



# Managed Services

---

## Security Guide



[englerit.com](https://englerit.com)

# The Invisible Threat

Breaking down the **damage**  
your business faces after  
a **cyberattack**

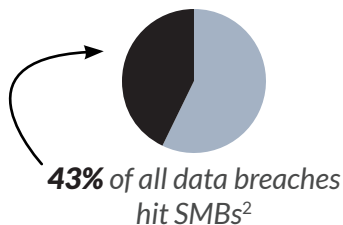


## ► Most cyberattacks don't make the news.

The ones you hear about are high-profile breaches that cost major corporations hundreds of millions of dollars. This gives the general public the impression that cybercrime is relatively rare. This perception isn't just false — it's dangerous.

## SMBs are Targets

Small and medium-sized businesses (SMBs) suffer from a false sense of (cyber)security, with **66%** of SMBs believing they are “too small” to experience a cyberattack.<sup>1</sup>



Malicious actors know that most SMBs simply don't have the cybersecurity measures in place to defend their data.

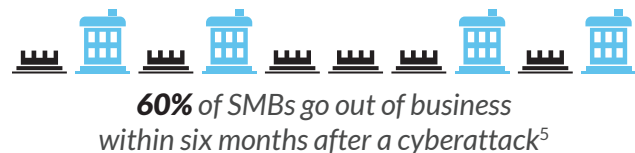
## Not “if,” but “when”...

The odds aren't pretty. **57%** of SMBs will be victimized by phishing or social engineering attacks. **33%** will have devices compromised or stolen. **30%** will experience credential theft.<sup>3</sup>

The global cost of cybercrime damages is predicted to grow considerably:<sup>4</sup>



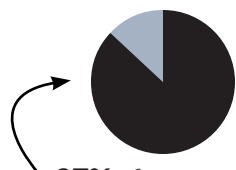
Cybercrime is real, and it's not going anywhere. It isn't rare, it is rampant. The time to get proactive about cybersecurity isn't next year or even next week. It's right now.



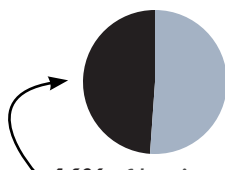
## Reputation Matters

In business, reputation is everything. Suffering a costly data breach can cause your customers to lose faith in your organization and take their business elsewhere.

Would you continue doing business with an organization if you knew it allowed a cyberattack?



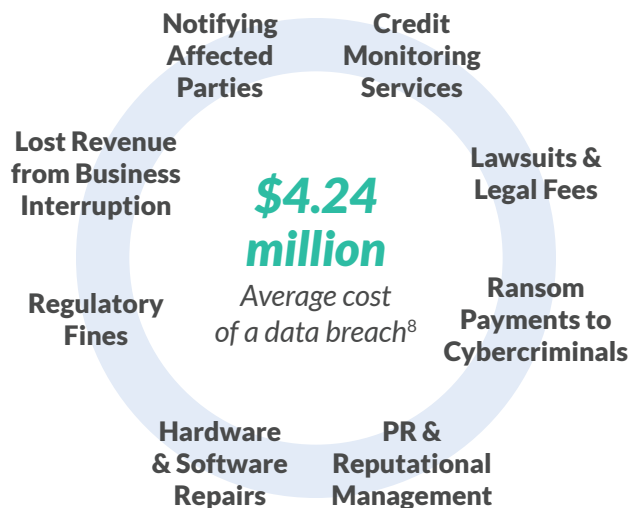
**87%** of consumers are willing to cut ties with an organization after it suffers a data breach<sup>6</sup>



**46%** of businesses have suffered reputational damage as a result of getting breached<sup>7</sup>

## The Many Costs of a Cyberattack

A data breach at your organization can leave you feeling broken, and the business repercussions are severe:



## Vulnerabilities of Remote Work

More organizations than ever before are embracing remote work.

Allowing your employees to work from home has its benefits, but it also makes your organization more vulnerable to cybercrime, especially ransomware attacks. Remote network access is less secure without proper implementation.

- **Remote work** has caused **data breaches** in **20%** of organizations<sup>9</sup>
- **Remote work** has increased the average cost of a **data breach** by **\$137k**<sup>10</sup>



► In order to effectively protect your informational assets, you should implement a framework of prevention techniques at every level in your organization. This framework is called the Blueprint for Prevention.

## Complete Visibility

An organization cannot defend assets it does not know about. This is increasingly becoming important as the workplace expands outside of the office to remote work situations and bring-your-own-device policies that give employees more flexibility to do their work.


A comprehensive prevention strategy provides solutions to combat threats outside of the physical security that an organization would traditionally have.

## Reduce the Attack Surface

Oftentimes, hardware and software come preconfigured with unnecessary applications and insecure default settings for ease of use. This adds complexity to the threat landscape and enriches the attack surface of an organization.

A prevention-centric solution reduces the number of items that are insecure by design, removing threat vectors that an attacker could use to compromise a system.

**You have the power to shift your business** from being reactive, to preventing attacks before any damage can be done with a comprehensive cybersecurity solution from **Engler IT**.



# How do you keep your business safe?

## Stop Known Threats

There is a wealth of intelligence regarding known malicious files and threat vectors that have been used by threat actors to compromise an organization.

Compiling this information and using it to protect an organization's assets is one of the easiest ways to implementing a prevention-centric approach to secure an organization's assets.

## Prevent Unknown Threats

Traditional antivirus solutions rely on malware signatures — unique fingerprints that represent a specific, known threat.

In today's sophisticated threat landscape, this approach is no longer adequate. A comprehensive protection suite coupling machine learning and artificial intelligence is needed to catch unknown and evolving threats to stay ahead of attackers.

## Automation with Human Validation

The increasing use of security tools using AI and machine learning to prevent threats is a double-edged sword. While the protection is superb, no solution is perfect. There is the slim chance that a threat will go undetected by the AI, while legitimate files may be incorrectly flagged as malicious.

This is where trained security professionals come into play — remediating threats that fly under the radar while validating benign files that are classified as a threat.

**Prevention is better than reaction** when it comes to cybersecurity.

***Implement a multi-layer cybersecurity approach.***



# Eliminate the Weakest Link in your Cybersecurity.

**Over 85% of data breaches** in 2020 involved human factors.<sup>11</sup>

**Social engineering** is the process hackers use to break into systems by relying on human nature rather than just technology.

What happens when “John” from Accounting calls into HR because he forgot the door’s key code? What about a password reset?

**All it takes is  
one mishap and  
a hacker is in.**



## Protect your business with ID 20/20® software.

ID 20/20® is a cloud-based, multi-factor authentication tool that takes human error out of live caller verification.

Protect your business from social engineering.



## User Verification, Simplified.

Verification with ID 20/20® software takes less than a minute on average.

No application download  
is required.

## ID 20/20® Software Nuts & Bolts

**ID 20/20®** is an in-house, SaaS application developed by MSP Solutions Group in order to allow a technician to verify a live caller on demand via a contact's email or cell phone.

### How It Works:

**ID 20/20®** software uses electronic communications to verify a user via either text messaging or email. This allows you to leverage telecommunications services tied to a specific individual in order to verify their personal identity (preventing identity fraud), prevent privilege escalation via social engineering, or provide security by ensuring your technician is speaking to the correct individual.

An 8 digit code is dispatched to the selected communication medium (cellular phone or email) which a technician verifies with the system. If this code is incorrect, the system will log and alert the technician.

**ID 20/20®** software takes the questioning and human element out of the equation for preventing unauthorized access or other identity fraud without taking the humanity out of the call.

**ID 20/20®** software operates from a standalone SaaS cloud platform circumventing the need to download or maintain an application. This allows verification from any system with a modern browser and an internet connection without any separate download. Just because a tech is onsite, doesn't mean they can't follow process.

A woman with long brown hair, wearing a black headset with a microphone, is smiling. She is wearing a light blue button-down shirt. The background is blurred, showing other people in an office setting. Overlaid on the right side of the image is white text.

**Engler IT**  
is proud  
to utilize  
**ID 20/20®**  
to protect  
clients  
against social  
engineering  
attacks.

## Next Generation Preventive Endpoint Protection

The game has gotten more complex, and a broader set of countermeasures is needed. Modern infrastructure defense requires the use of threat intelligence to search for malware and threats that are already inside systems, in addition to using next-generation technologies like deep learning, fileless activity detection, EDR, and rollback remediations to keep new threats out.

Endpoint security monitoring and management tools must deliver high accuracy in identifying legitimate threats and avoiding false positives and be able to contain malicious applications at the first encounter.



*A recent study found that legacy AntiVirus and EDR solutions prevent compromises **less than 50%** of the time.*

### ADVANCED ENDPOINT PROTECT FEATURES



Artificial Intelligence



Powershell Script Control



Deep Static Analysis



Enhanced Ransomware Prevention



Zero Time Prevention



Behavioral Analysis



Cloud Managed



Resource Theft Detection (Crypto Mining)



Suspicious Tool Detection



System Process Verifier

### SECURITY OPERATIONS CENTER SERVICES



Security Event Incident Monitoring - 24/7/365



Incident Response



Event Correlation and Human Analysis



Script Monitoring



Policy Customization



Threat Hunting



Security Reporting



Remediation Support



US-Based SOC Teams

**MAED (Managed Advanced Endpoint Defense)** is the premier preventive endpoint protection solution designed to successfully manage and protect your environment, no matter how large or small, before catastrophic incidents can occur.



Conventional solutions, built for on-premises email have **failed** to adequately adapt for the cloud.

## Fully Secure Your Cloud Email and Collaboration Apps

Proxies and gateways impair native security tools, will forever be blind to cloud threats like compromised accounts and don't extend protection across connected applications like SharePoint and Slack.

With a unique architecture built specifically for the cloud, SCUD connects to your environment and scans for threats after your existing security — but before the inbox. Because it deploys inside the cloud, it offers the best defense against insider threats, Business Email Compromise and breached accounts. SCUD deploys like an app, and configures in a few clicks, to start blocking phishing, malware, and other advanced threats that have evaded existing security.

### CLOUD APPLICATION DEFENSE FEATURES



**Collaborative  
Policy Optimization**



**WORX Incident  
Response**



**Anti-  
Phishing**



**Malware  
Protection**



**Compromised  
Account Detection**



**Data Loss  
Prevention**



**URL Click-Time  
Protection**



**Encryption for  
Office 365**



**Shadow IT  
Detection**

### SECURITY OPERATIONS CENTER SERVICES



**Security Event Incident  
Monitoring - 24/7/365**



**Incident  
Response**



**Event Correlation and  
Human Analysis**



**Script  
Monitoring**



**Policy  
Customization**



**Threat  
Hunting**



**Security  
Reporting**



**Remediation  
Support**



**US-Based  
SOC Teams**

**Artificial Intelligence (AI)** learns from relationships between employees, historical emails, and communication patterns to build a custom threat profile that blocks attacks specific to each organization. No change to MX records means that it is impossible for hackers to see if an organization is using SCUD to secure their cloud. At the same time, the seamless security doesn't interrupt user experience in cloud applications.



### ZERO-TIME THREAT PREVENTION

Predictive threat prevention platform with multi-layer protection against any known or unknown threat.

Deep Instinct's protective solution can be applied to any device with any operating system.

**100%** prevention rate | **ZERO** false positives

*Independent Lab Test, April 2019*



### CLOUD-BASED SECURITY PLATFORM

Protection against threats on the internet such as malware, phishing and ransomware.

OpenDNS is a cloud security platform that provides the first line of defense against threats wherever users go.

Cisco analyzes over **175 billion** internet requests a day

*OpenDNS is part of Cisco*



### MICROSOFT DEFENDER FOR OFFICE 365

Protect all of Office 365 against advanced threats like business email compromise and credential phishing.

Automatically investigate and remediate attacks.

**Best-in-class** configuration, protection and detection

*Against both known and emerging email-based threats*



### ADVANCED THREAT DETECTION

Threat detection and swift remediation techniques in the case of a data breach.

Huntress Labs is a leading provider of advanced threat detection and actionable cybersecurity intelligence.

**12K+** discovered breaches

*Since 2017*



### POWERFUL PASSWORD MANAGEMENT

Keeper is the top-rated password manager for protecting you, your family and your business from password-related data breaches and cyberthreats.

Stay protected and productive remotely.

Trusted by **thousands of businesses**

*Available for Windows, iOS and Android*



### USER VERIFICATION

Secure your clients from social engineering attacks.

ID 20/20® software makes the process nearly completely transparent to the end user.

Secure access with MFA **without an extra application**

*Prevent unauthorized access via social engineering*



## Security Stack & Client Testimonials

# “————— What are others saying? —————”

## **Detect a ransomware attack before it can do damage**

*Because of The 20 MSP's top-notch security stack, we were able to detect a ransomware attack on a client and stop it before it could damage their files.*

*We were able to respond within an hour because of The 20 MSP's 24/7/365 monitoring and continual maintenance.*

## **Stop social engineering in its tracks**

*We looked around for a solution to social engineering that (a) worked, and (b) made things easy on our clients and end users.*

*ID 20/20 checked all our boxes. There have been multiple social engineering attempts on our clients' businesses since we adopted ID 20/20 software — but not a single one has been successful.*

## **Stay a step ahead of threat actors**

*The difference between the legacy solutions that we used to rely on and the next generation tools that make up The 20 MSP's security stack — it's like night and day.*

*The advanced AI and machine learning have been particularly eye-opening. Threats to our clients that we used to have no way of seeing are now easy catches.*



**We're happy to answer any questions you may have.  
Contact us to schedule a FREE consultation!**

### **Sources:**

1. Keeper Security 2. Verizon 3. Ponemon 4. Cybersecurity Ventures 5. National Cyber Security Alliance  
6. PwC 7. Forbes 8. IBM 9. Malwarebytes 10. IBM 11. Verizon

# Implement a multi-layer cybersecurity approach.

You know you're a target for cyberattack.

Proactively prevent cyberthreats  
to stop bad actors in their tracks.

**Get in touch today!**

**englerit.com | (443) 390-2575**

## **Corporate HQ**

1910 Towne Centre Blvd, Suite 250  
Annapolis, MD 21401

## **Operations Center**

6600 Chase Oaks Blvd, Suite 100  
Plano, TX 75023



© 2022, MSP Solutions Group LLC ALL RIGHTS RESERVED.

This digital copy is licensed for performance/presentation purposes only. DO NOT DUPLICATE.