Enhanced Security Services

What is Enhanced Security Services?

The Enhanced Security Services consist of various proactive technology solutions designed to protect and prevent malicious attacks, data compromises, and vulnerabilities. The Enhanced Security Services delivers a holistic approach by adding multiple layers of security to an organization's technology systems, including email communications, user authentication, and mobile devices. The Enhanced Security Services is offered as a subscription service based on the number of users.

Why Do You Need It?

As cyber threats become more widespread and sophisticated, organizations can no longer ignore these risks. As demonstrated by many high profile cyber-attacks (Sony, OPM, Target, Anthem BCBS, Home Depot etc.) a cyber breach can have a devastating impact on an organization including damage of customer/member trust, reputation, and direct financial losses. Cyber security is now an essential component of an organization's technology operations.

How does it work?

The Enhanced Security Services utilizes various tools to proactively respond, protect, and prevent attacks and breaches in five key areas.

Targeted Threat Protection

Targeted Threat Protection protects organizations against spear-phishing and targeted attacks in inbound email by focusing on three measures:

Attachment Protect reduces the threat from weaponized or malware-laden attachments used in spear phishing and other advanced attacks. It includes preemptive sandboxing to automatically security check email attachments before they are delivered to employees. Attachments are opened in a virtual environment or sandbox, isolated from the corporate email system, security checked and passed on to the employee only if clean

URL Protect rewrites URLs in all inbound email. When clicked, the destination website is scanned in real-time for potential risks before being opened in the employee's browser. If the site is safe, it opens as normal. If not, a warning page is displayed and access to the website is blocked.

Impersonation Protect offers instant and comprehensive protection from the latest malware-less social engineering attacks, often called CEO fraud, whaling or business email compromise, by identifying combinations of key indicators in an email to determine if the content is likely to be suspicious, even in the absence of a URL or attachment.

Two Factor Authentication

Two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using a second factor (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password.

Passwords are increasingly easy to compromise. They can often be stolen, guessed, or hacked, you might not even know someone is accessing your account. Two-factor authentication adds a second layer of security, keeping your account secure even if your password is compromised. With Push notification, you'll be alerted right away (on your phone) if someone is trying to log in as you. This second factor of authentication is separate and independent from your username and password.

Mobile Device Security

Mobile Device Security provides centralized management of smartphones and tablets, to help safeguard devices and data. Mobile Device Security includes the following compliance and security features:

- Set granular security policies for specific devices or persona policies that span across devices.
- Specify passcode policies and encryption settings.
- Detect and restrict jailbroken and rooted devices.
- Remotely locate, lock and wipe lost or stolen devices; selectively wipe corporate data while leaving personal data intact.
- Create near real-time compliance rules with automated actions.

Network Vulnerability Scans

OSIbeyond's team of Network Security engineers will perform monthly external and internal vulnerability scans of your organization and identify potential vulnerabilities. High risk vulnerabilities are remediated as part of the Managed Services plan, and a report is provided each month.

OSIbeyond's vulnerability scanner is kept up to date with the latest network and host security audits available and includes the latest security tests for publicly available security patches, disclosed vulnerabilities, and common worms. In addition, UNIX and Windows servers can be audited for compliant configurations. OSIbeyond provides several audit policies based on public best practices for hardening UNIX and Windows servers from the NSA, NIST (FDCC), CERT, and Center for Internet Security. New polices can also be easily created.

Phishing Security Tests

OSIbeyond conducts automated monthly employee Phishing Security Tests (PST). The Phishing Reply Tracking allows you to track if a user replies to a simulated phishing email and can capture the information sent in the reply. You can also track links clicked by users as well as test and track if users are opening Office attachments and then enabling macros.

In case an employee falls for one of the simulated phishing attacks, you have several options for correction, including instant remedial online training. The scheduled monthly simulated phishing attacks are highly effective and immediately allow you to see which employees fall for these social engineering attacks.

Interested in Learning More?

Contact Us