GuideIT
A PEROT COMPANY

End User Protection for Large Campus-Style Retail Environment

GuideIT provides strategic cybersecurity partnership to a campus-style commercial retail environment through consulting, infrastructure, and end-user protection security solutions to implement a defense-in-depth security strategy and position the organization for the future.

The Customer

A sprawling, campus-style retail environment routinely serves over one million annual visitors. The IT infrastructure has become an increasingly important component of the operations touching everything from facilities operations to customer care and internal communications. As the organization continues to grow, new technologies will further enhance operations and marketing outreach as it seeks to expand the customer base.

The Challenge

The organization recently sought a strategic technology partner to provide a comprehensive managed security solution protecting users and the IT environment from risks related to malware, ransomware, email threats, and critical security updates. It faced numerous challenges related to implementing and managing a defense-in-depth cybersecurity strategy.

An aging infrastructure and application environment paired with a lack of internal resources led to a struggle on the part of the organization to keep pace with a changing threat landscape and cybersecurity best practices. The customer realized that email in particular represented significant risk due to the ever-increasing volume of spam and potentially dangerous attachments at the email threat vector. non-technical end users did not have the proper training or awareness to protect the organization, leading to increased risk of a potentially damaging attack.

The existing security solution did NOT:

- **Actively monitor the environment**
- **Centrally manage patches and updates**
- **Enable scalability & adaptability**
- **Provide for remote management & Maintenance**

GuideIT
A PEROT COMPANY

End User Protection for Large Campus-Style Retail Environment

GuideIT Cyber Security solutions safeguard organizations against malicious cyber threats. We utilize individualized approach to provide comprehensive protection that aligns with industry best practices. GuideIT end-user protection enables defense-in-depth strategies for end-user devices such as laptops, desktops and mobile devices which are targeted by malicious actors to gain access into enterprise networks.

The Solution

GuideIT developed a solution to holistically address shortcomings of the aging infrastructure and application environment with a fully managed approach. Comprehensive management and monitoring services focused on endpoint security would address the risk to the environment at the end-user attack surface. A robust strategy for patch management would ensure the environment was properly safeguarded against existing vulnerabilities with the latest updates available. Email security comprising of inbound traffic scanning, link protection, and threat quarantine, would mitigate the risk of ransomware phishing attempts, and malicious payloads. A centrally managed data protection strategy would protect against data loss with full data encryption and in browser web monitoring.

Solution Benefits

- Central management & monitoring
- End-to-end data encryption
- Web monitoring & protection
- Real-time malware protection
- Patch management and deployment
- Email link & attachment scanning
- Outbound data protection
- End user threat awareness training

Why GuideIT

IDENTIFY > PROTECT > DETECT > EDUCATE

GuideIT takes a holistic view of the security environment to evaluate the full threat landscape and identify unique vulnerabilities within an organization. Customers benefit from best-in-class security tools paired with a consultative, strategic approach. Leveraging a defense-in-depth framework that aligns with NIST best practices, the GuideIT security solutions methodology focuses on root cause analysis, visibility, and data-driven decision making to deliver an end-to-end cybersecurity strategy that hardens the IT infrastructure against attacks while also promoting security awareness within the entire organization.

GuideIT
A PEROT COMPANY

End User Protection for Large Campus-Style Retail Environment

GuideIT developed a comprehensive plan to transform the cybersecurity strategy with a defense-in-depth model. Levering industry best practices and the NIST framework, GuideIT assessed the landscape to identify threats and vulnerabilities, created a plan to address risks and promote awareness, and deployed solutions to secure the infrastructure and change end-user behavior, securing the IT environment.

The Implementation

1

ASSESSMENT

Upon initiation of the project, GuideIT quickly performed a comprehensive assessment of the environment to identify and evaluate legacy and stand-alone security solutions in place. High risk devices were identified and prioritized for phase one. Infrastructure and existing security postures were evaluated and tested.

2

PLANNING

With data collected from the assessment, GuideIT cybersecurity professionals developed a comprehensive plan and to address issues with patch management, end-point protection, infrastructure security, and email security.

3

DEPLOYMENT

With data collected from the assessment, agents were deployed within a week to immediately deploy the centrally managed end-point protection solution. The patching program was also deployed targeting the most critical and vulnerable devices first.

The Results

The team identified systems in the environment that had not been actively patched in over six months. The systems were updated and brought into compliance with the policy. Initially, less than 35% of the environment was current with patches released within 30 days. Since implementation of new patch management processes and tools, the environment now maintains a 30-day rolling update ratio of over 95%.

Since the deployment of managed anti-virus, over 400 threats associated with malware, exploits and attempted access have been either blocked or resolved, ensuring the endpoints and users are secure.

The email security solution initially scanned over 83,000 emails effectively protecting the organization from nearly 20 different malware threats and over 50 individual phishing attempts. 27,000 links were scanned and protected, resulting in 70,000 clean messages being successfully derived during the initial deployment.