SECURITY TOOLS OVERVIEW

MERIT 2.0

According to a cyber-readiness survey, small businesses with less than 100 users now face the same risk of attack as a large enterprise. Ransomware attacks are up over 300% and cost American companies over $13B in 2019. Today, businesses of all sizes are under constant threat from cybercriminals who bypass defenses and infect networks, servers, computers, and more. Some threats are automated, while others are highly targeted. With the variety of threats, it's never been more critical to deploy an effective, broad-spectrum security strategy that can detect and prevent today's malware, ransomware, phishing, crypto-threats, and other advanced persistent threats.

ENTERPRISE WIDE STRATEGY

THREAT OPS

Our threat operations tools actively hunt within your network for malicious footholds, detecting threats using innovative techniques, and providing the right tools for fast and efficient remediation. Our tools inventory each application at start-up or user login, so metadata is sent to the analysis engine for inspection. This lightweight design ensures resource-intensive processes never hinder end user's productivity, while the distributed cloud architecture protects users in the office, at home, or on the go.

END-POINT SECURITY

Threat data is delivered to Merit's-protected devices from the cloud in real-time. Our business endpoint protection is a fully cloud-based endpoint security solution that harnesses the power of machine learning by continuously monitoring and adapting endpoint threat detection, protection, and prevention. Our tools defend all users, in the office or remote, via physical and virtual systems against modern threats by employing a multi-layered approach to stop real-time attacks. MERIT business endpoint protection offers a faster and significantly more effective alternative to first-generation business antivirus solutions.

EMAIL CONTINUITY

With email continuity from MERIT, your email stays within reach at all times from any device, regardless of what happens in the world around you. We enable your business continuity plan with uninterrupted email connectivity, providing fail-safe protection for your email service at all times — so email is always accessible.

SAAS PROTECTION

Software as a service (SaaS) Alerts guard against the three most significant threats to a customer's SaaS environment: theft of data, due to employee error, and bad actors. Our tools integrate with a growing list of the world's most popular SaaS applications to identify threats, instantly alert our network operations center (NOC), mitigate and remediate the data privacy and exposure risks, and provide regular reporting for IT security audits.

SECURITY TOOLS OVERVIEW

MERIT 2.0

ENTERPRISE-WIDE STRATEGY continued

FIREWALL AS A SERVICE

Our equipment secures the largest enterprise, enterprises, small and medium businesses (SMB), service providers, and government organizations worldwide. As part of our on-boarding process, the MERIT team installs a new, state of the art firewall to secure your network today and into the future.

BACK UP AND RECOVERY

Our backup technology confirms daily server backups, assuring disaster recovery and intelligent data management for virtual and physical infrastructures. We use image-based backups and recovery for all workloads, from VMware, Hyper-V, Windows, Amazon Web Services (AWS), and more.

GOOD HYGIENE

O365

Microsoft 365 offers the latest A.I.-powered Office applications, including Word, Excel, PowerPoint, and more. With 1TB of cloud storage, premium features, and mobile experiences, you can stay on top of things wherever you are on any device, from your desktop, laptop, tablet, and phone.

MFA and 2FA

Multi-factor and two-factor authentication are authentication methods that a website or application only after successfully presenting two or more pieces of authentication: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). It's an essential safety component to protect your business from hackers and bad actors. Note: Since 2018, enabling MFA has been mandatory for all new MERIT clients.

PASSWORD POLICIES

Long, complex, or rotating - a strong pass strong password contains two of these attributes when they are created uniquely to each site. These combinations make passwords difficult to guess by both humans and password hacking programs which protects your data from unauthorized access. A long password consists of at least 16 characters. A complex password contains a combination of letters, numbers, and symbols. A rotating password amounts to changing your password every 90 days, but only if you do not have a secondary authentication mechanism like a text message or mobile app to approve access. This sounds harder than it really is. The password "IWantWorldPeace4All." would take a computer one hundred quintillion years to crack. Easy to remember, tough to crack.

PHISHING TRAINING

Phishing is a gateway to modern fraud, especially in a distributed workforce. Phishing can be an email, instant message, or text message, fooling your employees to enter personal information or credentials on a fake website with the look and feel of a legitimate site. MERIT's phishing awareness training teaches your employees about phishing tactics and empowers them to resist future phishing scams.