization unencrypted. Email Continuity assures that in the case of an interruption in your email service, no downtime is experienced and no email is lost. The ePrism Secure Email Archive, with unlimited storage capacity, preserves your organization's email in an unalterable state and indexes them for quick retrieval. And your emails are retained for as long as you subscribe to the service.

iPrism Web Security Exclusive Outbound Botnet Defense

iPrism leverages its exclusive botnet blocking data, which is automatically downloaded to your iPrism, to block criminal malware (botnets, Trojans, worms etc.). This defense protects your organization by blocking bots from connecting with their command and control contacts outside your network. This avoids the expense, complexity and time you might spend deploying an additional appliance or software solution. Once you deploy your iPrism solution and enable botnet protection, it begins to block any bots from being activated, rendering them harmless.

iPrism Blocks Outbound Botnet Attempts

Using the continuously updated botnet database, iPrism monitors and blocks bots from connecting back to the known malicious botnet hosts detected. iPrism blocks any attempt at an outbound connection, over any port, with no known false-positives. Using the botnet technology iPrism is able to inspect and enforce communication attempts over any network port on a per user and/or network-based policy.

To activate the botnet blocking feature, iPrism customers simply select the botnet check box. They can also set email alerts to be generated when a block occurs. Any IP addresses detected will show up in iPrism reporting. Enforcement requires no manual rule or signature updates because iPrism pulls the botnet database as soon as it is updated.

iPrism Botnet Technology

Threat Feeds
iPrism aggregates feeds from leading malware monitors and other proprietary sources to get the extensive list of botnet threats available.

An example of the sources we use includes:

- DShield
- SRI
- ShadowServer
- AutoShun
- Cyber-TA
- PhishTank
- SpamHaus
- Abuse.ch
- Emerging Threats

Correlation Engine
We then filter the raw feeds to produce a predictive threat inventory by evaluating factors such as:

- dates an IP address is first and last seen in their database
- frequency of appearances
- how many sources have reported it

These algorithms are weighted for low false-positives. An address that appears in multiple reports from different sources is more likely to be added than one from the same source multiple times. Likewise, an address which has been on their list before is more likely to be added than one that appears for the first time. Finally they check to make sure that the address is not on a global whitelist of major Internet sites, and if it is, it will be removed. This is done because cybercriminals frequently seek to poison IP reputation services by spoofing the address of someone else and because the major sites are very active in removing malware on their servers and taking over the domains used by bot herders.

ePrism Email Security

ePrism Botnet Outbound Protection
Our email security solutions protects your outbound traffic by identifying computers that have been surreptitiously converted to zombies or botnet clients. Many spammers use viruses, trojans, fake software downloads, and other tactics to create a network of infected client computers that are then used for sending out spam without the user's knowledge. These zombies can result in your network being black-listed by other spam filters, preventing legitimate email sent by anyone on your network from reaching its intended recipient. ePrism Email Security's managed appliances will block outbound spam and malicious email and then notify your network administrator so that any zombie computers can be identified and treated for the underlying infection.

ePrism Zero-Minute-Defense offers Inbound Botnet Protection
ePrism also defends against botnet infections by protecting inbound email from spammers and hackers trying to circumvent existing filters and other defenses in order to introduce bots or other malware into your networks. ePrism's Zero-Minute-Defense Network gathers real-time knowledge from its worldwide sensor network and uses it to create new detection and protection rules. These rules are then sent out as updates on a continuous basis. EdgeWave's data centers recieve these automatic updates instantly, making sure email protection is always up-to-date. The exceptional speed of rule execution as well as the quantity and breadth of rules produced is unrivalled in the industry and adds an important additional layer of protection to your regulatory compliance strategy.

ePrism Data Loss Protection

ePrism includes a content analysis and policy engine that uses proprietary technology to protect private information transmitted via outgoing email. As part of the ePrism Suite, this data protection technology analyzes data being sent out of your network to detect private content in data in motion and prevent sensitive and protected data from leaving your network. EdgeWave Data Loss Protection gives you the powerful tools you need to comply with government regulations, such as SOX, HIPAA and GLBA, and prevents the loss of all types of private data, including, patient healthcare information, financial information and social security and credit card numbers.

Easy Deployment
EdgeWave Data Loss Protection is easily managed from ePrism's central dashboard and can be provisioned immediately to start protecting your organization. With technology that delivers unrivalled accuracy while assuring low latency, you can add a layer of protection to your security strategy without adversely affecting the delivery of your legitimate email.

Proprietary Technology
ePrism DLP analyzes the content of data in motion and detects sensitive data before it can leave the network by performing deep packet inspection across a wide range of hundreds of file types. Additionally, if administrators have enabled ePrism Encryption, they can direct it to be triggered when DLP violations are detected, and the emails in question will be automatically encrypted before they are sent.

ePrism Email Encryption

EdgeWave helps protect against outbound content exposure with ePrism Email Encryption to assure the secure delivery of corporate outbound email to customers, vendors, partners and other individuals. ePrism's next-generation technology is easy to deploy and simple to use, eliminating the cost and complexity associated with many traditional encryption services. As a completely hosted service, there is no hardware or software to implement and encryption can be enabled on a per user basis or as part of an automated routing policy.

Park and Pull Technology
ePrism Encryption's park and pull technology is designed to provide secure communication between the sender and the recipient of messages, even if they are individuals outside and unrelated to a user's organization. All emails using encryption can be routed based on a variety of rules leveraging ePrism's email filtering technology.

Once encryption is enabled, either per policy, per DLP detection or manually, the message is encrypted, sent and stored on ePrism's secure encrypted message portal. A notification message is sent to the recipients that takes them to the secured Web portal where the message can be viewed and action taken.

ePrism Email Continuity

ePrism Email Continuity is an in-the-cloud disaster recovery tool that provides an uninterrupted flow of the email stream in case of planned or unplanned email outages. It assures that users get access to their email and empowers them to manage messaging as though no interruption had occurred. With ePrism Continuity deployed, organizations avoid the productivity losses associated with any disruption in the flow of critical, legitimate business communications.

As part of EdgeWave's ePrism Email Security Suite, Continuity is easy to enable for continuous protection:

- It prevents the loss of access to critical email and avoids productivity loss due to email interruptions
- It's easy to enable from the ePrism central management console – just check the box for continuous email protection
- Once enabled, users have complete access to their email and can remain productive
- ePrism Continuity supports direct LDAP integration so end-users' credentials can be configured to synchronize and will be cached during the outage

Begins Protecting Email Immediately
When an interruption occurs, messages are automatically spooled as soon as the destination mail server becomes unavailable. Once continuity is activated, users can access their email for normal business processes:

- Read, compose, reply to, forward and delete messages
- Upload and download attachments
- Perform header text searches of all the messages in their mailboxes
- The administrator can implement rules to have outbound messages diverted to users' Sent Mail folders to complete the activity synchronization.

Email Retention
ePrism Continuity provides a rolling 35-day backup of both inbound and outbound messages, which are made available for use during the interruption just as they would if messaging systems were working. Emails can be sent and received as if no interruption had occurred.

ePrism Secure Archive

ePrism offers secure email archiving that is scalable to fit the requirements of any size organization. Our affordable archiving retains your email in an unalterable state to help you meet requirements for regulatory compliance, litigation issues, storage management needs, or to fulfill business best practices guidelines. EdgeWave Archiving Services are in-the-cloud, so infinite scalability is assured. And our secure data collection technology provides comprehensive interoperability with all messaging systems.

As a SaaS solution, ePrism Email Archive delivers maximum scalability, provided by off-premises archiving that reduces costs and provides unlimited storage capacity that can grow to meet your organization's demands. Our archive is easy-to-deploy and includes an intuitive interface and role-based administration via your browser, so implementation can be achieved within minutes and ongoing management and maintenance are virtually touch-free.

Archiving is essential to regulatory compliance as well as e-discovery legal requirements. The ePrism Email Archive supports all unicode and search of all languages and includes the features you need to assure regulatory and legal compliance:

- Archiving of all inbound and outbound messages, internal and external
- Legal analysis features including, Annotation, Litigation Hold, Classification Search
- Provides email tagging for Confidential, Privileged, Personal, Reviewed, Responsive and Notify HR
- Automatic backup
- Configurable scheduled archiving
- Unlimited storage
- All data searchable at all times
- Individual End User search
- Supports all messaging systems

EdgeWave SCM Reporting

iPrism Web Security includes comprehensive on-box reporting to help enforce your internal acceptable use and security policies and provide records to help fulfill compliance requirements The ePrism Email Security suite has reporting tools that provide comprehensive data on both inbound and outbound messages, to help you review and manage your organization's email filtering. For all solutions, you may choose from a wide-range of available report templates or customize reports to fit your organization's requirements. Get aggregate reports that include your entire organization or drill-down to individual users. Reports can be generated on-demand or scheduled to generate automatically, when you need them.

EdgeWave Secure Content Management Solutions

EdgeWave™ develops and markets innovative Secure Content Management (SCM) solutions including iPrism Web Security and the ePrism Email Security Suite with next generation solutions for Email Filtering, Continuity, Data Loss Protection, Encryption and Archive. EdgeWave innovative technologies deliver comprehensive protection with unrivalled ease of deployment and the lowest TCO on the market. The company's award winning solutions can be delivered as hosted, on-premises, and hybrid services.